A Design of VCM (Vessel Communication Manager) Improving Communication Efficiency and Security with ARP (Azimuth based Routing Protocol) and NATF (Network Attack Traceback Facility) for Vessel Networking

Ina Jung[1], EunHee Jeong[2] and ByungKwan Lee[3]

[1]*Department of Computer, College of Engineering, Kwandong University, Gangneung-si, Gangwon-do 210-701, Korea*
[2]*Department of Regional Economics, College of Humanity & Social Science, Kangwon National University, Samcheok, Gangwon-do 245-711, Korea*
[3]*Department of Computer, College of Engineering, Kwandong University, Gangneung-si, Gangwon-do 210-701, Korea*
lupinus07@nate.com, jeongeh@kangwon.ac.kr, bklee@kwandong.ac.kr

Abstract

The VCM (Vessel Communication Manager) proposed in this paper consists of ARP (Azimuth based Routing Protocol) and NATF (Network Attack Traceback Facility). The ARP can transmit accident information from a source to a headquarter rapidly and accurately by using Azimuths. It designs the Ac-RREQ message that appends an azimuth, a cumulation S/N, and a standby packet count field to the exiting RREQ message and the Ac-RREP message that appends an azimuth and a cumulation S/N field to the existing RREP message. It adjusts the transmission scope of the Ac-RREQ message with azimuths and decides the optimal path by judging the priority of Ac-RREP with the standby packet count and the cumulation S/N. Therefore, its simulation shows that the transmission time of the Ac-RREQ message is reduced more largely than the existing RREQ by using azimuths. In collision, as it transmits data through optimal paths, not only unexpected accidents are prevented with an urgent action, but also the life of nodes is prolonged due to the energy-saving of nodes. And, the NATF can trace back network attacks happening inter-vessel by recording the routes of routers with marking and logging function and can reduce a traceback overhead because of not marking all the packets.

Keywords: *VCM, ARP, NATF, Azimuth, Marking, Logging, Traceback*

1. Introduction

When two electronic systems communicate autonomously without human intervention, the process is described as M2M (Machine-to-Machine) communications. M2M communications are gaining attention from both academia and industry. There will be more machines connected to the Internet than human beings in the next decade. M2M communications transfer data on the condition of physical devices to a remote central location for effective monitoring and control [1, 2] by using Ad-Hoc networks and an AODV (Ad Hoc On-demand Distance Vector) routing protocol. The AODV has trouble deciding the optimal routing

[1] First Author
[2] Co-First Author
[3] Corresponding Author

because it considers only the shortest paths without considering the cumulation S/N and standby packet count.

This paper proposes the VCM improving communication efficiency and security with ARP and NATF for Vessel Networking. The ARP transmits accident information from a source to a headquarter rapidly and accurately by using Azimuths. It designs the Ac-RREQ (Accumulated Routing REQuest) message that appends an azimuth, a cumulation S/N, and a standby packet count field to the exiting RREQ message and the Ac-RREP message that appends an azimuth and a cumulation S/N field to the existing RREP message. It adjusts the transmission scope of the Ac-RREQ message with azimuths and decides the optimal path by judging the priority of Ac-RREP (Accumulated Routing REQuest) with the standby packet count and the cumulation S/N. And, the NATF can trace back network attacks happening inter-vessel by recording the routes of routers with the marking and logging function.

2. Related Works

2.1 Reactive Routing Protocol

The typical protocol of Reactive Routing Protocol is AODV that routes messages between mobile computers [3, 4, 5]. It is an on-demand and distance-vector routing protocol, meaning that a route is established by the AODV from a destination only on demand [6, 7, 8, 9]. The AODV uses the RREQ and the RREP. The RREQ messages are used to initiate the route finding process, and the RREP messages are used to finalize the routes. When a route does not exist to a given destination, a RREQ message is flooded by the source and by the intermediate nodes if they have no previous routes in their table. Upon receiving a RREQ message, the receiving node will record the route information in its own routing table [9, 10]. Table 1 shows the RREQ message format [8].

Table 1. RREQ message format

Type	Join flag	Repair flag	Gratuitous RREP flag	Reserved	Hop Count
Broadcast ID					
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Source Sequence Number					

Once the RREQ message reaches the destination or an intermediate node, the node responds by unicasting a RREP message back to the neighbor from which it first received the RREQ message. As the RREP message is forwarded back along the reverse path, nodes along this path set up forwarding entries in their routing tables, pointing to the node from which they received the RREP message [9, 10, 11]. Table 2 shows the RREP message format [8].

Table 2. RREP message format

Type	Repair flag	A	Reserved	Pfx Length	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Life Time					

2.2 Probabilistic packet marking

PPM (Probabilistic packet marking) was originally suggested by Burch and Cheswick [12] and was carefully designed and implemented by Savage [13]. It is defined to be the most famous packet identification techniques. In this methods, the packets are marked with the router's IP address from which they traversed or the path edges from which the packet is being transmitted. Marking the packets with the router's address is the best approach when compared to the others, where if a packet is lost due to any attack, the source router address can be fetched and sent back to the actual router [14, 15].

