An Inter-domain Route Maintenance Scheme Based on Autonomous Clustering for Heterogeneous Mobile Ad Hoc Networks

Keisei Okano, Tomoyuki Ohta, and Yoshiaki Kakuda
Graduate School of Information Sciences, Hiroshima City University
3-4-1 Ozukahigashi, Asaminami-ku, Hiroshima 731-3194, Japan
Email: {okano@nsw.info, ohta@, kakuda@}hiroshima-cu.ac.jp

Abstract—**Many types of mobile ad hoc networks such as vehicular ad hoc networks have been proposed for various application. In heterogeneous mobile ad hoc network environment that consists of many types of mobile ad hoc networks, each network uses a routing protocol suitable for the characteristics such as topology change frequency and data traffic. In such a network environment, nodes between different networks cannot communicate with each other because each network uses a different routing protocol. In this paper, we propose a new inter-domain routing protocol based on the autonomous clustering according to the network topology change in heterogeneous mobile ad hoc network environment and evaluate the effectiveness of the proposed scheme through simulation experiments.**

Keywords-Ad hoc network; Autonomous Clustering.

I. Introduction

There are many types of mobile ad hoc networks [1] such as vehicular ad hoc networks. Since the characteristics such as the topology change frequency and data traffic are different between networks, routing protocols that considered the characteristic of each network have been proposed for mobile ad hoc networks. Each network selects a suitable routing protocol from many routing protocols and uses it to enhance the network performance. As a result, in case that some mobile ad hoc networks exist in a region, it is possible that each network uses a different routing protocol. In such a heterogeneous mobile ad hoc network environment, there is no interoperability between networks and each network cannot communicate with each other so that each node cannot obtain much information and services even if much information and many services might exist in all networks. So far for inter-domain routing protocol in heterogeneous mobile ad hoc network environment, Cluster-based Inter-Domain Routing (CIDR)[2] and Inter-Domain Routing for MANETs (IDRM)[3] have been proposed. However, intra-routing protocol in each network is specified and it is difficult to select the routing protocol suitable for each network environment.

Therefore, this paper proposes an inter-domain routing protocol based on autonomous clustering to provide the communication between any two nodes in different networks for heterogeneous mobile ad hoc networks. In heterogeneous MANET environment, the network gateway nodes (shortly, NwGW nodes) are required to communicate between two different networks. In [4] and [5], we have proposed the two schemes to realize a new inter-domain routing protocol based on the autonomous clustering that we propose in this paper. In [4], we proposed the scheme to convert the control packet for providing the interoperability between two different network as ATR (Ad hoc Traversal Routing) and evaluate it in the environment where a specified number of nodes in the network is NwGW nodes. Next, in [5], we proposed the scheme to dynamically select the NwGW nodes between two different networks according to the network topology change. In this paper, we propose a route creation and maintenance scheme for the inter-domain routing protocol in heterogeneous MANET environment where the network topology change occurs frequently, and then evaluate it to show the effectiveness through simulation experiments.

The rest of the paper is organized as follows. In Section II, we describe requirements about our proposed scheme. In Section III, we introduce the proposed scheme itself. In Section IV, the experiments will be illustrated and the results will be discussed in the end.

II. Requirements

In order to implement the proposed scheme, the mechanisms of ATR [4] and autonomous clustering [6], [7] in each node are required as a common platform. Each node has the routing protocol specified by the network on the common platform. In the heterogeneous mobile ad hoc network environment where some networks exist, each network is divided into multiple clusters and the nodes in the cluster is managed by the autonomous clustering. In the proposed inter-domain routing protocol, each cluster in the networks autonomously and dynamically selects one or more NwGW nodes from the nodes in the cluster, and then the source and the destination node in different networks can communicate with each other through NwGW nodes. In this time, the nodes which become NwGW nodes can forward any packets to nodes of the different network by using the mechanism of ATR so that the interoperability between different networks can be provided.

