A Reliable and Hybrid Multi-path Routing Protocol for Multi-Interface Tactical Ad Hoc Networks

Sung-Won Lee, Ji Yong Choi, Keun Woo Lim, Young-Bae Ko, and Byeong-Hee Roh
Department of Computer Engineering, Graduate School of Ajou University
Suwon, Republic of Korea
Email : {sungwon, gchoi, kwlim27}@uns.ajou.ac.kr, {youngko, bhroh}@ajou.ac.kr

Abstract— **Reliable communication in the tactical area networks is critical because successful exchange of tactical information plays a vital role in achievement of military missions. However, this is an extremely challenging task due to several detrimental factors, such as low signal strength, interference and jamming. To increase communication reliability in tactical ad hoc networks, a robust and adaptive routing protocol can be a benefactor. To support this feature, efficient proactive multi-path discovery is desirable for the design of a routing protocol. We describe the shortcomings of such protocols in multi-interface multi-channel environment and present a solution for its effective utilization. In this paper we propose a Reliable and Hybrid Multi-path Routing protocol for tactical ad hoc networks which proactively discovers multiple routes toward every node in the initial phase, taking the link quality and channel diversity into consideration. In addition, we propose a fast error recovery scheme to cope with the potential route failures caused due to node destruction or jamming by enemy. The performance of the proposed scheme is evaluated with the OPNET simulator and shows good performance in packet delivery ratio and control message overhead.**

Keywords-component; Tactical Ad Hoc Networks, Multi-channel Multi-interface, Multi-path Routing, reliability, robustness, multiple gateway, anti-jamming

I. Introduction

The recent trend in the area of mobile ad hoc networks (MANETs) is focused on the development of self-organizing, self-maintaining, and self-healing networks. These network properties increase practicality and reality to future MANETs, especially in the battlefield scenarios where fixed central base stations can be unavailable. Thus, the study of the tactical MANET environments required to operate even in the most extreme conditions has been a popular topic of interest to the researchers. One of the prominent issues actively discussed is the reliable communication in mission-critical applications and its maintenance. This can be an extremely challenging task due to newly introduced problems in this unique environment, which are the frequent link failure by node destruction and/or obstacles and the radio jamming. To solve these problems, many different approaches in various layers of the network can be suggested, such as TCP[1](transport layer), route error recovery[2] (network layer), dynamic resource allocation[3](MAC layer), and various modulation methods [4](PHY layer). In this paper, our focus will be designing reliable routing protocol providing robust and efficient route management for achieving reliable communication in tactical MANETs.

Routing protocols discover and maintain one or multiple multi-hop routes between the source node and the destination node. These routing protocols can be classified into reactive and proactive categories. Depending on the network environment and situation, each one has its own advantages and disadvantages. Reactive types represented by schemes like AODV [5] and DSR [6], initiate the creation of a route when there is a request of data transmission from the application layer. Since optimal routes are created 'on-demand' while a request for data transmission is made, the protocol can be resilient to mobility and link dynamics during the data transmission. On the other hand, proactive routing protocols such as DSDV [7] and OLSR [8] increase reliability by periodically updating routes in the entire network regardless of when the data transmission is requested. Thus, they minimize the data transmission delay to discover the route by benefiting from its proactive properties.

However, these protocols also have their problems. For example, on-demand routing protocols induce additional end-to-end delay in data transmission from its reactive features. For a tactical environment where reliability and real-time data service is essential, it may not be suitable. Proactive routing protocols on the other hand might have excessive control message transmission due to node mobility and link errors. Since both downsides cannot be solved by the selection of either protocol, different approaches are needed to alleviate these problems. Among such approaches, a hybrid routing protocol can benefit from the advantages of the two routing types, while alleviating the disadvantages. By fusing the characteristics of on-demand and proactive routing, hybrid routing designs can not only reduce data transmission delay and control message overhead, but also be more resilient to node mobility and errors.