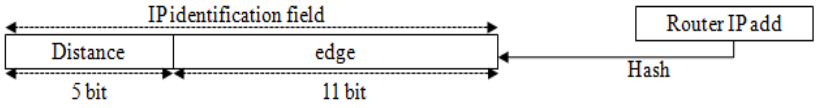


Figure 1. The structure of Advanced Marking Scheme [16]

3. A VCM(Vessel Communication Manager) Design

When a collision is sensed, this paper proposes a VCM improving communication efficiency and security with ARP and NATF to transmit image data and location data to a headquarter rapidly and accurately and to trace back network attacks with marking and Logging function for Vessel Networking.

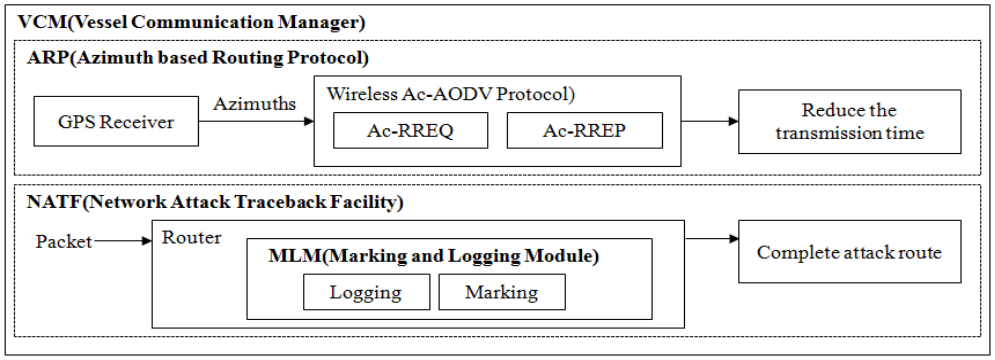


Figure 2. The components of VCM(Vessel Communication Manager)

3.1 An ARP (Azimuth based Routing Protocol) design

3.1.1 A GPS Receiver design

The GPS Receiver is designed to transmit the coordinate on a current location to the WAP (Wireless Ac-AODV Protocol). At this time, the GPS Receiver measures the location not only of collision but also of the headquarter and decides an azimuth.

The processing steps of the GPS Receiver are as follows.

[The 1st steps] The GPS Receiver delivers collision location information to the WAP and searches for the nearest place to transmit the collision information to the headquarter.

[The 2nd step] The GPS Receiver computes the direction for the optimal path so that it can transfer the collision information to the headquarter, where the direction means an angle and

the distance between a source and a destination must be first computed before deciding the direction. The following expression (1) computes the distance between two points and all the coordinates are expressed with radians [17, 18].

radian_distance=acos(sin(Lat1)×sin(Lat2)
+cos(Lat1)×cos(Lat2)×cos(Lon1-on2)) .....(1)

[The 3rd step] An actual distance is obtained by multiplying 3437.7387 by the radian_distance which is the result of the 2nd step. The moving direction is computed by the following expression with the distance between two points(2)[12,13].

radian_bearing=acos((sin(Lat2)-sin(Lat1)×
cos(radian_distance))/(cos(Lat1)×sin(radian_distance)))……..…..(2)

[The 4th step] As a radian value is applied to the moving direction value obtained in the 3rd step, it must be changed to an actual azimuth. The expression (3) used to change to an actual azimuth is as follows[12,13].

true_bearing = radian_bearing × (180/π) …….. (3)

If sin(Lon2)–sin(Lon1)<0, the moving course must be decided as (360–true_bearing).

[The 5th step] The azimuth computed through the above 4 steps is transferred to the WAP.

The WAP must transmit the data to a headquarter.

3.1.2 A WAP(Wireless Ac-AODV Protocol) design

When the WAP receives the sensed data on vessel, it set the routing path to transmit the data to a headquarter. This paper proposes an AODV based Ac-AODV design to improve the efficiency of wireless communication.

1) Ac-RREQ message format

The Ac-RREQ message format proposed in this paper appends an azimuth field to consider a direction from a source to a destination, a cumulation S/N field to store the cumulative values of S/N ratio, and a standby packet count field to store the value cumulating the number of waiting packets within each node's queue to the AODV based RREQ message format. In this way, this ARP transmits data through the routing paths with less waiting time relatively

Table 3. Ac-RREQ message format

Type	Join flag	Repair flag	Gratuitous RREP flag	Reserved	Hop Count
Broadcast ID					
Destination IP Address					
Destination Sequence Number of destination					
Source IP Address					
Source Sequence Number					
azimuth		cumulation S/N		standby packet count	

2) Path Setting

The path setting of the Ac-RREQ message based on Ac-AODV proposed in this paper considers an azimuth, a cumulation S/N ratio, and a standby packet count to improve the transmission speed of messages.