ATR [4] is the scheme to provide the interoperability between different networks in the heterogeneous mobile ad hoc network environment. Both any routing protocol and ATR work on each node. Each node converts from control packets which are used as the routing protocol in the network to control packets of ATR format, and forwards them to the neighboring node with ATR in the different network. The node with ATR that received the control packets of ATR format converts from

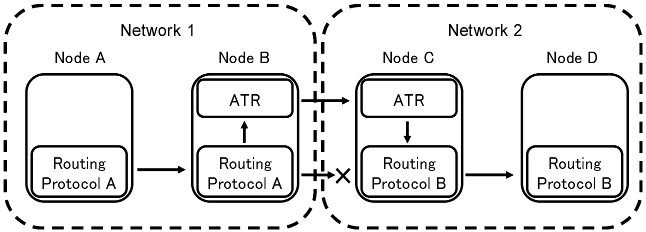

Figure 1: Behavior of ATR in heterogeneous network environment.

them to the control packets of a routing protocol used in the different network, and then forwards them in the different network. As a result, a node in a network can communicate with another node in a different network through nodes with ATR.

We explain ATR using an example as shown in Figure 1. Given that there are two networks, which are Network 1 and Network 2, and nodes A and B belong to Network 1 and nodes C and D belong to Network 2. When node A wants to communicate with node D, the route between nodes B and C cannot be created because the routing protocols are different. However, in this example, ATR works on nodes B and C so that nodes between Network 1 and Network 2 can communicate with each other through nodes B and C. Node B that receives a control packet of routing protocol A from node A converts from the control packet to a control packet of ATR, and then forwards it to node C. Node C that receives the control packet of ATR converts from the control packet to the corresponding control packet of routing protocol B, and then forwards it to node D. As a result, the route between nodes A and D can be created through nodes B and C.

A. Autonomous Clustering

Outline

Autonomous clustering [6], [7] is the scheme to divide the network into multiple clusters and manage nodes hierarchically. Each cluster consists of one cluster head, one or more gateways and cluster members. The cluster head manages nodes in each cluster and the cluster ID is assigned to the node ID of the cluster head. The gateway is neighbor to the nodes in the neighboring clusters. The packets are forwarded between clusters through gateways. In the autonomous clustering, the number of nodes in each cluster (that is, cluster size) is adjusted between the upper bound and lower bound given in advance.

Node State and State Transition

In mobile ad hoc network environment, nodes are always moving around the network so that the network topology is changed frequently. In the autonomous clustering, each node autonomously changes the state according to the situation of neighboring nodes to maintain the cluster. In the autonomous clustering, there are five states: CN, BN, BCN, NSN, and ON, and each node becomes one state of them and has a role in the cluster.

- CN (Control Node): This node works as a cluster head.
- BN (Border Node): This node works as a gateway.

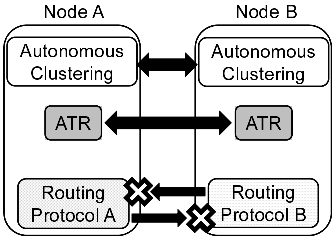

Figure 2: Protocol design of the proposed inter-domain routing.

- BCN (Border and Control Node): This node works as both a cluster head and gateway.
- NSN (Normal State Node): The node is a cluster member and does not work as a cluster head and gateway.
- ON (Orphan Node): This node does not belong to any clusters. In the initial state, a node becomes this state.

Cluster Configuration and Maintenance

The cluster head periodically broadcasts a control packet called MEP (MEmber Packet) within the cluster, and then cluster members that received the MEP sends MAP (Member Acknowledgment Packet) back to the cluster head. The cluster head can collect the information on cluster members and construct the cluster head-based tree in the cluster by these procedures.

The MEP includes the cluster ID and the node ID of the cluster head. The node that received MEPs stores the information and broadcasts it again. Each node receives MEPs from the neighboring node including the parent node and nodes of different clusters. Based on the received MEPs from the neighboring nodes, each node autonomously decides and changes its own state and cluster ID. For instance, if the cluster ID included in the received MEP is different from its own cluster ID, the node becomes gateway.

The nodes in the cluster that received the MEP sends a control packet MAP back to the cluster head as a reply. The MAP includes the cluster ID of the neighboring cluster, the node ID of gateways and the cluster ID of the neighboring cluster to which each gateway is neighbor, and the number of nodes in each neighboring cluster. The cluster head that receives MAPs from the cluster members manages the cluster by recognizing the number of nodes and the state of each node in the cluster as well as those in the neighboring clusters.

