JRGP: Jamming Resilient Geocasting Protocol for Mobile Tactical Ad Hoc Networks

Sun-Joong Yoon and Young-Bae Ko
Department of NCW Engineering
Ajou University, Suwon, Republic of Korea
{sun2015, youngko}@ajou.ac.kr

Abstract— **Jamming attack by adversaries is the critical threat in Network Centric Warfare that uses tactical wireless networks. Thus research on developing new networking protocols that are resilient to such attacks are of high importance. Geocasting is a prominent routing mechanism in tactical networks to send critical messages such as alarm about chemical attack, guerrilla detection etc, to the nodes within a specific geographical region. To apply geocast protocols in the tactical environment, it should provide assurance that the packet delivery is reliable despite of jamming attacks. In this paper, we propose two jamming resilient geocasting schemes for tactical mobile ad hoc networks. Our first scheme called the "Failure-Based Learning" in which the sender nodes are not aware of the jamming attacks and try to send packets repeatedly. This method is enhanced by another scheme called "Detour by Anchor Point" with information about the jamming attack which sent to the source node, such that it can proactively avoid the jamming region for successful packet delivery. The simulation results show that our proposed schemes significantly outperform single and dual path geocasting protocols under jamming attack and mobile scenarios.**

Keywords; jamming attack, geocasting, tactical MANETS, failure-based learning, detour by anchor point.

I. INTRODUCTION

The concept of network centric warfare (NCW) is to connect weapon systems that are geographically distributed forming mobile ad hoc network in the battlefield. Such a networking system is required to efficiently share command control (C2) and situation awareness (SA) messages, which is highly critical while conducting war. Geocasting is an efficient networking protocol that can be used for disseminating SA and C2 messages required in the certain geographical region of the tactical domain. Failure in data-delivery ends up compromising the reliability of the network and thus war operation in question. In the battlefield where mobile ad hoc networking technologies are used, electronic attacks like jamming by the enemy is highly probable to prevent tactical communication. Jamming attacks in radio networks is the deliberate transmission of radio signals by adversaries to disrupt communication through interference and cause data delivery failures. In presence of fatal jamming attacks, geocasting protocols such as [1][2] fail to deliver any data to the destined geocast region. Therefore, the need of reliable protocols for transmitting packet under jamming attacks motivates this paper.

Our proposed protocol considers two cases depending upon whether the nodes are informed of jamming attacks or not during the data transmission. In the first case, if a transmission from the sender node to the next hop node fails, it tries to send the same packet to another neighbor node without regard to whether jamming attack is present or not. This process is repeated until the packet is transmitted successfully. In the second case, the source node is informed about the jamming attack through jammer detection messages. The alternative routing path is thus selected that avoids the jammed region in the network for successful delivery. To the best of our knowledge this is the first work that proposes efficient geocasting protocol considering jamming attacks.

This rest of this paper is organized as follows. In Section II we introduce the overview of jamming and jammer detection schemes. In Section III we propose jammer resilient geocasting protocol (JRGP) under jamming attacks in detail. Section IV provides performance evaluation of our proposed schemes and finally, in Section V, we conclude the paper.

II. RELATED WORK

Jamming is an important factor in the electronic warfare. The role of jamming in tactical wireless networks is to radiate interfering signals to disrupt communication and data transmission. By doing so, they disrupt enemy's rapid C2 and SA message delivery and lead the battlefield initiative. Frater et al. [3] suggest several types of communication jamming. The main types are spot, swept, comb, barrage and responsive jamming. Spot jammer focuses all of its power on jamming a single channel and sweep jammer can shift its power from one channel to another. Barrage and comb jammer can jam multiple channels at once. In barrage jamming, the jammer spreads its signal across several adjacent channels, but comb jammer can select channels to jam. Responsive jamming is similar to the spot jamming but it jams only when the transmission is detected.