In order to enhance reliability, multi-path routing protocols can be utilized. A single path routing can be easily broken by node mobility or unpredictable link conditions. Such situation causes transmission failures and delay in the network, which renders the protocol unreliable. To overcome the limitation of a single path, many methods that discover multiple paths between the source and destination node have been suggested. Multipath routing protocols can easily recover path failure by utilizing alternative routes without any delay to re-discover the

"This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency" (NIPA-2010-(C1090-1021-0011)) and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0016189)

route, while providing benefits such as fault tolerance, load balancing, and bandwidth aggregation [9], etc.

The performance of an ideal hybrid (proactive and reactive), multi-path routing protocol can be complemented in the *multi-interface multi-channel* (MIMC) environment. In this environment, channel contention delay can be reduced and more bandwidth can be made available to improve reliability of the network. A reliable routing protocol that can support all the features mentioned above can be resilient to jamming and interference, and increase performances in reliability, end-to-end delay, and error treatment. This would indeed be an ideal protocol for tactical MANETs.

In this paper, we propose the "Reliable and Hybrid Multi-path Routing (RHMR)" which considers the characteristics of tactical environment and implements all the properties explained above. Before going to the specific details of the protocol, we will discuss the related works in Section 2. In Section 3, we present our proposed multipath routing protocol for multi-interface multi-channel tactical MANETs. The performance evaluation is discussed in Section 4. We conclude our paper and discuss the potential future works in Section 5.

II. Related Works

How to discover and select multiple routes in a network is one of the fundamental issues in multipath routing. For this purpose, two concepts are suggested; node-disjoint and link-disjoint [9]. In node-disjointed paths, multiple routes are created with an assurance that no common node can exist between them. In the link-disjointed paths, common nodes may exist between several routes, but links between two nodes do not overlap. Existing route discovery mechanisms attempt to discover a maximum number of node-disjointed or link-disjointed paths from the source to the destination. Then, the best route among them is selected using specific metrics/rules. If a link failure occurs breaking a primary routing path, a best route among the alternatives shall be selected to continue the communication.

Numerous multipath routing protocols have been proposed based on the popular reactive routing protocols, such as DSR and AODV. MP-DSR [10] was designed with consideration of Quality-of-Service based on the DSR. It tries to achieve high end-to-end reliability by determining the number of paths enough to support minimum reliability requirement. Split multipath touting (SMR) [11] is also based on the DSR and is designed to concurrently utilize multiple paths by splitting multiple packets across multiple paths. If any route fails, every entry in the routing table of the source which has common intermediate nodes is removed. After this process, the source checks whether both routes toward the destination are broken and if so, a new route discovery will be initiated for less control overhead. Since both are based on the DSR protocol, they have an excessive packet overhead because routing path are included in the header of every data packet. AODVM [2] is a multipath enhancement over the AODV that can discover multiple node-disjoint paths. Here, the intermediate nodes forward and record all duplicated RREQ packets in the RREQ table. The destination node sends an RREP message whenever it receives an RREQ. Intermediate nodes then forward RREP message to the neighbor node with the shortest path to the source in the RREQ table, and deletes the entry of the neighbor from the RREQ table to ensure node-disjoint properties. If the intermediate node cannot find any neighbor in the RREQ table, the node generates a route discovery error message (RDER) and sends it to the previous node that sent the RREP. After receiving a RDER message, the node in the previous hop forwards the RREP message to another neighbor. In the end, Route Request Confirmation Message (RRCM) is sent by the source node to the destination. AOMDV [12] is another design over the AODV to provide multiple paths with loop-free and link-disjoint properties.

Recently, MP-OLSR [13], one of proactive mechanism for multipath routing, was proposed over the OLSR protocol. Every node periodically broadcasts its topology information and receives the information of the entire network. Then, the node uses the *Multi-path Dijkstra* algorithm to find the multiple paths with node-disjoint or path-disjoint properties based on the entire topology information. The source routes discovered is then inserted in the data packet header, which is inspected by each intermediate hop along the path during the transmission. If a link or node failure occurs, the node detecting the failure re-computes the alternative path based on the topology information and then forwards the packet through the new route.