In order for the cluster head to maintain the number of nodes in the cluster between the upper bound and lower bound, the cluster head does the following procedures: it merges its own cluster with one of the neighboring clusters if the number of nodes is less than the lower bound and it divides the cluster into two clusters if the number of nodes is more than the upper bound.

III. An Inter-domain Routing based on Autonomous Clustering

A. Protocol Design

Figure 2 shows the protocol design of the proposed inter-domain routing protocol. In the proposed scheme, the autonomous clustering and ATR are required as a common

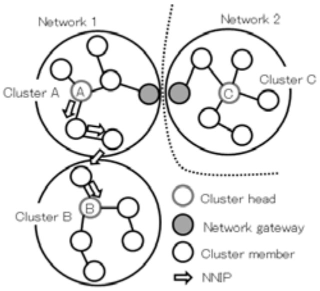

Figure 3: Connection status sharing among clusters.

platform in each node. The local routing protocol is a protocol to be used in each network.

In the proposed inter-domain routing, the communication between the source and the destination nodes in different networks can be provided with lower overhead and high data packet delivery ratio. In [5], we proposed the scheme to dynamically select the NwGW nodes between two different networks according to the network topology change.

B. Connection Status Sharing Mechanism

In heterogeneous MANET environment, since the route is created through NwGW nodes, the number of hops between the source and the destination nodes increases and the route break occurs more frequently. In the proposed inter-domain routing, when the route between the source and the destination nodes in different networks breaks, NwGW nodes try to repair the route. In order that NwGW nodes repair a route, each cluster heads share the connection status to the different network with neighboring clusters. The connection status to the different network consists of its own cluster ID, the network address of the neighboring network, and the number of hops to the cluster head of the neighboring cluster. Here, we explain how clusters share it with each other. In Section III-D, we describe the route repair mechanism based on the connection status.

After a cluster head sends a RNGP (Recommendation for Network Gateway node Packet), it periodically sends NNIP (Neighbor Network Information Packet) including its own connection status to the cluster heads of neighboring clusters. The cluster head that received NNIP from the neighboring clusters stores the connection status of the neighboring clusters.

We explain the the connection status sharing mechanism using Figure 3. As shown in Figure 3, given that there are clusters A and B in Network 1 and cluster C in Network 2. In this time, cluster head A recognizes the NwGW node (node E) that is neighbor to Network 2. Cluster head A adds (A, Network 2, 0) into NNIP, and then sends it to cluster head B. Cluster head B that received NNIP stores (A, Network 2, 4) into the neighboring cluster list. Here, the number of hops to the cluster head of the neighboring cluster contained in NNIP is changed from 0 to 4. This is because the hop count is incremented whenever the NNIP is forwarded at hop by hop based on the cluster head-based tree. Each cluster periodically exchanges the connection status with the neighboring clusters.

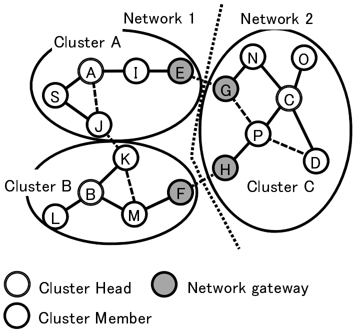

Figure 4: Network topology in heterogeneous MANETs.

C. Route Creation in Inter-Domain Routing

In heterogeneous MANETs, the route creation mechanisms in inter-domain routing are different according to the types of routing protocol in each network. In Figure 4, given that there are two networks in the field, and nodes S and D are a source node and a destination node. In this case, there are four cases, that is, (a) Networks 1 and 2 use reactive routing protocols, (b) Networks 1 and 2 use a reactive and a proactive routing protocol, (c) Networks 1 and 2 use a proactive and a reactive routing protocol, and (d) Networks 1 and 2 use proactive routing protocols.

