A Reliable Multicast Routing Protocol for High-speed Mobile Ad Hoc Networks: R-ODMRP

Zhiming Xu
Department of Space Engineering, Academy of Opto-electronics, Chinese Academy of Sciences, Beijing, China; School of Information Science and Engineering, Graduate University of Chinese Academy of Sciences, Beijing, China
Email: zhimingxu2006@gmail.com

Yu Wang
Department of Space Engineering, Academy of Opto-electronics, Chinese Academy of Sciences, Beijing, China
Email: wynt@aoe.ac.cn

Jingguo Zhu
Department of Space Engineering, Academy of Opto-electronics, Chinese Academy of Sciences, Beijing, China
zhujingg@mails.gucas.ac.cn

***Abstract*—Based on the ODMRP (On-Demand Multicast Routing Protocol) in MANET (Mobile Ad hoc NETwork), a reliable ODMRP (R-ODMRP) is proposed for preferable throughput and especially suited for high-speed MANET, which includes packet acknowledgement, lost packet recovery, secure authentication and QoS based packet delivery. With the exploration of active network, R-ODMRP constructs the multicast routing based on the cluster, establishes a distributed mechanism of the acknowledgment and recovery of packet delivery. Along with cluster key distributed in one cluster, this protocol can authenticate the consistency of multicast source and receivers depending on local security strategy. The specific mesh links are adaptively chosen by virtue of the descriptive QoS vectors meanwhile, the forwarding nodes can flexibly schedule different multicast packets according to the types of the multicast applications. The performance of the proposed schemes is evaluated based on the network simulator and achieves a significant improvement.**

***Index Terms*—ad hoc networks; mobile; reliable; clustering; ODMRP; R-ODMRP**

I. INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is an autonomous system with large numbers of mobile nodes which voluntarily organize into a network and communicate with each other over wireless links [1]. In a MANET, there is no differentiation between a host and a router, since all nodes can be senders or receivers as well as forwarders of traffic. Moreover, all MANET members can remove freely. As needn't any infrastructure but have high mobility, MANETs are applied to critical environments where robustness and reliability are essential, such as military battlefield, emergency rescue, vehicular communication, mining operations and so on. In the presence of these applications, multicast is very important and useful that holds down network bandwidth and resources, since a single message from one source can be delivered to the multiple receivers simultaneously. One of the main challenges for multicast routing in MANETs is the need to achieve robustness under the condition of frequent, especially high-speed mobility and nodes outages. For this purpose, mesh-based protocols construct a mesh for forwarding multicast packets which can be delivered even in the presence of links breaking, and thus meet robustness and reliability demands with path redundancy owing to meshes on networks.

Existing multicast routing protocols for MANET can be classified into two kinds: tree-based and mesh-based protocols. The tree based ones, for example MAODV (Multicast of Ad hoc On Demand Distance Vector) typically representing tree-based schemes, unfits high-speed ad hoc networks. Typical mesh-based multicast routing protocol is ODMRP (On-Demand Multicast Routing Protocol)[2], which uses the concept of forwarding group, builds multicast mesh which is maintained through soft state and gains high performance [3, 4]. In [5], V. Kumar, et al. obtains comparative conclusions about MAODV and ODMRP based on the simulation results. Even though the performance of all multicast protocols degrade in terms of packet delivery and group reliability as node mobility and traffic load increases, mesh-based protocol ODMRP performs considerably better than tree-based protocol MAODV. ODMRP brings forth decent robustness in virtue of its mesh structure. MAODV underperforms as well as the other protocols with a view to packet delivery ratio and group reliability.

Although ODMRP holds above-mentioned visible advantages and also can support unicast in high-speed networks environments, it doesn't take security, reliability and QoS provision into consideration.

In this paper, we present a reliable multicast routing protocol R-ODMRP based on ODMRP in MANET. We set up multi-level clusters so that the multicast packets can be buffered reasonably in cluster head and

doi:10.4304/jsw.5.1.20-27

acknowledged distributedly to procure the congestion avoidance. It is also convenient to resume the lost packets. In order to communicate safely, a reliable authentication mechanism based on local information is proposed. With the definition of QoS descriptive vector *DV*, QoS multicast can be implemented by local QoS link selection and packet scheduling based on priority.

The remainder of this paper is organized as follows: Section II reviews the related works about multicast routing protocols. The models we used for R-ODMRP will be illustrated in section III. Section IV describes the R-ODMRP in detail. The simulation and results analysis will be give out in section V, section VI concludes this paper.