As described before, hybrid multipath routing protocols can alleviate some of the problems that these works may have. Works such as [14][15] deploys both routing methods in a hybrid multi-tier mesh architecture. They utilize one of proactive routing protocol for higher tier and one of reactive routing protocol for lower tier. However, due to the difference in the network environment, we can consider these works as out of scope. [16] provides a hybrid routing mechanism based on the DSR protocol. It uses a periodic maintenance message to support proactive routing, as well as allows reactive DSR routing when all the links from the source to the destination is broken. Maintenance of the links are only given to the current active paths to reduce overhead. However, this kind of approach may not be appropriate in the tactical networks where link quality can change frequently, and the maintained links may become congested or jammed over time.

Most of these previous works have been designed for the single interface single channel environment. Therefore, problems arise when they are deployed in the MIMC environment. In this environment, the existing multipath routing protocols underplay the advantages gained from the channel diversity and provide poor scalability [17]. Also, a new type of routing loop named as a *ping-pong problem* might occur since the protocols are only focused on optimizing the link and channel disjoint properties. Therefore, additional considerations are required to efficiently discover and maintain multiple paths in MANETs with MIMC.

III. Reliable Hybrid Multi-path Routing

In this section, we make some assumptions about the tactical networks and its environment, and then propose a suitable novel scheme. Terminals in tactical mobile ad hoc networks have longer transmission range than traditional

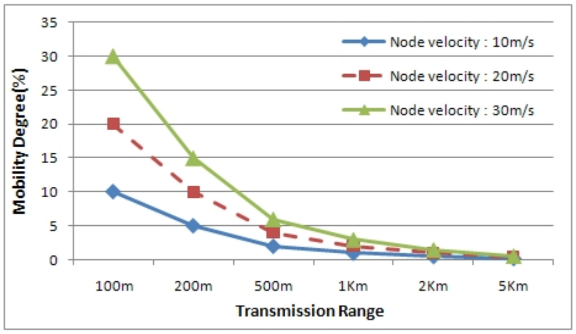


Fig. 1 Mobility Degree Analysis

Type	Flags	RREQ ID	Ori. IP	Ori. Seq.	Dst. IP	Dst. Seq.	Hop Count

(a) Structure of RREQ message

Type	Src. IP	Dst. IP	Seq. Num	Hop Count	Prev. Ch	CTC	Accumulative LQ

(b) Structure of the PRDM/ORRM

Fig. 2 Structure of the Control Messages

Destination IP
Sequence Number
Hop Count
Next Hop IP
Expiration_timeout

(a) Route Entry for AODV

Destination IP		
Sequence Number		
Route List		
Next Hop IP	Next Hop Channel	
Master Route Flag	Valid Flag	CTC
Hop Count	Accumulative LQ	

(b) Route Entry for RHMR

Fig. 3 The entry structure of the routing table

MANETs. Thus, they have lesser impact of mobility on the network. We define the *mobility degree* as the ratio of the node velocity over the transmission range, as shown in Fig. 1. It represents the maximum probability of a node to move away from the transmission range of its neighbor after 1 second. A result shows that the mobility degree in the tactical network with long transmission range [18] has lower mobility degree than the commercial vehicular networks [19]. Therefore, the multipath routing protocols with the proactive approach can be suitable due to less dynamicity in mobility in tactical environments. However, there are still some impediments against reliable communication, such as unexpected node failure, destruction of nodes and jamming attacks. To alleviate these problems, the proposed Reliable and Hybrid Multi-path Routing (RHMR) protocol provides proactive-like routing while utilizing the route discovery and maintenance mechanism of the reactive routing protocols. Also, RHMR considers the link quality and the MIMC environment. In this paper, the channel assignment mechanism for MIMC environment is out of scope and we assume the *identical channel assignment* [20] in which the channel assignment of each node is the same per each interface (i.e., NIC-1 is assigned with the first predefined channel, NIC-2 is assigned with the second predefined channel, and so on).