Detecting jamming attack and finding the location of a jammer is important to assure reliable communication and

packet delivery. Xu et al. [4] propose two schemes for jamming detection with consistency checks. The first scheme continuously checks the received signal strength (RSS) and packet delivery ratio (PDR). If RSS is high but PDR is low, we can presume that the receiver is in the jammed region. The second scheme uses location information to serve as a proactive consistency checks. Every node advertises its location information periodically. If the node's PDR is low, it checks the distance of neighbor nodes. In the jammed case, receiver nodes PDR shall be low despite being close to the transmitter node. After detecting the jamming attack the location of the jammer can be estimated to avoid the jammed region [9].

There are several related researches to find the location of a jammer. Liu et al. [5] explain three algorithms of jammer localization: centroid localization (CL), weighted centroid localization (WCL) and virtual force iterative localization (VFIL). Jammed nodes are the ones located within the transmission range of the jammer. CL gathers location information of the jammed nodes, and averages their coordinates for predicting the jammer's location. However, this average value might be inaccurate and is affected by the distribution of jammed nodes. WCL enhances CL, by calculating the weighted average RSS received by the jammer node. VFIL applies CL to first estimate the location of jammer. Further, location is re-estimated based on the network topology iteratively until the region includes all the jammed nodes and other nodes falling in the boundary of the jammed region.

III. JAMMING RESILIENT GEOCASTING

In this section, we describe jamming resilient geocasting protocol (JRGP). JRGP is based on the greedy forwarding from the source to the geocast region and local flooding within the geocast region. If a node receives a geocast packet, it forwards the packet to the neighbor node closest to the destined geocast region. Sometimes, a void problem where a node does not have any other nodes that are closer to the geocast region may occur. In case of void, the perimeter mode and other schemes generally can be applied to make a detour [6]. In case of a jamming attack, although a node may have some nodes that are closer to the geocast region, the nodes suffering from jamming attack may mostly fail their packet transmission to the next hop node. If the inter arrival time of jamming signals is above the threshold, geocast packets can go through the jammed region. If the inter arrival time is below the threshold, they should circumvent the jammed region. Since the jamming attack can be classified as different from the void problem that we mentioned above, we propose two different schemes to solve the jamming problem.

We can classify two types of jamming environment. First, the nodes in the jammed region are unaware of the jamming attacks. This type of attack is called deceptive jamming [7]. If adversary sends fake data periodically in regular intervals, we cannot recognize the existence of jammer easily and it might severely influence the tactical operations utilizing wireless networks. Second, the nodes in the jammed area can identify the jamming attacks. In this case, it is necessary to reduce the control overhead of jammer detection messages and suggest efficient route to avoid the jammed region. In this paper, we assume that there is one jammer that jams the network between the source and the destination region.

A. *Scheme 1 : Failure-based learning (FBL)*

This scheme can be applied in both cases of jamming environment described in the sub section above. Every node in the tactical networks periodically sends HELLO messages including its location information. A node receiving a HELLO message adds the new neighbor information or updates the existing entry in its neighbor table. During the data transmission, when the node receives a geocast packet, it selects the neighbor that is closest to the geocast region and tries to send the packet. Sometimes link failures occur because the selected node may not exist within the transmission range owing to the node's mobility and asymmetric communication range. Son et al. [8] suggest the prediction of neighbor location to solve these link failures. Under the jamming attack, a link failure occurs even when the next hop node exists in the transmission range. In scheme 1, if a sender node fails to send a packet to the designated next hop node, it will remove that node from the neighbor table. Then it selects another closest node and tries to deliver the packet again. Every forwarding node in the path repeats the same procedure in presence of the jamming attack until the packet is successfully sent to the destination. However, in case when many nodes are under the jammer's influence, overhead of reselecting the neighbor node becomes higher and data delivery delay is increased. Thus in our proposed scheme, if the number of link failure exceeds the predefined limit, it sets the next hop node to the one nearby the threshold right angles or predefined angle based on the line through the sender node and the destination center-point of the geocast region. We called this scheme, failure-based learning (FBL).