II. Related Works

As a promising network for future mobile applications, MANETs are attracting more and more researchers to study, especially on the routing protocols. For example, the multicast extension of Ad hoc On Demand Distance Vector (MAODV) routing protocol uses destination sequence number for each multicast entry but with a lot of control messages [6], Although MAODV can offer more efficient path, its ineffective link repair method may tempestuously decrease the packet delivery ratio in the situation of the mobility, which also increases the redundant control overhead and the probability of packets collision. Yao Zhao et al. presents ODMRP-MPR in control packets flooding and unidirectional links in [7], ODMRP-MPR uses multipoint relay technology to reduce the control overhead, optimizes the mesh structure and inducts congestion control to obtain high scalability. Chien-Chung in [8] gives out a protocol-dependent multicast packet delivery improvement service called PIDIS which uses swarm intelligence to report on lost packets effectively, adapts to network conditions and lost message recovery attempts are made. PIDIS employs the positive and negative feedback mechanisms of swarm intelligence to quickly cast about good candidate routes. ODMRP+PIDIS can work more efficient than ODMRP. There are papers about energy-aware multicast routing protocols and high throughput multicast routing solutions. H. Moustafa presents source routing-based multicast protocol (SRMP) in [9], which decides stable paths based on links availability according to future prediction of links state, and higher battery life paths tending to power conserving. Because of SRMP based on the source routing mechanism in DSR unicast protocol, there exist shortcomings of the unicast groundwork. In [10], M. Tridib describes a node-based energy metric that minimizes the energy consumption of the multicast tree in consideration of the overhearing cost, and applies it to Self-Stabilizing Shortest Path Spanning Tree protocol to obtain energy-aware SS-SPST, which misfits the high-speed ad hoc networks. However, these references mentioned above don’t consider the safety or QoS.

There are two solutions for reliability of the multicast transmission. One is multicast reliability grounded on MAC layer [11] and reliable coding [12], which utilizes the floor technologies of the forward error correction (FEC) and grouping coding. The other makes use of the reliable strategies including retransmission of lost or error packets and congestion avoidance. The redundant multicast networks can also be used to assure reliable multicast [13, 14]. R. Vaishampayan represents an adaptive mesh-based multicast mechanism that controls mesh redundancy by link reliability metric called Mesh Reliability Index in the neighborhood of the node. Reza proposes a novel secure multicast routing protocol that withstands insider attacks from colluding with adversaries, but this paper doesn’t take external assaults into account [15]. Jorg investigates how to manage key and encrypt, but he doesn’t consider the packet acknowledgment and the lost packet recovery [16]. Y. Soon in [17] presents an enhancement of ODMRP based on receivers’ loss reports to source with the refresh rate dynamically adapted to the environment. If time out expires, the disconnected node proactively grafts onto the FG mesh instead of waiting until next route refresh.

QoS multicast routing protocols provide a mechanism to establish a QoS multicast session. In [18], L. Layuan discusses the challenge of QoS multicast protocol in Ad hoc networks and represents a solution, which can perform routing decision by means of local link state. A survey of existing QoS multicast routing performance is epurated in [19], the author advocates that *fuzzy logic* and *neural* networks can be appropriate methods to supply the required bandwidth for diverse services, and considers success ratio in establishing session as an important metric to evaluate the multicast protocols. While a mesh based QoS multicast routing protocol is shown in [20], four different configurations that involve waiting at receiver or not and on demand or periodic maintenance are proposed and studied. This protocol uses bandwidth reservation and takes over only requests satisfying bandwidth demand.

With regard to ODMRP, it is an on demand protocol. A source initiates JOIN QUERY flooding only when it wants to send data. The sender periodically floods JOIN QUERY control messages, and all intermediate nodes establish routes to the sender. Members send JOIN REPLY messages generated by goal receiver(s) backtracking to the source. Route redundancy from sources to receivers constitutes a mesh of nodes called FG (forwarding group) [21], which provides more plenitudinous connectivity among multicast members and avails to countervail nodes displacements and channel fading. So, frequent reconfigurations in tree-baesd structure protocol are needless. Source broadcasts data packet to neighbors, and Forwarding Group nodes forward multicast packets via flooding on the forwarding mesh restrictively as shown in Fig. 1. Soft state is maintained with no explicit receiver joining or leaving messages and forwarding nodes clear state upon timeout, which is extremely robust to mobility, channel fluctuating, obstacles, and interference.

III. The System Model for R-ODMRP

A. Relay-based Multicast Forwarding Cluster

Considering a network NW= (N, L), here N is a set of all the mobile nodes of the network, and L is the set of all the direct links between mobile nodes in N. If we assume the direct link or path set between n_i and n_j is $l(i, j)$and $R(i, j)$respectively ($i, j \in Z^+$), it is obvious that $l(i, j) \subset R(i, j)$. Each node periodically sends HELLO messages that comprise a list of neighbors from whom it can receive packets. So n_i can get not only the one-hop neighbor nodes set $NE_{1,i}$, but also the two-hop neighbors set $NE_{2,ij}$ by exchanging the neighbor nodes set with the neighbor n_j. Meantime, it includes some characteristic information W about the links, such as bandwidth, delay and so on. Θ denotes the redundance degree, namely the amount of the links between n_i and n_j and Θ >=1 means at least a link.

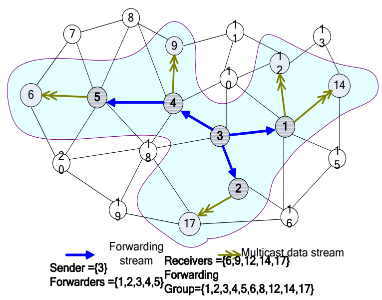


Figure 1. Mseh based multicast forwarding.