(1) Azimuth

The WAP reduces the path search time by transmitting Ac-RREQ messages to only the nodes lying within the 90°, not within the 360°of the existing RREQ message by using the azimuth that the GPS Receiver decided. When the data is transmitted from a source to a destination like Figure 3, the RREQ message is broadcast to all nodes, but the Ac-RREQ message is transmitted to only the nodes within an azimuth obtained through the following steps.

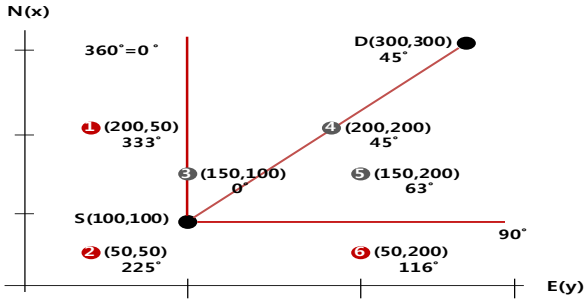


Figure 3. The transmission scope of AC-RREQ using an azimuth

[The 1st step] The azimuth of a source node S(100,100) and a destination node D(300,300) is computed.

[The 2nd step] If the azimuth 45° is decided, both directions on the basis of 45° becomes 90° in Fig. 4. That is, the transmission scope of Ac-RREQ message is decided within 0°~ 90°.

[The 3rd step] The azimuths of the neighboring nodes are computed on the basis of a source.

[The 4th step] If the azimuth of the neighboring nodes lies within the transmission scope of an Ac-RREQ, the Ac-RREQ message is generated and transmitted. That is, the Ac-RREQ message is not transmitted to the 1, 2, 6 nodes beyond the scope. As it is transmitted to only the normal neighboring 3, 4, 5 nodes and the routing paths are searched for, this paper can reduce the unnecessary message generation and path search.

(2) Standby packet count

As the existing method transmitting an RREP message through the paths with the shortest hops considers only the hop count, not the packets waiting within the queue of nodes, the rate of data transmission can be lower. Therefore, in an Ac-RREQ message, the standby packet count field storing the total number of the waiting packets of each node is appended to solve this problem. Therefore, this paper improves data transmission speed by selecting the node with the fewest packets waiting within the queue of each node.

(3) Cumulation S/N

If a noise collides with a signal terribly and errors happen, some of data packets must be retransmitted. It is why data transmission speed is reduced. By using an Ac-RREP, when the final path set in reverse path is decided, this paper selects the path with the largest value among the cumulation S/Ns and improves the data accuracy and transmission speed.

The expression of S/N used in this paper is shown in expression (4). Where Vs means incoming signal strength and Vn means a noise.

$$S/N = 20 \log10(Vs/Vn) \quad \text{..... (4)}$$

3) Reverse Path Setting

When an Ac-RREQ message proposed in this paper is broadcast, two cases happen. One case is to find paths from an intermediate node to a destination and the other case is not to find paths in neighboring nodes. In broadcasting an Ac-RREQ message, the processing procedure is different in these two cases.

① In an Ac-RREQ message being broadcast, paths from an intermediate node to a destination can't be found

[The 1st step] In Figure 4(a), when an Ac-RREQ is transmitted to the neighboring nodes within the scope of the 45° in the left direction and the 45° in the right based on a azimuth, the neighboring nodes, a, b within the scope may not know the path for a destination. In this case, the node, a, b that received an Ac-RREQ message set the path destined for a final destination, setting the reverse path for the search of the reverse path so that they can go back to the sender

[The 2nd step] In Figure 4(b), each intermediate node, a, b which set the reverse path transmits an Ac-RREQ message to its neighboring nodes, f, d, e. At this time, as each node a, b are not source nodes, each updates the Ac-RREQ message that incremented Hop count by cumulating its S/N value to its S/N cumulation field and by cumulating its standby packet count within the queue of its router to the Standby Packet count filed. And then, the updated Ac-RREQ message is also transmitted to the neighboring nodes f, d, e.

[The 3rd step] Each intermediate node d, f also set the reverse path by transmitting to its neighboring node the result that cumulated its own information to the cumulation field of the Ac_RREQ message. At this time, as the neighboring node D to which f transmitted an Ac_RREQ message becomes a destination, the sequence number of a destination in Ac_RREQ message that was transmitted from the f node is that of the final destination on the same path. In the same way, a S/N cumulation value, a standby packet cumulation value and Hop Count are also decided as the final value on the same path.

[The 4th step] As the intermediate node g also transmied an Ac-RREQ message to the neighboring and final node D like f node, the final S/N cumulation value, the sequence number of the destination, the standby packet cumulation value and the Hop Count are decided.