(a) Networks 1 and 2 use reactive routing protocols

In this case, Network 1 to which the source node belongs and Network 2 to which the destination node belongs use a reactive routing protocol. The source node sends a route request message to the destination node by flooding. When NwGW nodes E and F in Network 1 receive the route request message, they convert it to the route request message of ATR and forward it to the neighboring NwGW nodes G and H. NwGW nodes G and H that received the route request message of ATR convert it to the route request message of the local routing protocol which is used in Network 2, and then forward it to nodes in Network 2. In case that the destination node D receives the route request message, it sends the route reply message toward the source node along the reverse route of the route request message.

(b) Networks 1 and 2 use a reactive and a proactive routing protocol

In this case, Network 1 to which the source node belongs uses a reactive routing protocol and Network 2 to which the destination node belongs uses a proactive routing protocol. The source node sends a route request message to the destination node by flooding. When NwGW nodes E and F in Network 1 receive the route request message, they convert it to the route request message of ATR and forward it to the neighboring NwGW nodes G and H. In case that NwGW nodes G and H that received the route request message of ATR have the route entry to the destination node, they send the route reply message to the source node.

(c) Networks 1 and 2 use a proactive and a reactive routing protocol

In this case, Network 1 to which the source node belongs uses a proactive routing protocol and Network 2 to which

ISBN: 978-1-61208-318-6

the destination node belongs uses a reactive routing protocol. In case that the local routing protocol is a proactive routing protocol, NwGW nodes inform the neighboring network information of the local routing protocol. When the source node has the entry to NwGW nodes E or F that is neighbor to Network to which the destination node belongs, the source node forwards data packets to the NwGW node. The NwGW node that received data packets forwards them to NwGW node G or H in the neighboring network. The NwGW node that received data packets from NwGW node of the neighboring network sends a route request message by flooding in the network as a source node. When the destination node receives the route request message, it sends the route reply message to the NwGW node which is set as the designated source node. After the NwGW receives the route reply message, it forwards data packets to the destination node along the route.

(d) Networks 1 and 2 use proactive routing protocols

In this case, Network 1 to which the source node belongs and Network 2 to which the destination node belongs use a proactive routing protocol. A NwGW node can obtain the routing tables in the network from the local routing protocol, and then exchanges it with the NwGW node of the neighboring network. As a result, each node can add the route entry to the NwGW node which is neighbor to each network in the routing table. The source node forwards data packets based on the routing table.

D. Route Maintenance in Inter-Domain Routing

The route between the source node and the destination node is broken due to node movement. In case that the both nodes belong to an identical network, the route is repaired based on the local routing protocol which is installed in the network. However, in heterogeneous MANETs, it is impossible to repair the route based on one routing protocol because the route between the source node and the destination node is not created by one routing protocol. Therefore, the route repair procedures are different according to the location where the link was broken. There are three types of procedures for the route repair. The procedures are that (a) the route is broken in the networks that the destination node belongs to, (b) the route is broken in the networks the source node belongs to, and (c) the route is broken between two NwGW nodes in different networks. We explain the route repair procedure based on Figure 4. As shown in Figure 4, given that the source and destination nodes are nodes S and D, and the route is S, A, I, E, G, P, and D. In addition, since the procedure of a proactive routing is different from that of a reactive routing, we explain two types of procedures of reactive and proactive routings as (R) and (P).

(a) Route is broken in the networks that the destination node belongs to

In this case, given that the link between nodes P and D on the route is broken in Figure 4.

(R): Node P can detect the link break to the downstream nodes because of the notification of MAC protocol. After that, node P sends a route error message to the upstream node along the reverse route. NwGW node (node G) that received the route error message tries to recreate a new route to the destination node (node D) based on the local routing protocol in Network 2. In case that a route is recreated, node G restarts to forward data packets. Otherwise, node G sends the route error to the upstream nodes in the different network.

(P): After NwGW node G recognizes the route break based on the local routing protocol, it sends a route error message to the source node if it does not have the alternative route. Then, the source node tries to recreate a route to the destination node.

(b) Route is broken in the networks the source node belongs to

In this case, a node that detected the link break sends a route error message to the source node, and then the source node tries to recreate a new route to the destination node.