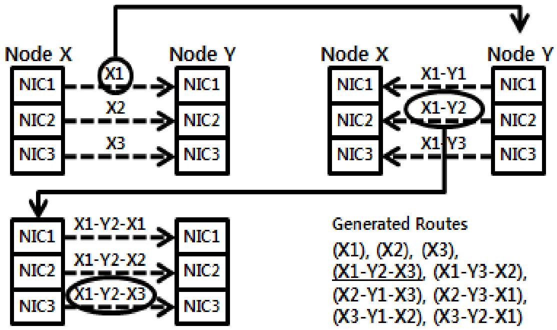
A. *Message and Routing Table Structures*

There are three kinds of control messages used in RHMR; HELLO message, periodic route discovery message (PRDM), and on-demand route recovery message (ORRM). All of the control messages are fundamentally based on the HELLO and RREQ message used in the AODV protocol. HELLO message is utilized to estimate the link quality and detect link failures. The PRDM and the ORRM are modified versions of the RREQ message as shown in Fig. 2 and both can be classified by their type fields. The PRDM is periodically generated and flooded into the whole network to provide proactive route discovery and maintenance. On the other hand, ORRM is flooded to the whole network to provide reactive route discovery and maintenance when all multi-hop paths to the destination is broken. The link quality (LQ) field contains the accumulative value of the link quality of each hop throughout the route. The channel trigger count (CTC) field contains the event count of the change of channels between the channels of current hop and the previous hop. The channel information where previous hop received the packet can be gotten from the previous channel (PC) field. For example, if the channel sequence of PRDM or ORRM passed in the network is 1-2-3-2, then the value of the CTC field will be 3 because the change in the channel has been triggered 3 times. The structure of the routing table is designed to support multi-path routes with the consideration for MIMC environment and link quality as shown in Fig 3. The RHMR utilizes the channel index as well as the address of previous hop to classify a route that includes a link with different channel from the same neighbor as the different route. The fields for each route quality acquired from the PRDM or ORRM are used for the selection of the master route by setting the master route flag.

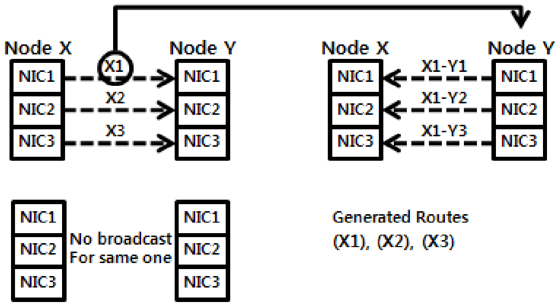
B. *Route Discovery*

The proposed RHMR protocol updates the routing table with multiple routes toward every node in the network and selects the best route among them. This route will be defined as the *master route*. In the traditional proactive routing protocols, the exchanging of topology information among every node is essential for discovering and maintaining routes in the whole network. However, to validate and update the routes in a mobile network, the interval of the control packet exchange needs to be short, which consequently results in waste of network resources. On the other hand, the proposed scheme proactively discovers multiple routes through PRDM flooding with a period of long time intervals. The interval can be dynamically reconfigured depending on the node mobility or the link quality. In addition, the RHMR will send ORRM to rediscover the routes toward the destination only when no route exists in the routing table.

For proactive route discovery and maintenance, the nodes periodically flood the PRDM so that the other nodes can create multiple paths toward the source node. In detail, a node sends the PRDM after initializing the fields with zero such as hop count, previous channel index, CTC, and accumulative LQ. The nodes receiving the PRDM identify the source address, previous hop address and receiving channel index and then checks whether the entry related to the route to the source node through previous link exists in the routing table. If no entry exists, the node creates a new entry and fills the fields of the route entry from the PRDM. If the entry exists, the node compares the sequence number of PRDM with the recorded sequence number in the entry and updates the route information with the latest information. Then, the RHMR compares the



(a) Ping-pong Problem in MIMC



(b) Proposed Scheme

Fig. 4 Forwarding Mechanism

route quality of existing master route in the routing table with the newly updated route and marks the route with better quality as the master route.