[The 5th step] In Figure 4(e), if the Ac-RREQ message is transmitted to a node, all the reverse paths on the node is set, the destination D which received two Ac_RREQ messages selects the final path between the two Ac-RREQ messages and selects the inside information of each Ac-RREQ message to transmit the Ac-RREQ message after selecting the final path.

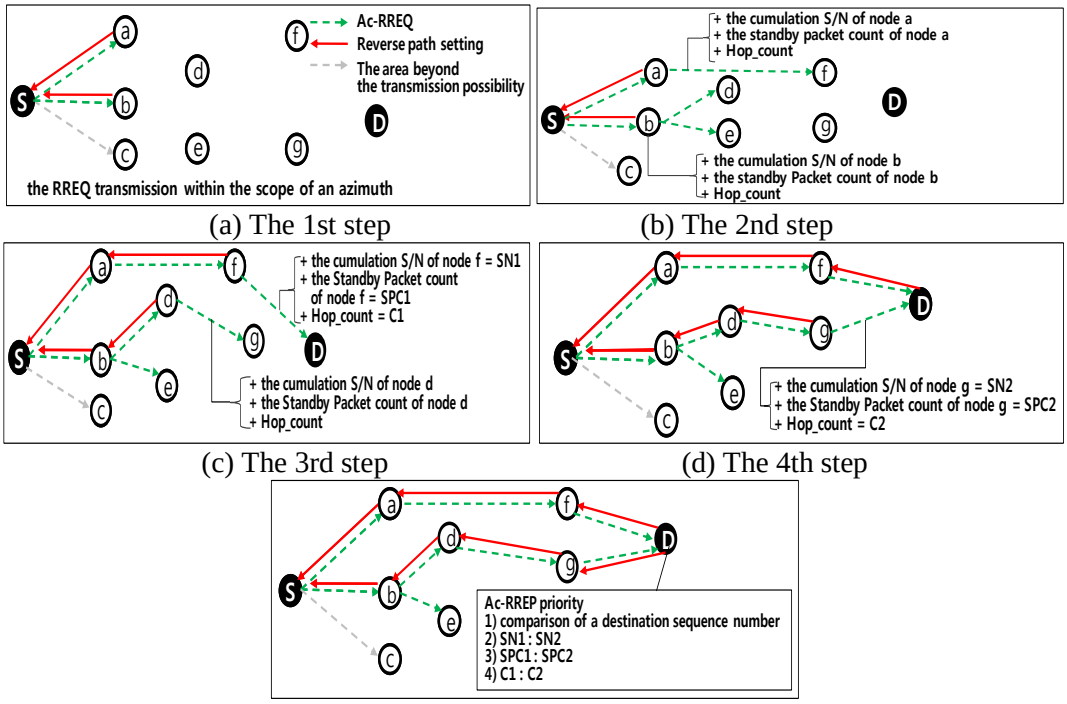


Figure 4. Ac-RREQ broad casting

This paper is to decide multi-path by choosing the paths which are far away from the "0.9 X (the maximum transmission scope of a node)" which is the expression on interference prevention for the paths which granted priority like that.

② In Ac-RREQ message being broadcast, the path from an intermediate node to a destination node on the routing table can be found

When the Ac-AODV in this paper finds the path from an intermediate node to a destination, the Ac-AODV unicasts the Ac-RREP message in the same way that AODV unicasts the RREP message. Not only among the paths transmitted from the intermediate node but also among the newly generated paths to which the Ac-RREP is transmitted, the Ac-AODV selects and updates the optimum paths in the routing table on the basis of the priority decided by the cumulated value of the Ac-RREP field. The priority at this time is used in the same way that the path from an intermediate node to a destination can't be found.

[The 1st step] When the source node S delivers the Ac-RREQ message to the node a, b and receives the Ac-RREP message as a response, it is assumed that the node a knows the path to destination.

The Ac-RREQ message is transmitted to the node a. As it found the path to destination after checking its routing table, it transmits Ac-RREP message to a source in spite of an intermediate nod. At this time, the Ac-RREP message including the sequence number of destination(SA) which the node a has and the number of its hops(CA) is transmitted. When the node b receives the Ac-RREQ message from the node and checks the routing table, the path is not found.

[The 2nd step] The node b that doesn't find a path sets a reverse path. The Ac-RREQ message field that accumulated its information and incremented the Hop count is retransmitted to the node d, e neighboring to the node b

[The 3rd step] After the node d check a routing table and when it is assumed that the path to a destination exists, the node d compares the destination sequence number(SA) in the node a with its destination sequence number(SD). The path which has the larger value of the two is selected and the Ac-RREP message is transmitted through the path to the node b. As the node E received Ac-RREQ message and it didn't find the path to the end, it didn't deliver the RREP message to the node b for some time. At this time, the path to which the RREP is not transmitted for some time is automatically deleted.