Definition 1 For any n_i, there is a subset $sub(NE_{1,i})$ of $NE_{1,i}$, if $NE_{2,i} \subseteq \bigcup_{j \in sub(NE_{1,i})} NE_{1,j}$ with a restriction(W, Θ), we call $sub(NE_{1,i})$ a broadcast subset of n_i.

According to the ODMRP, the JOIN REPLY will backtrack to the source from the receivers after the JOIN QUERY is received. So the nearer to the multicast source, the much heavier traffic in networks. We call a node nearer to the source "upstream node" and the farther one "downstream node". The confirming subset is defined as follows:

Definition 2 For any upstream node n_i , there exists $CF_{2,i}$, $CF_{1,i}$ is a subset of $NE_{1,i}$, if $CF_{2,i} \subset \bigcup_{j \in sub(CF_{1,i})} NE_{1,j}$ with a restriction (W, Θ), we call $CF_{1,i}$ a confirming subset of n_i.

$CF_{2,i}$ is two-hop downstream forwarding nodes subset of n_i and $CF_{1,i} \subset NE_{1,i}$, while $CF_{1,i}$ is one-hop feedback forwarding nodes subset in $NE_{1,i}$.

Our proposed multicast forwarding cluster is based on the broadcast subset and confirming subset. Once source S has any multicast packet to send, it will sends JOIN QUERY message through its *sub* ($NE_{1,i}$) and any others that received the JOIN QUERY forward the messages to their downstream nodes according to their own broadcast subset. JOIN QUREY comprises message ID and number of hops which are used to distinguish multicast source and group from network so as to choose the shortest route with loop avoidance.

Cluster head voting: When any node receives the JOIN QUERY and wants to join the group, it will add the ID into its multicast table and generates a JOIN REPLY which comprises multicast ID, the upstream one-hop node address and amount of the cluster hops. And then, the node forwards it to its upstream nodes. The cluster hops are either fixed to accord with multicast types or tailored by JOIN QUREY. Generally speaking, the amount of the hops for multimedia application is less than that for others. Whoever receives the JOIN REPLY will record the downstream node and check if the hops passed **equals to the ones expected. If they are equal, local *CC* is** set to 1, which means current node is candidate cluster head and cleans the number of the hops, then forwards the JOIN REPLY until to the source, S. Then, S will compute the $CF_{2,s}$ and $CF_{1,s}$ through the downstream node. And S sends confirming packet for cluster-head to the nodes in $CF_{1,s}$. The candidate node who receives the confirming packet earliest will be the cluster-head and sends cluster-head assertion to other nodes in $CF_{1,\ n_c}$. All the forwarding nodes between two heads will join in the cluster near the source, or an upstream cluster.

We assume the clusters as shown in Fig. 2, in which S is the multicast source and a cluster head of $Clus_1$ which is the upstream cluster of $Clus_2$ and $Clus_{2'}$ (Θ =1). The cluster head can buffer, confirm, authenticate and mediate which will be discussed in section 3.

B. Cluster based Authentication Strategy

It is assumed that each node has a symmetric key K, a public key K_{pub} and a private key K_{pri}. Any node can exchange public key with neighbors through HELLO message. Note that n_i uses $K_{pub,j}$ to encrypt the message and sends it to n_j, n_j decrypts this message by $K_{pri,j}$. Specially, symmetric key K is used for signature and authentication.

It will remarkably increase multicast delay and complexity if all the nodes perform the operation referred above [22]. Hence, we design a cluster based authentication strategy. After a cluster head is voted, cluster key CK will be distributed with the cooperation of SN which is the neighbor's signature and exchanged

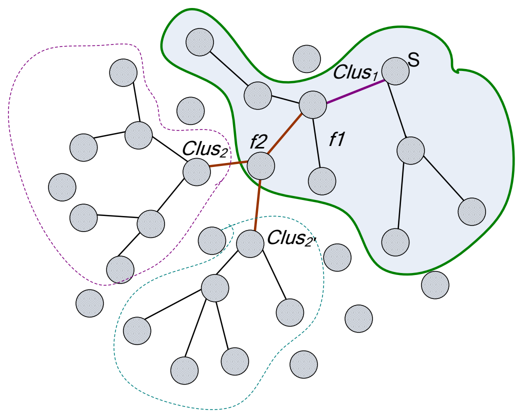


Figure 2. Hierarchical multicast cluster

through Key message after HELLO message. A new CK distribution will be triggered when 1) a new node joins in;

2) a node leaves explicitly or implicitly; 3) the cluster is initialized.

Exchange of K_{pub} and SN is shown in Fig. 3. The HELLO message from n_j to n_i includes $K_{pub,\,j}$ and other information. CK is exchanged as shown in Fig. 3, after that each node in the cluster owns its cluster key. SN_i and SN_j are the signatures of n_i and n_j, respectively. In Fig. 4, *CK_request* is the request for cluster key and CK_{ID} is the cluster key belongs to the cluster ID. The node between $Clus_x$ and $Clus_y$ needs to maintain two cluster keys in order to assure the data transmitted between clusters in security.