In the case of link-disjointed forwarding in the previous multipath routing protocols, a *ping-pong problem* may occur in MIMC environments due to this mechanism, as shown in Fig. 4(a). The node X receiving the first RREQ broadcasts the RREQ into all interfaces and the Node Y receiving the RREQ from Node X through channel 1, presented by X1 in Fig. 4(a) also performs same procedure. Then, node X may receive the same RREQ from interface 2 and broadcast the RREQ because the RREQ is received from a different interface, considering the link-disjoint properties. Consequently, this may cause broadcast storming of the duplicated RREQ and generate 6 routes with unnecessarily longer hop count. On the contrary, the node disjointed forwarding avoids this by only forwarding the first received RREQ message regardless of the channels. However, this may result in limiting the benefits that can be gained from multi-channel multi-interface environments. To avoid these problems, the RHMR approaches this problem via the concept of node-channel-disjoint as shown in Fig. 4(b), where the forwarding of PRDM is only progressed if the sequence number is new or if there is no entry in the routing table which has the route with the previous hop and the channel index toward the source node. In other cases, the node will just update the route information toward the source node without forwarding the PRDM. When the node forwards the PRDM, the node increases the hop count, adds the link quality of previous hop in the value of accumulative link quality field. Then it will update the value of channel trigger count field by incrementing the value, only if the current value of previous channel index is different compared to the receiving channel index, and updates the receiving channel index in the previous channel field. To ensure a loop-free master route, the hop count

Table 1. Simulation Parameters

Environment Parameter	Value
Medium Access Control Protocol	IEEE 802.11a
Area Size of Environment	12.5Km×12.5Km
Number of nodes (N)	10, 20
Number of Traffic (T)	1, 2, 5, 10, 15, 20
Node Velocity (V)	0, 10, 20, 30m/s
Interval of PRDM	50 second
Node transmission range	5Km [18]
Jamming range	1Km
Mobility Model	Random Waypoint
Simulation Time	300 seconds

of a route will be the most important parameter for comparison of each route. If the hop count of several routes is equal, the accumulative link quality and channel trigger count will be considered respectively. The priority among the metrics selects the route that has fewer hop count and less accumulative link quality as the master route.

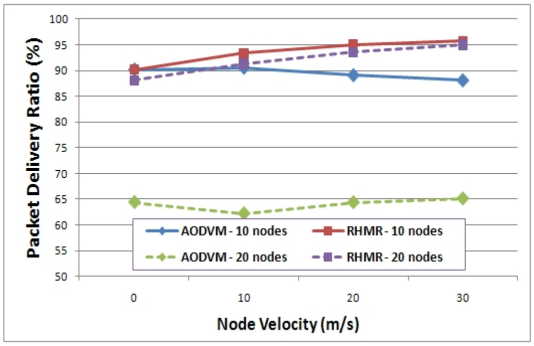
C. *Route Maintenance*

The route discovery of RHMR passively discovers and updates the multiple routes with relatively small control overhead. However, there are still several factors that prevent effective maintenance of the multiple routes, such as node sabotage, mobility, and radio jamming. These disturbances may severely affect the quality of the discovered routes. To cope with these external problems, a reactive method of route maintenance is required. When the master route is broken in RHMR, the node selects the second highest route as the master route, and the entry of previous master route is removed from the routing table. If more link breaks occur, there may be an occasion where no route to the destination may be remaining due to removal of all the entries in the routing table. In this case, the proposed RHMR scheme utilizes the reactive route discovery and recovers by utilizing the ORRM as well as the passive exchanges of PRDM. The node sends and floods the ORRM when the node has no more routes to the desired destination. The forwarding mechanism for route update and forwarding decision in the intermediate node is identical to the processing of PRDM. The destination node receiving ORRM immediately floods the PRDM in the whole network. All the nodes will receive both control messages and update multiple routes toward the source and the destination. Therefore, multiple routes between two nodes can be quickly rediscovered in every node while preventing route loops that may occur from local rediscovery.