4) An Ac-RREP design

The Ac-RREP message format proposed in this paper is shown in Table 4. The azimuth field and cumulation S/N field of the Ac-RREQ message are appended to the existing RREQ message so that the azimuth information and S/N cumulation value of a final path can be stored in the routing table. When the azimuth information is stored in the routing table and the data is transmitted to the designated destination later. The Ac-RREP has the advantage not to pass through the GPS Receiver.

The Ac-AODV proposed in this paper doesn't transmit the Ac-RREP right to the node which has the least interference through the expression of the existing method, but applies priority to the node with less interference. The priority applying to the process of the Ac-RREP field selection is as follows.

The 1st, the reverse path with the large sequence number of a destination. That is, the path used recently.

The 2nd, the largest value of S/N values.

The 3rd, the node with the smallest cumulative standby packet count.

The 4th, the reverse path with the least interference after expression is applied.

The 5th, the path with an ascending order of the cumulative hops count is decided as an optimum path.

Table 4. Ac-RREP message format

Type	Repair flag	acknowledgment	Reserved	Prefix Sz	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Lifetime					
azimuth			cumulation S/N		

3.2 A NATF(Network Attack Traceback Facility) design

The NATF decides if it will mark packets by checking the marking count of the packets passing through routers, or if it will record the contents of packets in a Logging DG(Digest) Table according to the following conditions.

Condition 1] The NATF does the logging if the marking count of a packet is the multiple of 2 and does the marking if it is not the multiple of 2.

Condition 2] The NATF does the logging and the marking count becomes 0 if both Ac_RID(Router ID) and Last_RID are 0

When the NATF does the Logging, it records Time Stamp, Last_RID and Ac_RID(Router ID) in a Logging DG Table, and when it does the Marking, it records Marking Count, Last_RID, Ac_RID in a packet, where Last_RID means a router' last visit and Ac_RID accumulated router IDs. The Ac_RID is initialized by 0 during the Logging, but the Marking process is used to record the visited paths in the Ac_RID by XORing the contents of the Ac_RID recorded and its Router ID. The structure for storing Marking resultis as follows.

3.2.1 MLM(Marking and Logging Module) design

The MLM(Marking and Logging Module) records its ID to Last_RID so that a router which it visited last may mark itself. And the result which XORed a router ID recorded in the Ac_RID and its ID is stored in the Ac_RID. The MLM transfers the Marking Count increased by 1to the next Router.

The MLM records in its Logging table the Time Stamp, Last_RID and Ac_RID summarized about packets, and then records its ID in the Last_RID. As the Logging was done, the Ac_RID is again initialized by 0. And as the Marking was not done, Marking Count is not increased. Figure 5 shows the process in which the MLM judges and does the Marking and Logging.

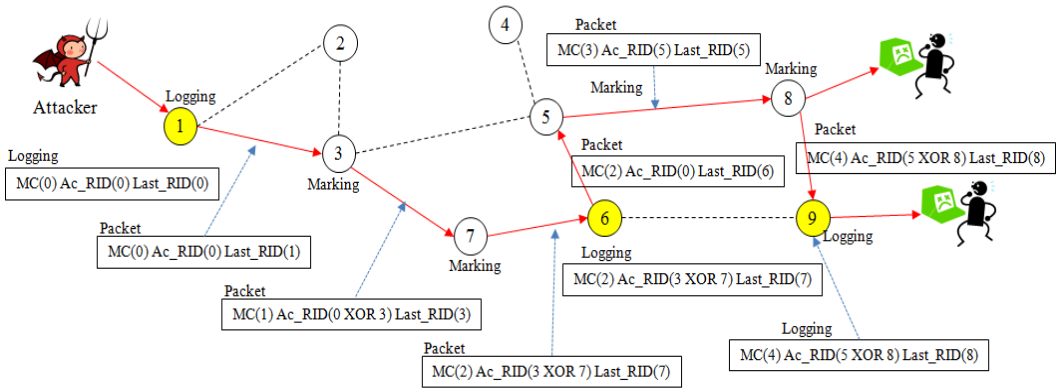


Figure 5. The procedure example of MLM

For example, it is assumed that Attack path is Router 1-3-7-6-5-8-9 and Router 1 is a source with Marking Count=0, Ac_RID=0, and Last_RID=0. As Router 1is a source, it unconditionally does the Logging and records the Time Stamp, Ac_RID(0), and Last_RID of a packet in its Logging DG Table. And after Router 1 records marking count=0, Ac_RID(0), and Last_RID(1) in a packet, it transfers the packet to the next Router. As in the Router 3 of intermediate route, Marking Count is less than 2 and is not the multiple of 2, the Marking can be done. That is, Router 3 increases Marking count by 1, records the result XORing 0 and3 in the Ac_RID, and router ID 3 in the Last_RID. And it transfers the packet with the information to the next router.