C. QoS-Aware Model

To satisfy the multicast routing requirements as possible after the mesh created, we define a vector DV to describe the QoS for forwarding path $l(i, j)$ and $DV(i, j)=(D, SNR, B, Buffer, E, COUNT)$. Here D is the delivery delay (or the sum of delays) for $l(i, j)$; SNR is the ratio of signal and noise of n_i received from n_j. B is the bandwidth of $l(i, j)$,while *Buffer* is the length of buffering queue which can indicate the QoS performance of networks exactly when they almost have the same bandwidth. E is the residual energy of a node that can support energy-aware routing. *COUNT* is a 5 bits binary number and each bit denotes the validity of a corresponding value in DV. A bit is "0" means the correlative value in DV is void and "1" means that is valid. So DV is scalable and flexible.

The weights of W referred in 3.1 are identical with those in DV. But the difference is that W denotes the requirements description of links or nodes which are the idiographic limits or interzone values, while the DV denotes the measured values of links or nodes. Furthermore, the weights in W or DV are arranged to satisfy a certain partial ordering relation that embodies the sequence of route selection.

To be simple during the route selection, we define several specific W corresponding to the multicast applications. That is to say, we have a W_M for every multicast application T_M. There is a mapping congruence $T \rightarrow W$ for set T and M when creating the cluster based mesh. $L(i, j)$ will be chosen if $l(i, j)$ satisfies the following relationship:

Hard-rule For $\forall T_M$, $DV(i, j) \geq W_M$,

If $DV(k, m) \geq W_M$ for $\forall l(k, m)$ *(* $k, m \in N$ *),* so we have*:*

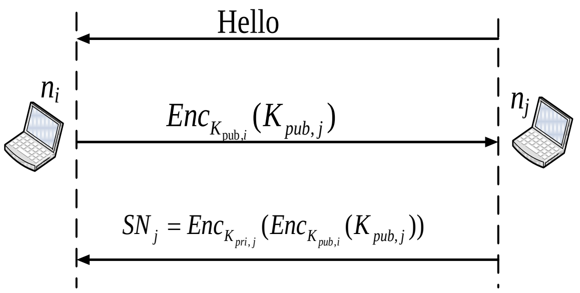


Figure 3. Exchange of public key and signature

$$Gap(DV(i, j), W_M) \leq Gap(DV(k, m), W_M) \quad (1)$$

Gap above is defined as:

$$Gap(DV(i, j), W_M) = \sum_{\gamma=1}^{5} Gap_\gamma(DV(i, j)_\gamma, W_{M,\gamma})$$
$$= \sum_{\gamma=1}^{5} \beta_\gamma \left| DV(i, j)_\gamma - W_{M,\gamma} \right|$$

If one link selection through hard-rule is fail, others will be checked until all the links cannot satisfy this rule. Then, Soft-rule will run when hard-rule cuts no ice.

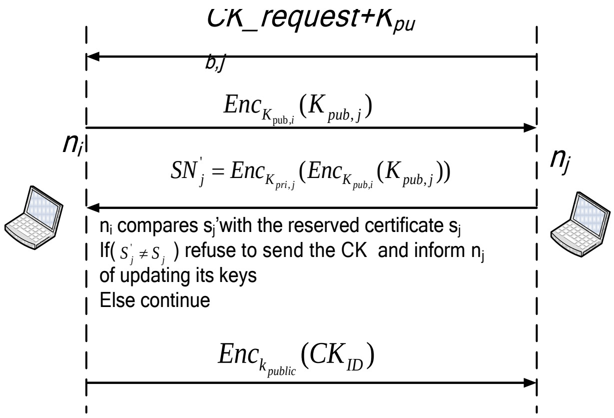


Figure 4. Exchange of cluster key

Soft-rule For $\forall T_N$, if $\forall$ *l(k`,m`)* and $DV(k', m') < W_N$, then, *l(I,j)* will be chosen, if *l(I,j)* for $\forall$ *l(k`,m`)* satisfies:

$$Gap(DV(i, j), W_N) \leq Gap(DV(k', m'), W_N)$$

That is min (Gap ($DV(k, m)$, W_N)) (2)

IV. Reliability Multicast Routing Protocol: R-ODMRP

A. Maintenance of Multicast Cluster

Cluster-based mesh, which is created following confirming subset and route selection strategy, is dynamic as the values of DV vary while mobile nodes wreck, join or leave at random. Thus, the mesh needs to be maintained in several situations. If upstream node n_j can not receive any HELLO message from downstream node n_i when t_l is overtime in the same cluster, the upstream node n_j will cut out the route to the downstream node n_i and search a new one. Node n_j searches its neighbor set to check if it can reach n_i via neighbors. If one of the neighbors can reach n_i, n_j will resume the route. Otherwise, n_j will search its neighbors of the neighbor until it finds a route to n_i or reaches the edge of the network. If a multicast member R does not say HELLO to upstream node, which means that R has quit the group, the upstream node will report and cut out the route. If the path between n_i and n_j can not satisfy (1) hard-rule, the protocol will choose a path to satisfy (2) soft-rule.