(c) Route is broken between two adjacent NwGW nodes in different networks

NwGW node (node E) that detected the route break forwards data packets to Cluster head (node A) and sets the timer. In case that NwGW node (node E) receives data packets until the timer is expired, it forwards data packets to the cluster head. The cluster head that received data packets from NwGW node (node E) forwards them to the neighboring cluster that is neighbor to the network including the destination node. Here, the neighboring cluster with the lowest number of hops to cluster head is selected from the neighboring cluster list. The cluster head (node B) that received data packets from the neighboring cluster forwards them to NwGW node (node F) in the same cluster, and NwGW node (node F) forwards data packet to NwGW node (node H) and tries to recreate the route to the destination.

(R): : If NwGW node (node H) has a route entry to the destination node, it forwards data packets to the destination node. Otherwise, NwGW node (node H) sends a route request by flooding only in the network to recreate a route. Data packets are forwarded to the destination node along the route in case that the route is created, while it sends a route error message to the source node in case that the route is not created. In this case, the source node that received the route error message recreates the route.

(P): : If NwGW node (node H) has a route entry to the destination node, it forwards data packets to the destination node. Otherwise, it sends a route error message to the neighboring NwGW node (node F).

After the timer on NwGW node (node E) is expired, it sends a route error message to the source node, and then the source node sends a route request message by flooding to recreate a route. In this case, since NwGW node (node F) has created the route entry to the destination node, it immediately sends the route reply message back to the source node, resulting in reducing the number of control packets.

TABLE I: Simulation environment.

Simulator	QualNet ver.5.0 [8]
Simulation time [s]	300
Number of nodes	200
Number of neighboring nodes	8, 10, 12
Transmission range [m]	250
Node moving speed [m/s]	10, 20
Number of transmitted data packets	1000
Data packet size [byte]	512
Interval of sending data packets [s]	0.25
Number of pairs of source and destination nodes	10
Node mobility model	Random Waypoint Model
Maximum cluster size	50
Minimum cluster size	10
Interval of sending MEP [s]	2
MAC protocol	IEEE802.11b

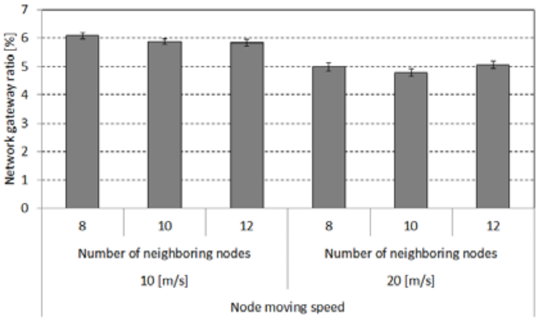

Figure 5: NwGW node ratio.

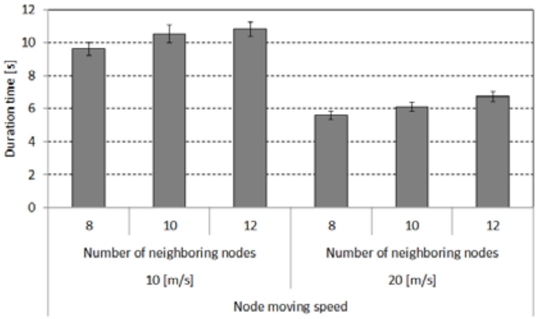

Figure 6: Duration time of two NwGW nodes.

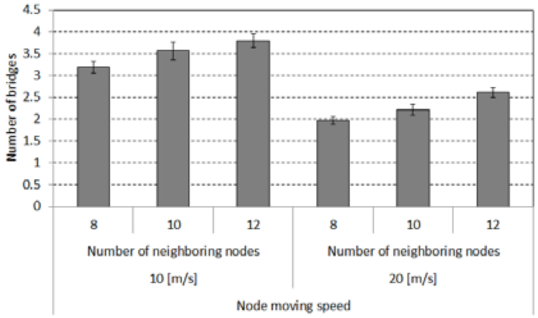

Figure 7: Number of bridges.

IV. Simulation Evaluation

A. Simulation Plan

Table I shows the simulation environment. In heterogeneous MANET environment, there are two networks, which are Network 1 and Network 2. Although both networks use AODV [9], in the simulation each routing protocol is handled as a distinct routing protocol and both networks cannot communicate with each other. In each pair of a source and a destination node (SD pair), the source and the destination node belong to Network 1 and Network 2, respectively. In addition, each cluster selects one NwGW nodes for each network by the dynamic network gateway selection scheme.