As Router 6 is the multiple of 2, it does the Logging. The Router 6 records the packet's arrival time in timestamp, the result of (3 XOR 7 XOR 6) in Ac_RID, its Router ID in

Last_RID. As Router 6 did the Logging, it initializes Ac_RID by 0 and after it marks Marking count(2), Ac_RID(0), and Last_RID(6) in a packet, it transfers the packet to the next router. At this time, as the Router 6did the Logging, marking count is not increased.

3.3 A VCM(Vessel Communication Manager) traceback procedure

Figure 5 has two attack routes. Attack packets were detected in the Router 9 of the first attack route and in the Router 8 of the second attack route. The Router 9 did the Logging and The Router 8 the Marking.

The VCM traces back an attack route from a logging router as follows.

①The VCM receives the information of the Logging Router 1, 6, 9 from the NATF. The VCM does the traceback from Router 9 with the information.

②The VCM looks for the router which this attack packet visited. To begin with, the VCM has 3 routers which were transferred from the NAT and looks for the attack packet whose Marking Count is 4 in Router 9. And The VCM makes Path Count(=7) by adding Marking Count(=4) and the number of routers(3), where the Path Count means the hop count which the attack packet visited.

③ The VCM received the 8 of Last_RID and the (5 XOR 8) of Ac_RID from the Logging DG Table of Router 9. This means that an attack packet arrived at Router 9 via Router 8. By XORing the 8 of Ac_RID and the (5 XOR 8) of Last_RID, the VCM checks that the attack packet arrived at Router 8 via Router 5. Therefore, the VCM knows that the attack packet moved to the order of Router 5, 8 and 9.

④ The VCM receives the logging record from Router 6 and does the same as the ③. It knows that the attack packet was transferred in the order of Router 3, 7 and 6.

⑤ The VCM searches for Ac_RID=0 and Last_RID=0 from the logging record of Router 1 and knows that Router 1 is a source

⑥ The VCM checks if an attack was transferred to packet Router 1, Router 3, Router 7, Router 6, Router 5, Router 8, and Router 9 and judges that the attack route was found because the number of the completed reverse path routers matches path Count(=7).

The VCM traces back the second attack route with a marking router, contrary to the first traceback. But, if the VCM starts the traceback from the marking router without the record about an attack packet and computes the Path Count by adding marking count and the number of routers, an error will happen in it. To tackle this problem, the VCM was designed to add 1 to path Count when the traceback about an attack packet starts from the marking router.

The VCM traces back an attack route from the Marking Router as follows.

① The VCM receives Router 1 and 6 with the logging record of an attack packet from the NATF and starts the traceback from Router 8 which detected an attack.

② The VCM computes the Path Count(5) by adding the marking count(3) and the number of routers(2) because the marking count from an attack packet is 3 and the number of routers from the NATF is 2. At this time, the VCM computes the Path Count(6) by adding 1 to Path Count(5) because the Router 8 which detected an attack is a marking router.

③ As the Router 8 does the Logging, the VCM doesn't know the route. But as the Last_RID of an attack packet is 5, the VCM knows that the attack packet arrived at Router 8 via Router 5.

④ The VCM searches for the reverse path in the same way as the first path detection in Router 6 and Router 1. That is, the VCM checks if the attack packet is transferred to the order of Router 1, Router 3, Router 7, Router 6, Router 5, and Router 8. And the VCM judges that the exact reverse path was found because the number of routers which the attack packet visited matches Path Count(6).

4. Simulation

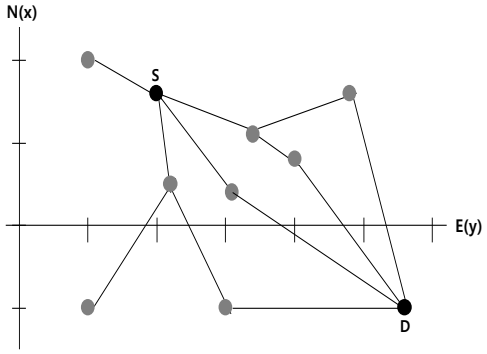
The simulation of the ARP proposed in this paper was experimented in two ways. The first way is to evaluate the performance used for an azimuth. The second way is to evaluate the performance on transmission speed.

4.1 An azimuth based the ARP simulation

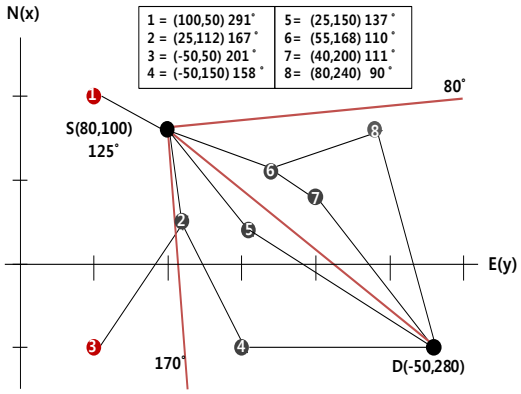
Compared the existing AODV method with the ARP based on azimuth, it is estimated that the Ac-AODV diminished the unnecessary generation of Ac-RREQ message more than the existing AODV method. In addition, the performance of the ARP is estimated according to an azimuth angle by applying an azimuth from a source to a destination to the transmission scope of the Ac-RREQ. The 25° in the left and 25° in the right direction, and the 45° in the left and 45° in the right direction are used as an azimuth angle in this experiment.