B. Multicast Packet Forwarding

Finished creating cluster-based mesh, multicast source S starts to send data packets through multicast mesh. Each cluster-head will produce a weight and put it into multicast packets and sent to downstream nodes in one cluster. Other nodes along the mesh will forward multicast packets as following if they receive the packets.

Rule of forwarding For $\forall n_i \in C_a, \|CF_{1,i}\| = Degree_i \geq 1$, n_i will divide a weight ($weight_i$) into $Degree_i$ ($Degree_i \in \mathrm{N}$) different subweights, and then sends them to the $Degree_i$ downstream nodes, respectively.

Here, C_a is the set of nodes in a^th cluster, $CF_{1,i}$ is the set of downstream nodes of n_i. Hence, each node receives a multicast packet with exclusive *ID* and sole subweight within one-hop. $Degree_i$ denotes the nodes number in $CF_{1,i}$.

Rule of confirming For $\forall n_j$, $0 < j \leq Degree_i$, $n_j \in CF_{1,i}$, 1) if $\|CF_{1,j}\| = 0$ and the packet ID is P, n_j will send the subweight received from n_i and *P-ack* to n_i, and confirm the packet P; 2) if $\|CF_{1,j}\| \neq 0$, n_j receives the *P-acks* from its downstream nodes, the sum of their subweights is $weight_j$ and the packets ID are all the same P, n_j will send the received $weight_j$ from n_i and *P-ack* to n_i, and confirm packets P. Timers are maintained for confirming.

If the sum of their subweights isn't equal to $weight_j$ and $\rho \geq \eta_0$, n_j will send the *pivotal-P-ack* or *incomplete-P-ack* to n_i, e.g. in terms of lose-tolerant applications, especially for high real-time application. Otherwise, n_j will not provide with any *ack* in response, until the timer is out and start retransmitting. Here, ρ is the ratio of pivotal reception, η_0 is a special threshold of multicast type relative to a certain application.

Obviously, $\sum_{j=1}^{Degree_i} weight_j = weight_i$ in the rule of forwarding. The $C_{a.head}$, head of the a^th cluster confirms P to upstream cluster when received all the confirmations in the cluster. If any n_i detects that the sum of the confirming subweights for P is less than $weight_i$, n_i will check the buffer for packet P at first. Node n_i will resend packet P to the downstream nodes if found packet P, or else request packet P from one upstream node. This process will continue until it reaches multicast source S or finds packet P.

C. Credible Packet Forwarding

With the authentication strategy mentioned in 3.2, credible local communication routing is built and cluster head can distribute cluster key independently. The goals of the implementation: 1) multicast packets are from the legal source; 2) packets are not juggled during the delivery; 3) receivers are legal group members. Multicast source S generates a multicast key *MBK* through which multicast packet P is encrypted and then encrypt *MBK* with a local cluster key *CK*. Finally, the message is transmitted as shown in Fig. 5(a). Any node in the same cluster just needs to transmit the packet based on local strategy. If the packet will be sent across clusters, the message will be tackled as Fig. 5(b), exchanging the cluster key. The multicast data only will be decrypted by receivers, as shown in Fig. 5(c).

In Fig. 5(d), we show how the multicast packet reaches receiver member R through different clusters. The transmission process between cluster a and cluster b is shown in Fig. 5(b), node in a will decrypt *MBK* with CK_a, encrypt *MBK* with CK_b and then send to the cluster b. Receiving the message, R will decrypt multicast data with *MBK* which can be deprived by cluster key decryption *MBK*. Undoubtedly, any abnormity will lead to inaccuracy for access multicast data and request the packet retransmission from the cluster head again.

D. QoS Provision

The QoS is enabled through spanning forwarding mesh and priority based packet scheduling. Specifically, forwarding mesh is based on the hard- or soft-rule, the QoS forwarding routing can be provided through hard-rule, the soft-rule just can offer the best effort forwarding routing for multicast service T_M.

Rule of packet scheduling For any two packets P_e, P_f and a default threshold BPN_{th}, when the forwarding queue length BPN of relay node $n_{forward}$ satisfies $BPN > BPN_{th}$, $n_{forward}$ will prefer forwarding P_f, if $\Gamma(P_e) \leq \Gamma(P_f)$.

Here $\Gamma(Z)$ is a classification function which can achieve the mapping from $Z \to \Gamma(Z)$, PS and PT are the set of multicast packets and multicast packet types, respectively. Where $Z \in PS$, $\Gamma(Z) \in PT$. Actually, the classification can base on application type of packets, for example, real time multimedia service. It also can base on packet characteristic; for example, control packet and data packet or the priority of different sources. Rule of packet scheduling is very efficacious to keep the traffic on the networks smooth.