Evaluation criteria are the NwGW node ratio, the duration time of two NwGW nodes, and the number of bridges. The duration time of two NwGW nodes is the time when two NwGW nodes in different networks are continuously neighboring. The number of bridges is the number of pairs of two network NwGW nodes between networks. In addition, in order to show the effectiveness of the route maintenance, we show the results of the data packet delivery ratio and control overhead by comparing between w/ route repair and w/o route repair.

B. Simulation Results

NwGW node ratio

Figure 5 shows the NwGW node ratio. From Figure 5, it is confirmed that the NwGW ratio is almost the same regardless of the number of neighboring nodes.

Next, in case that the node moving speed is 20 m/s, the NwGW node ratio decreases in comparison with the node moving speed is 10 m/s. The NwGW nodes are selected from cluster members and notified to a selected cluster member based on MAPs which are sent by cluster members. However, there is the difference between the time when cluster members send MAPs to the cluster head and the time when the cluster head selects a NwGW node. Therefore, due to node movement, there is the possibility that the new selected NwGW move out from the clsuter. In this case, the NwGW node is not selected, and then another new NwGW node is selected next time. As a result, as the node moving speed becomes faster, the NwGW node ratio becomes lower.

Duration time of two NwGW nodes

Figure 6 shows the duration time of two NwGW nodes. In these experiments, we set at the smaller field size in order to increase the number of neighboring nodes. Therefore, two NwGW nodes in different networks are adjacent at the high possibility. In addition, as the node moving speed becomes faster, the relative speed of two NwGW nodes becomes faster and the duration time of two NwGW nodes becomes shorter.

Number of bridges

Figure 7 shows the number of bridges. As shown in Figure 7, the number of bridges increases as the number of neighboring nodes becomes more. However, in case that the node moving speed is 20 m/s, the number of bridges decreases because the number of NwGW nodes decreases as shown in Figure 5.

Data packet delivery ratio

Figure 8 shows the data packet delivery ratio. In all cases, the scheme w/ route repair has the higher data packet delivery ratio than the scheme w/o route repair. In case that the node moving speed is 20 m/s and the number of neighboring nodes

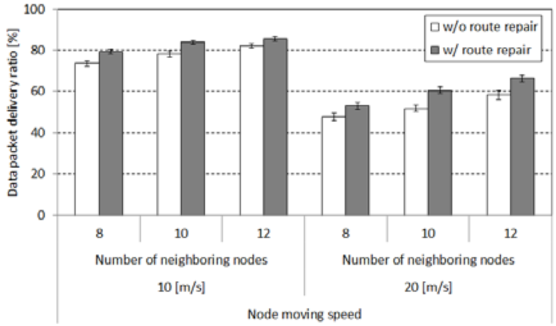

Figure 8: Data packet delivery ratio.

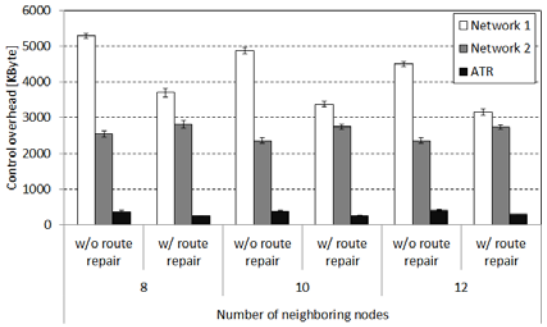

Figure 9: Total control overhead in case of node moving speed 20 m/s.

is 10, the scheme w/ route repair becomes 8.7% higher than the scheme w/o route repair. In this case, the route break occurs more frequently in comparison with the case of node moving speed 10 m/s. Therefore, as shown in Table II, the route repair is frequently invoked by not a source node but NwGW nodes.

On the other hand, in case that the node moving speed is 10 m/s and the number of neighboring nodes is 12, there is only 3.2% difference between the scheme w/ route repair and w/o route repair. Since the node density is high, the route repair is quickly invoked by the source node.