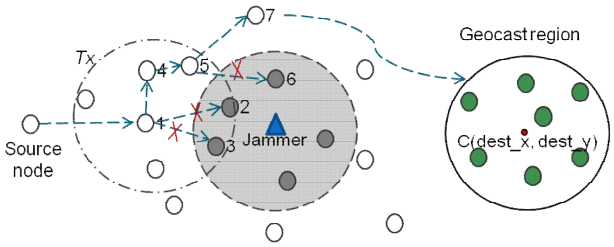

Figure 1: Example of failure-based learning

Fig. 1 shows an example of the FBL scheme. Node 1 is considered a current sender with neighbor nodes 3, 2 and 4 in its neighbor table, which also includes their location information. Point C is the center of the destined geocast region. The shaded region is the jammed region where, the jammer periodically emits signals at the periodic interval. The nodes around the jammer send their HELLO messages between the intervals of the jammer signals. If a HELLO message collides with the jammer signal, it cannot be received by the neighbor

nodes. In such cases the neighbor nodes shall delete this node information while updating their routing table. If the HELLO packet is received, the neighbor information is again updated. Note that the link failure is detected in the medium access layer. In fig.1, node 1 sends packet to node 2, but it does not receive clear-to-send (CTS) or acknowledgement (ACK) within the predefined time in 802.11 MAC indicating link failures. Thereafter, node 1 selects another node (node 3 in the example) but fails to transmit due to same reason. Given that we set the tolerance level of the number or link failures to 2, node 1 finally selects node 4 and sends the packet. Node 4 is selected because it is the closest node available to the 90 degree angle from the sender node. After receiving the packet, node 4 again forwards it to next neighbor node is closest to the geocast region.

B. *Scheme 2: Detour by Anchor Point (DAP)*

If a source node is aware of the jamming attack, it can proactively avoid such region while sending messages to the geocast region. In this paper, we apply jamming detection scheme, which can be referred in [9]. Anthony et al. [9] apply heuristics to decide whether the current node is suffering from jamming attacks. They assume that if the communication channel drops below a certain threshold, then a node is under jamming attacks. This paper focuses on guaranteeing packet delivery by avoiding transmission to the regions where jamming attacks have been detected. In [5], Liu et al. classify three node types; jammed node, boundary node and unaffected (ordinary) node. A jammed node is located in the jammed area and sends jammed messages periodically. The boundary nodes are located outside the jammed area and can receive the jammed messages from the jammed neighbors. These nodes send boundary node messages to the neighboring boundary nodes at periodic intervals. In [10], a boundary node sends jamming status messages to all nodes in the network to inform the existence of the jammer, which initiates everyone to update their routing table. This approach causes a lot of control overhead when jammers are mobile and operate randomly.