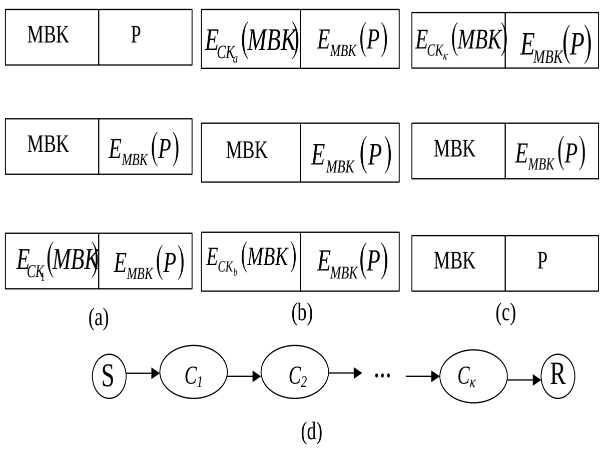


Figure 5. Credible packet delivery

V. PERFORMANCE EVALUATING

A. Simulation Environments

We consider an ad hoc network with full-duplex links which are unidirectional with the probability 0.02. The effective multicast radius of all links is 250 m and carrier sensing radius is 500 m. We use the radio transmitting model in free space at physical layer and the DCF and CSMA/CA mechanism in IEEE 802.11 for media access controlling at MAC layer. The length of multicast packet is assumed 512 bits while the bandwidth of wireless channel varies from 512 Kbps to 2.5 Mbps. In consideration of the control packets, we just count the number and ignore the size. Time spent to discover neighbor is 2.5 s and the update period is 10 s. Multicast member moves in random track at a speed of 1-10 m/s while it may pause for 0-2 s during its motion.

The number of mobile nodes ranges from 30 to 60 in the 1000 m×1000 m square area, which is established with NS2 and MATLAB. In order to predigest, we think that two nodes are neighbors when they can directly communicate with each other. A mobile node owns a buffer that ranges from 32 Kbits to 2 Mbits and has 3 energy levels. We run the simulation 500 s every time and the numerical results are all averaged.

B. Numerical Results and Analysis

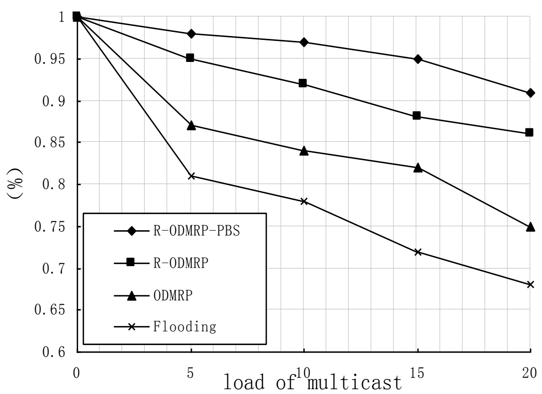


Figure 6(a). The ratio of successful delivery in different loads

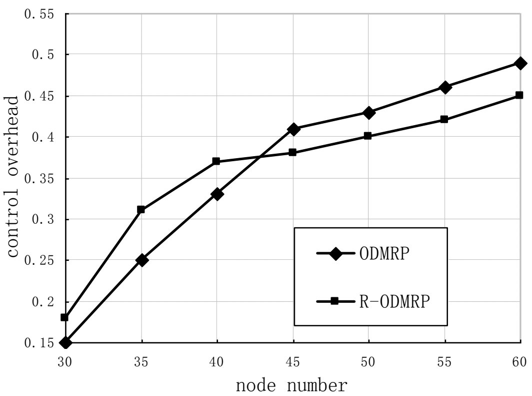


Figure 6(c). Control overhead in different scales

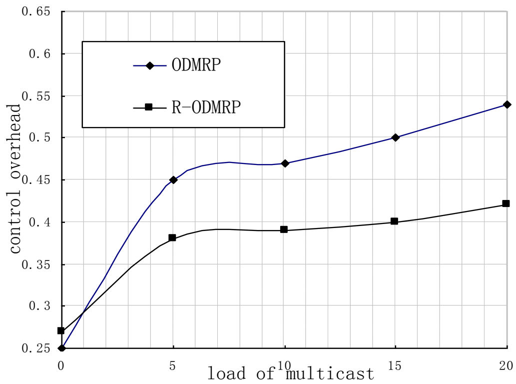
In order to evaluate the performance improvement of R-ODMRP, we compare it with ODMRP and Flooding based multicast protocol. The evaluation metrics include the ratio of successful delivery, control overhead and the average delivery delay.

(1) The ratio of successful delivery

The ratio of successful delivery can reflect the

reliability of routing protocol. The number of mobile nodes is 60 and multicast load range changes from 4 to 20 packets per second. We observe their different performances by varying the multicast load and result is given in Fig. 6(a). Only the R-ODMRP-PBS uses priority based scheduling.