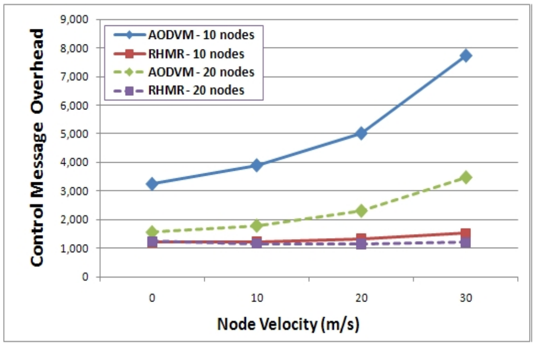
IV. Simulation and Results

A. *Simulation Environment*

Using OPNET simulator [21], we compare the performance of the proposed RHMR and AODVM because ADOVM provides robust route recovery. We use two evaluation metrics: *packet delivery ratio and control message overhead*. The packet delivery ratio represents the count of successful data reception compared to the total number of generated data. The control message overhead is defined by the average number of

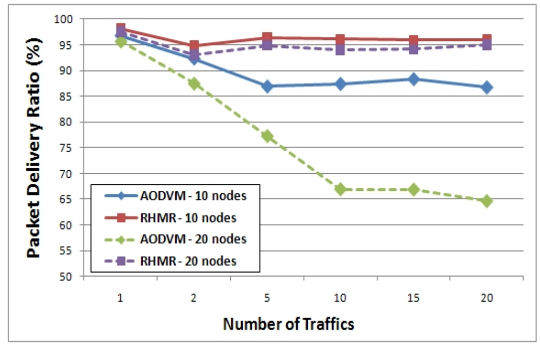


(a) Packet Delivery Ratio (%)

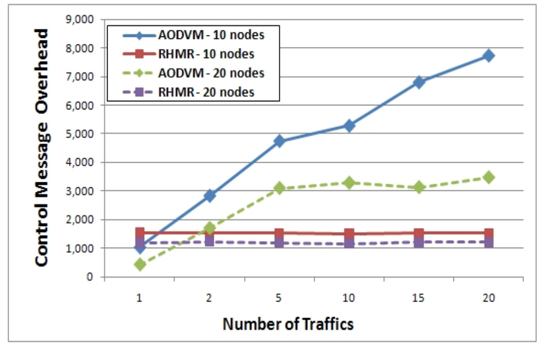


(b) Control Message Overhead

Fig. 5 Simulation Results with various Node Velocity (T=20)



(a) Packet Delivery Ratio (%)



(b) Control Message Overhead

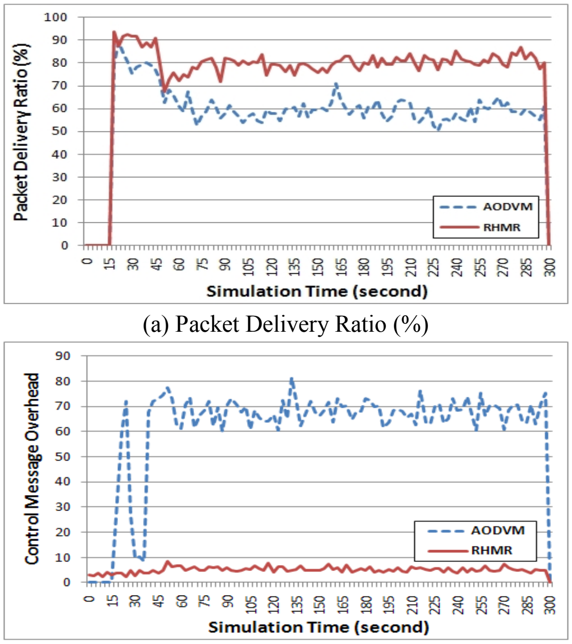
Fig. 6 Simulation Results with various number of traffics (M=30)

control messages generated and flooded per node during the simulation. A wide variety of system parameters is used for evaluation in the tactical MANET. We consider the application of tactical MANETs in the size of a brigade and its backbone networks made up of vehicles. The detailed network parameters are as shown in Table 1. In our simulation the node has three IEEE 802.11a interfaces with orthogonal channels in each interface, such as channel 1, 7, and 13. The transmission power is enlarged in which the delivery ratio of control messages is 98% and the delivery ratio of data packets with 1024 byte payload is about 70%. The data traffic generates a data packet with the payload size of 1024 bytes at every second after 20 seconds have elapsed in the simulation and the amount of data traffic will be various.