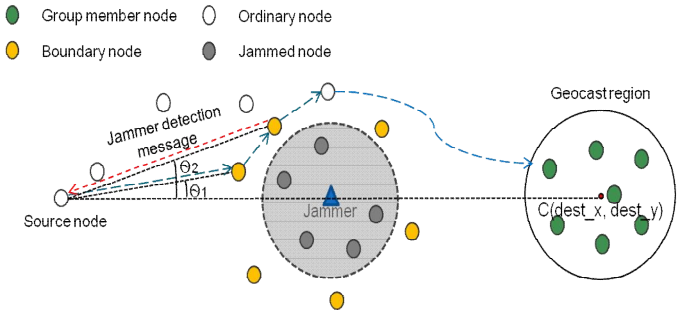

Figure 2: Example of a jammer detection message

Our scheme does not send jamming detection messages to all nodes. Instead, following measures are taken by the boundary nodes if the jammed messages are received while transmitting the geocast packet. First, it classifies all its neighbor nodes in the routing table into boundary nodes, ordinary nodes and jammed nodes. Then it selects its next-hop node that is closest to the destination point except from the jammed nodes and transmits the geocast packet. For sending the jamming detection message, the sending boundary node calculates the angle between the line connecting itself to the source node and the reference that connects the source node and the destination point. Let us call this angle (θ_1) as shown in Fig. 2.. Similarly, it also computes the angle of reference (θ_2) for the selected next hop node. Finally, if $\theta_2 < \theta_1$ or if the next-hop node is an ordinary node, it will send a jammer detection message back to the source node. Fig. 2 shows an example of sending a jammer detection message. The jammer detection message includes the average location of the jammed nodes that are located in the one hop distance of the sender boundary node. The source node may receive this message more than one time, depending on the node topology, jammer location and jammer interference range. If the source node receives jammer detection messages more than two times, it compares the location information of the boundary nodes. Among the boundary nodes that sent jammer detection messages, the one that has the largest angle is selected as an *anchor point*. Fig. 3 depicts how to compute the anchor point. We assume that the selected boundary node has N jammed nodes $\{(x_1, y_1), (x_2, y_2)\ldots(x_N, y_N)\}$ in one hop neighbors. The average location of jammed nodes is calculated by equation (1).

$$(X_a, Y_a) = \left(\frac{\sum_{k=1}^{N} X_k}{N}, \frac{\sum_{k=1}^{N} Y_k}{N}\right) \quad (1)$$

Let d be the distance between the boundary node and average location of the jammed nodes. The anchor point is set as to αd, where α is a variable that can be assigned any value from 1 to 3. Any node that is closest to the anchor point is selected as the forwarding node for the next packet transmission.

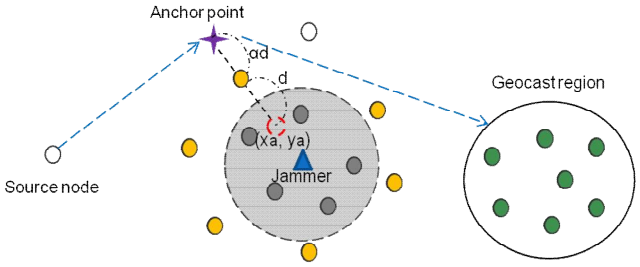

Figure 3: the source node sets the anchor point

IV. PERFORMANCE EVALUATION

A. *Simulation Environment*

In order to evaluate the performance, we implemented our algorithm in the ns-2 simulator [11]. The field area for our simulation model is 2000sqm where 400 nodes are deployed

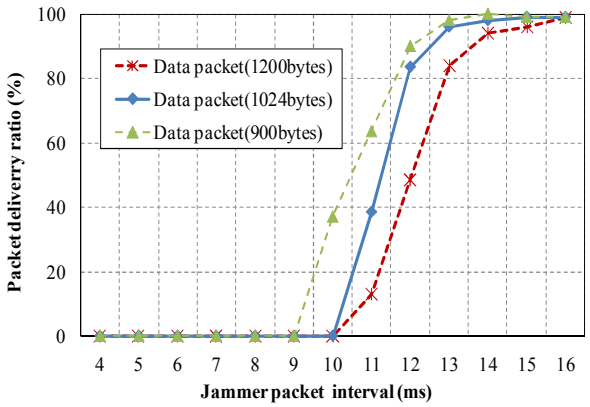

Figure 4: PDR under jamming attack

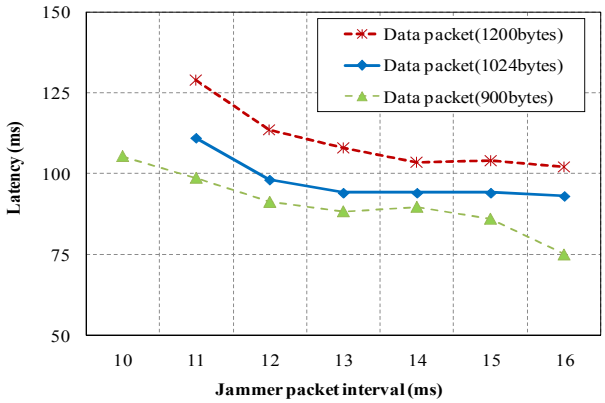

Figure 5: Latency under jamming attack

randomly and in the regular grid pattern. The simulation is performed in both static and mobile nodes. The random way point mobility model is considered with the nodes moving at the maximum speed of 5m/s without pause time. The IEEE 802.11 single channel radio is employed with the transmission range of 250m. The data rate is set to 2Mbps and each node sends periodic HELLO messages every second to the one hop neighbors. The source node is fixed at (300, 300). The geocast region is circular with the radius of 300m and the centre point located at (1600, 1600). The payload of geocast packet is 900, 1024 and 1200 bytes. The simulation time is 200 seconds and each scenario is repeated five times in the different topologies. We compared our proposed schemes with the single path geocasting protocol (SPGP) and dual path geocasting protocol (DPGP) in [12]. The metrics used for the evaluation are packet delivery ratio (PDR), latency and retrial counts.