Figure 6 shows the comparison of the existing AODV method with the ARP based on an azimuth for the search of the path from a source S to a destination D. Figure 6(a) shows that the RREQ message is transmitted to all the neighboring nodes of a source in the AODV method. If the path to destination in the routing table of an intermediate node can't be found, the RREQ message is generated 12 times.

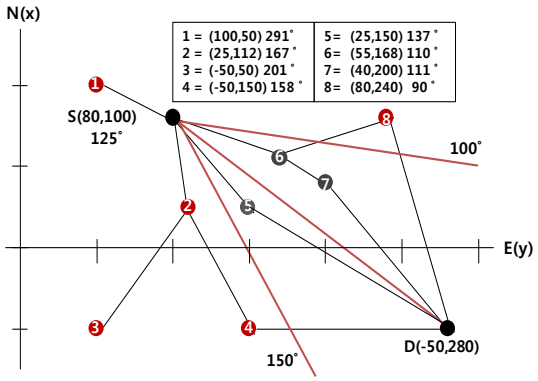
Figure 6(b) shows that Ac-RREQ generation and transmission times are reduced in the ARP based on an azimuth proposed in this paper. The ARP transmits the Ac-RREQ message only to the nodes existing between 80° and 170° at the cardinal point S(80, 100), in case the ARP applies the 45° in the left and 45° in the right direction to the azimuth angle 125° between a source S(80,100) and a destination D(-50,280) in the transmission scope. That is, as the node 1 with the azimuth angle 291° neighboring to a source is beyond the transmission scope of the Ac-RREQ, the Ac-RREQ message is not generated and transmitted. Each node 2, 5, 6 with each azimuth angle 167°, 137°, 110° exists between 80° and 170° of transmission scope. In this case, as it is estimated they exists within the direction for a destination, the Ac-RREQ message is generated and transmitted. Therefore, as the 3 Ac-RREQ messages happen in the initial source of the ARP and the 10 Ac-RREQ messages are finally generated and transmitted on the same condition as the existing AODV, The message generation and transmission times is reduced by 17%.



(a) AODV



(b) ARP (azimuth 45°)



(c) ARP (azimuth 25°)

Figure 6. Comparison the existing AODV to the proposed ARP

It is shown that Figure 6(c) is applies to the azimuth angle 25°. That is, only the nodes between 100° and 150° based on a source by applying to 25° in both sides on the basis of azimuth 125 can transmit messages. Therefore, in case the Ac-RREQ message is transmitted by applying to azimuths like as Table 5, the unnecessary message generation can be diminished. In addition, as the angle is getting smaller, the efficiency is the better. But, if the angle get too much smaller and the nodes transmitting the RREQ message don't exist. the path to destination can't be found.

Table 5. The comparison of Ac-RREQ generation and transmission times

	AODV	ARP(45°)	ARP(25°)
The number of nodes	10	10	10
Ac-RREQ generation and transmission times	12	10 (17% reduction)	5 (58% reduction)

4.2 NATF

The NATF proposed in this paper can detect the traceback with Marking and Logging. In it's experimentation, an NS-2 simulator and total 10 nodes are used to compare when the Marking and Logging was done to when nothing was done.

Table 6. The comparison of when "Yes" to when "no" about marking and logging

Marking and Logging	node	Packet size	interval	Time	The total number of transmission packets	The number of packets which arrived
Yes	10	500	0.05	8.0	125,490	5936
No					125,949	5970

In Table 6, when the Marking and Logging weren't done, the number of packets which arrived at a destination is 5970. But, when they were done, the number of packets which arrived at a destination is 5936. A little time delay happens in the NATF because of the marking and logging, but A little more time delay also happens when using the marking than when not using it in the existing probabilistic packet marking. As the existing probabilistic packet marking uses packet data to recover a path, it is impossible to recover the path with a single packet. As the NATF acquires the information of the router which a packet visited with the logging data of a router, contrary to the existing probabilistic packet marking, it can recover a path regardless of the number of packets.

5. Conclusion

This paper proposes the VCM improving communication efficiency and security with ARP and NATF for Vessel Networking. The ARP that transmits the accurate information to a destination rapidly by designating the transmission scope of message with an azimuth. The ARP appends an azimuth, a cumulation S/N, and a standby packet count field to Ac-RREQ message and appends an azimuth and a cumulation S/N field to the Ac-RREP

In the azimuth 45°, the ARP reduces the Ac-RREQ and the Ac-RREP message and takes less transmission time than the AODV message considering only the number of hops. Therefore, after sensing the collision, the ARP analyzes the fastest path and provides the routing path to transmit the accurate data. In addition, it not only prevents an unexpected accident rapidly but also prolongs the life of sensor nodes because of the energy- saving of sensor nodes.