Undoubtedly, the ratio of successful delivery of R-ODMRP is higher than that of ODMRP and Flooding, because the cluster based mesh improves the reliability of packet delivery through distributed packet acknowledgement and lost packet recovery. In contrast, Flooding incurs too much traffic and lacks of measure to resume the lost packets. It will be worse when the packets are blocked or impacted. ODMRP works better than Flooding but worse than R-ODMRP, as Flooding does not consider QoS routing. However, R-ODMRP-PBS, which adopts priority based scheduling, has 2% improvement than R-ODMRP, as it can mitigate congestion. After all, the lost data can be resumed from neighbors but the control packets can not be recovered.



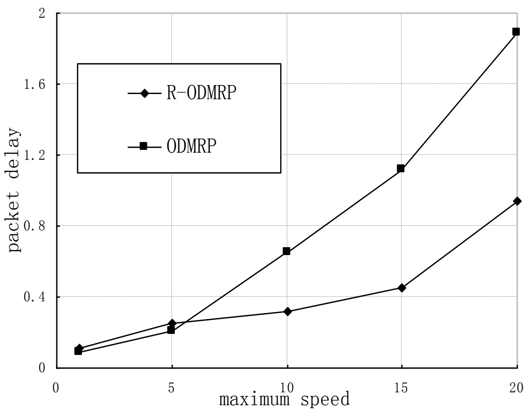


Figure 6(d). Comparisons of delivery delay

(2) Control overhead

Control overhead is evaluated through the ratio of the amount of the control packets and the amount of all packets. We consider a network which has 60 mobile nodes and compare the relationship between multicast load and overhead by changing the load in Fig. 6(b).

Then the load is deployed with 10 packets per second, we can observe how the overhead changes with different numbers of the mobile nodes in Fig. 6(c).

In Fig. 6(b), the control overhead of R-ODMRP is bigger than that of ODMRP when the load is low. As R-ODMRP needs to set up cluster based mesh and key exchanging, its overhead increases with the load and gets heavier at first. After 0.38, the overhead in R-ODMRP is influenced very little and nearly irrelative to the load. However, the overhead depends on the load especially when packet is blocked or lost. When the amount of the mobile nodes is small in Fig. 6(c), the change of the control overhead is similar to Fig. 6(b). It is intuitive that control overheads of the two protocols increase with the nodes number, as the more nodes, the more overhead. In comparison, R-ODMRP costs less than ODMRP does, because QoS-aware link selection and priority based scheduling can reduce unnecessary packets loss and congestion.

(3) Average delivery delay

It is the average time interval from the time packet sent to the time packet received. We set 60 mobile nodes, the multicast source sends 10 packets per second. To observe the average delivery delay, we change the nodes' maximum mobile speed, and the result is in Fig. 6(d). As network topology changes very slowly, neighbor nodes are almost fixed when the maximum speed is less than 10 m/s, the delivery delay is low and increases little. Once nodes move at speed varies from 10 to 20 m/s, rerouting leads to heavy control overhead and the delivery delay increases very fast. However, R-ODMRP employs cluster based forwarding and mobility prediction, its average delivery delay is lower than that of ODMRP.

VI. CONCLUSIONS

We have represented a reliable multicast routing protocol R-ODMRP, which is in character with reliability of cluster based mesh, safety of multicast delivery and QoS provision. R-ODMRP builds forwarding mesh for each multicast group, flexible soft-state maintenance, mobility prediction and QoS scheduling. Priority based packet scheduling can further to abate the control overhead and network congestion. Active network technique is introduced for Cluster-mesh-forward to distributedly perform active packet acknowledgment and lost packet recovery. Finally, the simulations results confirm effectiveness of our proposed protocol in efficient multicast delivery. However in the future, we will seek better multicast routing with new smart prediction scheme, and extend the R-ODMRP in severer network environments to analyze and verify its performance.

REFERENCES

[1] G. Krishna, "Routing protocols in mobile ad-hoc networks," pp. 1-30, 2006. http://www.cs.umu.se/education/examina/Rapporter/KrishnaGorantala.pdf

[2] L. Sung-Ju, S. William, G. Mario, "On-demand multicast routing protocol in multihop wireless mobile networks," *Mobile Networks and Applications*, 2001.

[3] S. J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia, "A performance comparison study of ad hoc wireless multicast protocols," *Proceedings of the IEEE INFOCOM'00*, 2000.

[4] P. Madhan, J. James, K. Murugan, V. Ramachandran, "A Comparative and Performance Study of On Demand Multicast Routing Protocols for Ad Hoc Networks," *9th International Conference on High Performance Computing (HiPC)*, 2002.

[5] V. Kumar, O. Katia and T. Gene, "Exploring mesh- and tree based multicast routing protocols for MANETs," *IEEE Transactions on Mobile Computing*, vol. 5, pp. 28–42, 2006.

[6] E. Royer, C. E. Perkins, "Multicast operations of the ad-hoc on-demand distance vector routing protocol," *Proceedings of ACM/IEEE MOBICOM'99*, 1999.

[7] Z. Yao, X. Leiming, S. Meilin, "On-demand multicast routing protocol with multipoint relay (ODMRP-MPR) in mobile ad-hoc network," *International Conference on Communication Technology Proceedings*, vol. 2, pp. 1295–1300, 2003.