B. Jammer model

We modeled spot jamming attack that occurs in a single channel. If adversaries emit jamming signals continuously, they can be easily detected and attacked. Therefore, we set a spot jammer that emits signals at periodic interval from a fixed location (800,800). The jamming range is in the radius of 550m around the given jammer location. The function of backoff and carrier sensing is eliminated so that the signals can be transmitted in the predefined intervals for occupying the spectrum. The 1024 and 120-byte jammer packet is used.

C. Simulation Results

First we show the impact of the jamming attack. Fig. 4, shows the PDR with respect to the jamming interval time. 10ms of jammer packet interval means that the jammer node emits the jamming signal (packet) every 10ms. PDR here is defined as the percentage of geocast group members that actually receive data packets. For example, if only three nodes among four geocast members receive a geocast packet, the PDR becomes 75%. In this scenario, we only consider static nodes deployed in the grid topology. Geocast packets are varied from 900 bytes to 1200 bytes and jammer packet is set as 1024 bytes. 400 nodes are deployed in the grid topology without node mobility. As the geocast packet size increases, PDR is decreased due to link failures by collision. Moreover, PDR is also directly affected as we decrease the interval time of jamming signal. Geocast packets and the HELLO messages should be delivered during the interval time when jamming signals are absent. Thus, lesser the jamming interval, lesser becomes the PDR irrespective of the data size. Fig. 5 shows the latency that represents the average time elapsed for delivering geocast packets from the source to geocast members. As the interval time of the jamming signal increases, the probability of collision decreases. Thus, the packets can transmit through the shortest path across the jammed region when the interval of jamming packets is longer. Moreover, probability of packet error too decreases as we decrease their sizes which improve latency.

Second, we compare our proposed schemes with SPGP and DPGP in [12] considering node mobility and jamming attack. Fig. 6 shows the simulation results of PDR with the node mobility. Comparing Fig. 6 and Fig. 4, the PDR of SPGP is significantly less because packet drop is high due to the link failure caused by the outdated location information in the mobile scenario. Even though DPGP shows improved PDR better than SPGP by using alternative path, it is still far below the expectation especially when the interval of jamming signals is less than 12ms. In the other hand, our scheme, FBL and JRGP shows almost above 95% of PDR success rate irrespective of jamming intervals. In case of FBL, its repeated attempt to transmit data packet eventually finds the neighbor for forwarding the data packet successfully, which is not observed in both SPGP and DPGP. However, FBL might drop packets when the routing loop is observed. i.e., when the node receives the same packet it forwarded before. The PDR of JRGP is higher than all other schemes as it avoids jamming region to successfully deliver the packets to the destination region. Fig. 7 depicts the latency and enlightens on the shortcomings of our proposed scheme FBL compared to JRGP. Since the successful delivery in the FBL comes with the cost of repeated trial in presence of link failures, its latency is high. However JRGP is almost always successful in detouring around the jammed region requires very few retrial attempts. Even though JRGP might fetch longer path causing some inherent delay, the tradeoff benefit observed from the effective