As a result, in case that the node moving speed is fast and the route breaks often occur, the proposed route maintenance scheme behaves efficiently and provides the high data packet delivery ratio.

Total control overhead

Figure 9 shows the total control overhead, which does not include the control overhead of the autonomous clustering. In cases of Network 1 and ATR, the control overhead of the scheme w/ route repair becomes 30% lower than that of the scheme w/o route repair. On the contrary, in case of Network 2, the control overhead of the scheme w/ route repair becomes 10% higher than that of the scheme w/o route repair. This is because in case of the scheme w/o route repair, when the route break occurs in Network 2 to which the destination node belongs, the source node sends a route request message by flooding in all network to recreate a route. On the contrary, in case of the scheme w/ route repair, when the route break occurs in Network 2, the NwGW node sends a route repair message by flooding only in Network 2 and the messages are not flooded in Network 1. However, if the NwGW cannot recreate a new route to the destination node in Network 2, the NwGW node sends a route error message to the source node, and then the source node tries to recreate a new route. In this case, a route request messages is flooded in all networks. Therefore, it is considered that the control overhead of the scheme w/ route repair increases in comparison with that of the scheme w/o route repair.

TABLE II: Number of route creations invoked by NwGW nodes

# of neighboring nodes	Moving speed [m/s]	# of route creation	Success	Failure
8	10	472	456	16
	20	588	563	25
10	10	444	437	7
	20	602	587	15
12	10	411	405	6
	20	592	582	10

V. Conclusion

This paper has proposed an inter-domain routing protocol based on autonomous clustering for heterogeneous MANETs and evaluated it through simulation experiments. From simulation experiments, it is confirmed that the route repair mechanism works more effective especially in case that the network topology change occurs more frequently. In the future work, we are planning to repair a route in a shorter time and become higher data packet delivery ratio with lower overhead.

Acknowledgments

This work was supported in part by JSPS KAKENHI (Grant Number 24700073 and 24300028), the Hiroshima City University under Grant for Special Academic Research, and MIC SCOPE (No.131408006).

References

[1] C.-K. Toh, “Ad Hoc Mobile Wireless Networks Protocols And Systems, ” Prentice Hall Inc., 2002.

[2] B. Zhou, Z Cao, and M Gerla, ”Cluster-based inter-domain routing (CIDR) protocol for MANETs,” Proc. 6th Int’l Conf. on Wireless On-Demand Network Systems and Services (WONS), pp.19-26, Feb. 2009.

[3] C.-K. Chau, J.Crowcroft, K.-W.Lee, and S.H.Y. Wong, ”Inter-domain routing for mobile ad hoc networks,” Proc. 3rd ACM Int’l Workshop on Mobility in the evolving internet architecture (MobiArch’08), pp.61-66, Aug. 2008.

[4] S.Fujiwara, T.Ohta, and Y.Kakuda, ”An inter-domain routing for heterogeneous mobile ad hoc networks using packet conversion and address sharing,” Proc. 32nd IEEE Int’l Conf. on Distributed Computing Systems Workshops (ADSN 2012), pp.349-355, June 2012.

[5] K.Okano, T.Ohta, and Y.Kakuda, “A dynamic network gateway selection scheme based on autonomous clustering for heterogeneous mobile ad hoc network environment, ” Proc. IEEE Global Communications Conference Workshop (GC’12 Workshop), pp.513-517, Dec. 2012.

[6] T.Ohta, S.Inoue, and Y.Kakuda., ”An adaptive multihop clustering scheme for highly mobile ad hoc networks,” Proc. 6th IEEE Int’l Symp. on Autonomous Decentralized Systems (ISADS2003), pp.293-300, April 2003.

[7] T.Ohta, S.Inoue, Y.Kakuda, and K.Ishida, ”An adaptive multihop clustering scheme for ad hoc networks with high mobility,” IEICE Transactions on Fundamentals, vol.E86-A, no.7, pp.1689-1697, July 2003.

[8] “Qualnet network simulator by scalable network technologies, ” http://www.scalable-networks.com/, 2012.

[9] C. Perkins, E. Belding-Royer, and S.Das, “Ad Hoc On-Demand Distance Vector (AODV) Routing, ” IETF RFC3561, 2003.