[8] S. Chien-Chung, R. Sundaram, "Protocol-independent multicast packet delivery improvement service for mobile Ad hoc networks," *Ad Hoc Networks*, vol. 5, pp. 210–227, 2007.

[9] M. Hasnaa, and L. Houda, "A multicast on-demand mesh-based routing protocol in multihop mobile wireless networks," *IEEE 58th Vehicular Technology Conference*, vol. 4, pp. 2192–2196, 2003.

[10] T. Mukherjee, G. Sridharan, S. K. S. Gupta, "Energy-aware self stabilization in mobile ad hoc networks: A multicasting case study," *IEEE International Parallel & Distributed Processing Symposium (IPDPS)*, 2007.

[11] D. Koutsonikolas, Y. Charlie Hu, "Exploring the design space of reliable multicast protocols for wireless mesh networks," *Ad Hoc Networks*, vol. 7, pp. 932–954, 2009.

[12] C. Shaobin, Y. NianMin, W. Nianbin, Y. Wenbin, G. Guochang, "Multipath passive data acknowledgement on-demand multicast protocol," *Computer Communications*, vol. 29, pp. 2074–2083, 2006.

[13] V. Ravindra, J. J. Garcia-Luna-Aceves, O. Katia, "An adaptive redundancy protocol for mesh based multicasting," *Computer Communications*, vol. 30, pp. 1015–1028, 2007.

[14] P. Dhammika, K. Minseok, "RODMRP: Resilient on-demand multicast routing protocol," *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW)*, vol. 2, pp. 85–92, 2007.

[15] Nita-Rotaru, "BSMR: Byzantine-Resilient secure multicast routing in multi-hop wireless networks," *IEEE Transactions on Mobile Computing*, 2008.

[16] L. Jorg, D. Guangyu, "An overlay approach to data security in ad-hoc networks," *Ad Hoc Networks*, vol. 5, pp. 1055–1072, 2007.

[17] Y. Soon, P. Joon-Sang, and G. Mario, "E-ODMRP: Enhanced ODMRP with motion adaptive refresh," *Journal Parallel Distribution Computering*, vol. 68, pp. 1044–1053, 2008.

[18] L. Layuan, L. Chunlin, "A QoS multicast routing protocol for clustering mobile ad hoc networks," *Computer Communications*, vol. 30, pp. 1641–1654, 2007.

[19] M. Masoudifar, “A review and performance comparison of QoS multicast routing protocols for MANETs,” *Ad Hoc Networks*, vol. 7, pp. 1150–1155, 2009.
[20] D. Promkotwong, O. Sornil, “A mesh-based QoS aware multicast routing protocol,” *8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, vol. 3, pp. 1046–1051, 2007.
[21] C. Ching-Chuan, G. Mario and Z. Lixia, “Forwarding group multicast protocol (FGMP) for multihop, mobile wireless networks,” *Cluster Computing*, vol. 1, pp. 187–196, 1998.
[22] R. Akbani, T. Korkmaz, G. V. S. Raju, “HEAP: A packet authentication scheme for mobile ad hoc networks,” *Ad Hoc Networks*, vol. 6, pp. 1134–1150, 2008.

Zhiming Xu, born in Anhui Province in1971, received his B.S. and M.S. degrees from University of Science and Technology of China and Academy of Equipment Command & Technology in 1994 and 2005 respectively. Currently, he is a Graduate Research Assistant in Department of Space Engineering, Academy of Opto-electronics, Chinese Academy of Sciences, pursuing his Ph.D. degree under the supervision of Prof. Yu Wang. His current interests include communication architecture, cognitive radio networks, wireless sensor and actor networks and mobile ad hoc networks.

Yu Wang, born in Shanghai City in1963, received his B.S. M.S. and Ph.D. degrees in Department of Engineering Physics from Tsinghua University, China, in 1985, 1987 and 1991 respectively. His current interests include integrated electronic technologies for aircrafts, wireless communication, materials engineering.

He started participating in the overall program feasibility study of the data store-and-forward communication of small satellites, Chinese Academy of Sciences (CAS) from 1997, and presided over the completion of the overall satellite design. He also masterminded over major projects commissioned by CAS, such as the inter-satellite laser communications, space information networks, satellite autonomous operations, spatial information access and payload integration of remote sensing information etc. He has taken part in directional research project, CAS, "the key to lunar exploration science and technology research", and presided over payload technology system configuration program of the lunar exploration satellite.

Prof. Wang is vice-president of Academy of Opto-electronics, and deputy director of the Small Satellite Projects Center, CAS.

Jingguo Zhu, born in Hunan Province in1977, received his B.S. and M.S. degrees from Northwestern Polytechnical University and Centre for Space Science & Applied Research Chinese Academy of Sciences in 1999 and 2006 respectively. He is currently a Graduate Research Assistant in Department of Space Engineering and pursuing his Ph.D. degree at Academy of Opto-electronics, Chinese Academy of Sciences under the guidance of Prof. Yu Wang. His current interests include UWB communication, ad hoc networks and space engineering.