B. *Simulation Results*

Two types of simulations were conducted, one case where there are no jamming and the other case where some nodes may suffer from radio jamming. The PRDM interval of 50 seconds has been configured for the performance comparison between the AODVM and the proposed RHMR. First, we compare the simulation result in the no jamming scenarios as shown in Fig. 5 and Fig. 6. Fig. 5 shows the performances of both protocols according to the node velocity (m/s) with 20 data flows from random sources. In Fig 5 (a), AODVM has the best packet delivery ratio in static scenarios when the number of nodes is 10. However, when the number of nodes is 20, AODVM shows the worst packet delivery ratio. The reason for this is due to the fact that RREQ/RREP exchange creates routes by considering only the minimal hop count. This results into having poor link quality because longer distance hops are created. For this reason, probability of data collision and rate of bit error increases. Furthermore, the following RERR flooding also adds the probability of data collision. The number of generated control messages per node in 20 nodes of AODVM is about half than the number when 10 nodes are deployed, as shown in Fig. 5 (b). However, the amount of received control message per node is duplicated due to RERR flooding. On the contrary, the RHMR utilizes the link quality and channel diversity as the metric to avoid links with data collision. Also it can utilize ORRM-PRDM exchange rather than RERR flooding for route recovery. Therefore, the proposed scheme shows good performance even when velocity is high. Fig. 6 shows the performances according to the number of traffics with node velocity configured to 30 m/s. When only a single traffic is configured, the AODVM with 10 nodes has similar control message overhead with RHMR while the latter having the least control message overhead when the number of nodes deployed is 20. The reason for this is because the AODVM discovers the node-disjointed routes restricting the number of multipath routes in the deployment of 10 nodes. Consequently, frequent RERR flooding and re-discovery is induced even though there is only a single data traffic. On the contrary, the RHMR discovers the multiple routes with the node-channel-disjointed to every node regardless of the number of traffics. As a result, the RHMR suffers less data collision that may be induced by the poor quality links and/or by flooding of control messages. Consequently, this keeps the overall performance from degrading regardless of the node velocity or number of traffics.

The performance comparison in jamming environment with 20 nodes without mobility is shown in Fig. 7. The jamming in all the channels starts from 50 seconds until the end of the simulation time. Packet delivery ratio and the control message overhead are presented with respect to the simulation time. The packet delivery ratio of AODVM is dramatically decreased



(a) Packet Delivery Ratio (%)

(b) Control Message Overhead

Fig. 7 Simulation Results with Jamming (N=20, V=0m/s)

from 83.75% to 55% directly after jamming, as shown in Fig. 7 (a). The performance is somewhat retained, at the cost of higher control message as shown in Fig. 7 (b). This tells us that AODVM tries to recover the routes against jamming, but its metric cannot reflect the poor link quality induced from jamming and interference. As a result, the discovered route cannot support efficient data transmission because collision or congestion in that link has dramatically increased from jamming. On the other hand, the proposed scheme shows less declination than that of AODVM as the packet delivery ratio is reduced from 88.75% to 72.5%. Paths are re-established based on the link quality and become more stabilized as the time flows. The RHMR keeps similar level of control overhead and average delay because the node with route failure floods the PRDM into the whole network using only a single ORRM. In this way, other nodes can conveniently update the route information without additional ORRM-PRDM flooding. On the other hand, every node experiencing route failure in AODVM will individually start route recovery with RREQ-RREP exchange and lead to excessive control overhead. In overall, the simulation results in jamming environment show that the RHMR takes efficient approaches to soften jamming attacks to provide more robustness in supporting reliable communication with restricted overhead.