As the NATF acquires the information of the router which a packet visited with the logging data of a router, contrary to the existing probabilistic packet marking, it can recover a path regardless of the number of packets.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2012R1A1A4A01012039).

References

[1] J. Rakkolainen, "Machine to Machine (M2M) Communications", CEPT Workshop, **(2011)** 28 February.
[2] D. Crowe, "Machine-to-Machine Communications", Wireless Telecom/Issue Three, **(2007)**, pp. 28-31.

[3] L. Klein-Berndt, "A Quick Guide to AODV Routing, NIST, www.antd.nist.gov/wctg/aodv_kernel_aodv_guide.pdf.
[4] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector(AODV) Routing"m RFC 3561 (Experimental), **(2003)**.
[5] C. Perkins and E. Royer, "Ad-hoc On-demanded Distance Vector Routing", In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Application (WMCSA), **(1999)** February 26-26, pp. 90-100, New Orleans, LA.
[6] G. Rajkumar and K. Duraisamy, A Review of Ad hoc On-Demand Distance Vector Routing Protocol for Mobile Ad hoc Networks, Journal of Theoretical and Applied Information Technology, vol. 36, no. 1, **(2012)**, pp.134-144.
[7] J. -H. Song, V. W. S .Wong and V. C. M. Leung, "Efficient On-Demand Routing For Mobile Ad Hoc Wireless Access Networks", IEEE Journal on Selected Areas in Communications, vol. 22, no. 7, **(2004)**, pp. 1374-1383.
[8] C. E. Perkins, E. M. Royer and S. R. Das, "Ad hoc On-Demanded Distance Vector(AODV) Routing", draft-ietf-manet-aodv-08.txt, **(2001),** tools.ietf.org/ html/draft-ietf-manet-aodv-08.
[9] T. V. P. Sundararajan, K. R. Kumar and R. K. Karthikeyan, "A novel survey towards various energy models with Ad Hoc on Demand Distance Vector Routing Protocol (AODV)", In Proc. INCACEC'09, **(2009)** June 4-6, pp. 1-5.
[10] H. Narra, Y. Cheng, E. K. Cetinkaya, J. P. Rohrer and J. P. G. Sterbenz, "Destination-Sequenced Distance Vector(DSDV) Routing Protocol Implementation in ns-3", WNS-2, **(2011)** March 21, pp. 439-446, Barcelona, Spain.
[11] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing(DSDV) for Mobile Computers", In proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM), **(1994)**, pp. 234-244.
[12] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source", LISA'00 Proceedings of the 14th USENX conference on system administration, **(2000),** pp. 319-328.
[13] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Network support for IP traceback", IEEE/ACM Transactions on Networking, vol. 9, no. 3, **(2001)**, pp. 226-237.
[14] S. Vodithala, S. Nagaraju and V. C. S. Rao, "A Resolved IP Traceback through Probabilistic Packet Marking Algorithm", IJCST, vol. 2, no. 7, **(2011)**, pp. 40-43.
[15] T. Ma, "A link signature based DDoS attacker tracing algorithm under IPv6", IJSIA, vol. 3, no. 2, **(2009)**, pp. 27-36.
[16] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback", IEEE INFOCOM'01, **(2001)**, pp. 878-886.
[17] E. Williams, "Aviation Formulary V1.46", http://williams.best.vwh.net/avform.htm.
[18] Google Earth Antarctica, http://www.ig.utexas. edu/outreach/googleearth/latlong.html.

Authors

Ina Jung

Ina Jung received her B.Eng. degree from Kwandong National University in 2011, the M.Eng. degree in Computer Science from Kwan-Dong University in 2012. She is currently working towards a doctorate in Computer Science from Kwandong University. Her current research interests are Sensor Network, IT security, and Network security.

EunHee Jeong

EunHee Jeong received her B.S. degree from Kangnung National University in 1991, the M.Eng. degree in Computer Science from Kwandong University in 1998 and the Ph.D. degree in Computer Science from Kwandong University in 2003 in Korea. She has been a professor of department of Regional Economics at Kangwon National University in Korea since 2003, Sept. She is a regular member of the KSII. Her current research interests are Sensor Network, IT security, web programming, and e-commerce.

ByungKwan Lee

Byung-Kwan Lee received his B.S. degree from Pusan National University in 1970, the M.S. Degree in Computer Science from Chung-Ang University in 1986 and the ph.D. degree in Computer Science from Chung-Ang University in 1990 in Korea. He has been on the faculty of department of Computer Science and Engineering, Kwan-Dong University, Kang-Won-Do, Korea since 1988. He had been a visiting processor in Saginaw Valley State University, Michigan, USA for two years since 2000. He is a permanent member of the KISS and KIPS. His current research interests are distributed and network management, network security.