V. CONCLUSION

The multi-path routing is an effective method to support the reliable communication with alternative paths in tactical environments. In tactical environments, there are distinguishable features such as lower mobility by long transmission range and unexpected route/link failure by destruction or jamming. For application of these features in the multipath, we propose a Reliable and Hybrid Multi-path Routing (RHMR) protocol which provides a proactive-like routing with less end-to-end delay and less control overhead. Simulation results have shown advantages of the proposed scheme with higher packet delivery ratio and lower control message overhead. Our future works will be focused on the theoretical analysis and the adaptation of dynamic PRDM intervals to enhance the reliability and efficiency. In addition, we will research the extended algorithms for the load balancing and more efficient route maintenance.

REFERENCES

[1] Özgür B. Akan , Ian F. Akyildiz, “Event-to-sink reliable transport in wireless sensor networks”, IEEE/ACM Transactions on Networking (TON), vol.13 no.5, pp.1003-1016, October 2005

[2] Ye, Z., Krishnamurthy, S.V., Tripathi, S.K., “A Framework for Reliable Routing in Mobile Ad Hoc Networks”, IEEE INFOCOM 2003

[3] S. H. Ali, K. D. Lee and V. C. M. Leung, “Dynamic Resource Allocation in OFDMA Wireless Metropolitan Area Networks,” IEEE Wireless Communications Magazine, vol.14, no.1, pp. 6-13, Feb. 2007

[4] T.-S. Yang, A. Duel-Hallen, and H. Hallen, "Reliable Adaptive Modulation Aided by Observations of Another Fading Channel", IEEE transactions on communications, 2004, vol.52, no.4, pp.605-611

[5] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. "Ad hoc On-Demand Distance Vector (AODV) Routing Protocol". RFC 3561

[6] D.B. Johnson, D.A. Maltz and Y-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", RFC 4728

[7] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", ACM SIGCOMM’94

[8] T. Clausen and P. Jacquet. "Optimized Link State Routing (OLSR) Protocol". RFC 3626

[9] S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath Routing in Mobile Ad Hoc Networks: Issue and Challenges”, In Performance Tools and Applications to Networked Systems, volume 2965, LNCS, pp. 209-234

[10] R. Leung, J. Liu, E. Poon, A. L. C. Chan, and B. Li, "MP-DSR: a QoSaware multi-path dynamic source routing protocol for wireless ad-hoc networks," Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on, Tampa, FL 2001.

[11] S. J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," IEEE ICC 2001.

[12] M. K. Marina and S. R. Das, " On-demand Multi Path Distance Vector Routing in Ad Hoc Networks," IEEE ICNP 2001

[13] J. Yi, Cizeron, S. Hamma, and B. Parrein, “Simulation and Performance Analysis of MP-OLSR for Mobile Ad Hoc Networks”, IEEE WCNC 2008.

[14] M. Siddiqui, S. Amin, J. Kim, C. Hong, “Mhrp: A secure multi-path hybrid routing protocol for wireless mesh network”, IEEE MILCOM 2007

[15] J. Haas, “A new routing protocol for the reconfigurable wireless networks”, Proc. of IEEE 6th International Conference on Universal Personal Communications 97, pp. 562–566.

[16] R. Zheng, Y. Li, L. X. Guo, “A Hybrid Multi-Path Routing for Wireless Mesh Network Backbone”, IEEE WiCom 2008.

[17] W.-H. Tam and Y.-C. Tseng, "Joint Multi-Channel Link Layer and Multi-Path Routing Design for Wireless Mesh Networks", IEEE InfoCom '07

[18] L. Li and T. Kunz, “Efficient Mobile Networking for Tactical Radios”, IEEE Milcom 2009.

[19] H. Hartenstein, B. Bochow, A. Ebner, M. Lott, M. Radimirsch, D. Vollmer, "Position-aware ad hoc wireless networks for inter-vehicle communications: the Fleetnet project", ACM MobiHoc 2001

[20] A. Raniwala, K. Gopalan, T. Chiueh. "Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks", ACM Mobile Computing and Communications Review, 2004

[21] http://www.opnet.com/, version 14.5