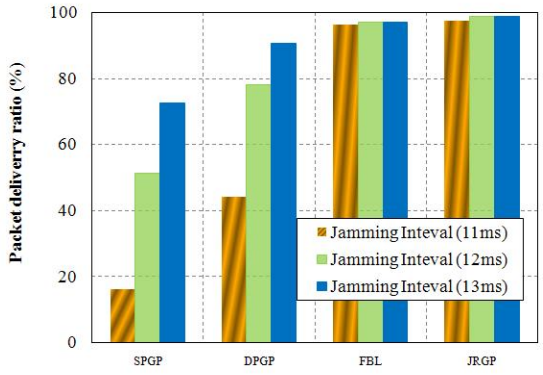

Figure 6: PDR with node mobility

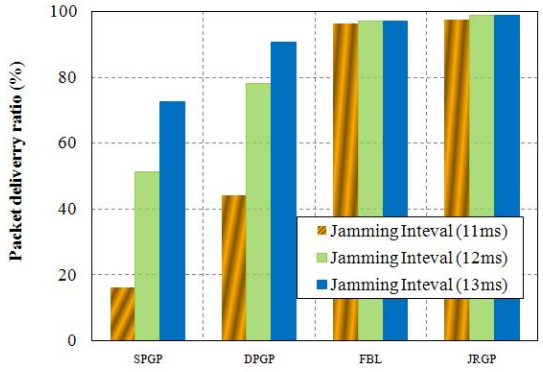

Figure 7: Latency with node mobility

PDR and reduced overhead compared to latency caused by repeated trial is significantly high.

To elaborate further on the advantages of our proposed scheme, we performed evaluation with small jamming intervals ranging from 1 to 9ms in the case of 120-byte jamming signal. Fig. 8 shows the PDR of FBL and JRGP in this scenario. We note that the PDR for SPGP and DPGP is almost zero, which can also be referred from Fig. 4 for packet sizes more than 900 bytes. The PDR for FBL is comparatively lesser than the JRGP with smaller jamming interval. The evidence in the trace shows that the HELLO messages from the affected nodes nearby jamming area frequently collide, which eventually outdate the location information. In addition, we observe infrequent routing loop error that drops packet. When the interval is less than 3ms, the results of FBL have 75% PDR. However, The PDR of JRGP is high, regardless of the jamming interval. Fig. 9 depicts the latency. When the interval is more than 3ms, most of the packets are attempted to be delivered through the jammed region. Therefore, frequent link failure increases delay. However, the latency is low at 1ms of interval, because packets are routed around the jammed region. This phenomenon occurs because jammed nodes are nonfunctional due to collision of HELLO messages with the frequent jamming signals from the jammer. Fig. 10 shows the average retrial counts. The retrial count is defined as the number of times a sender node detected link failures during one packet delivery from the source node to

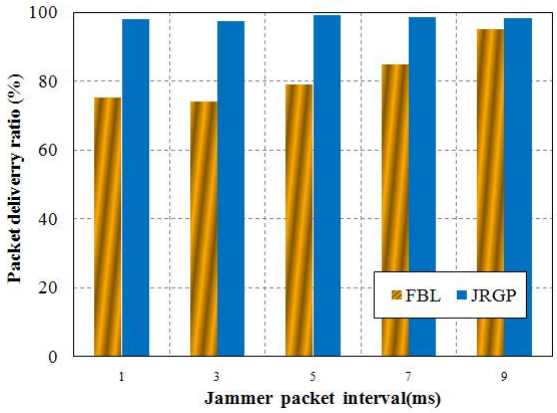

Figure 8: Packet delivery ratio

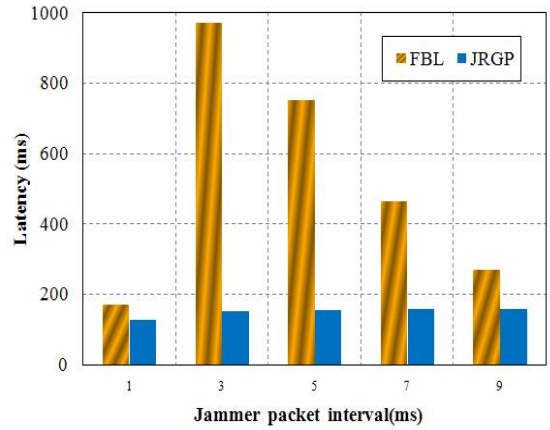

Figure 9: Latency

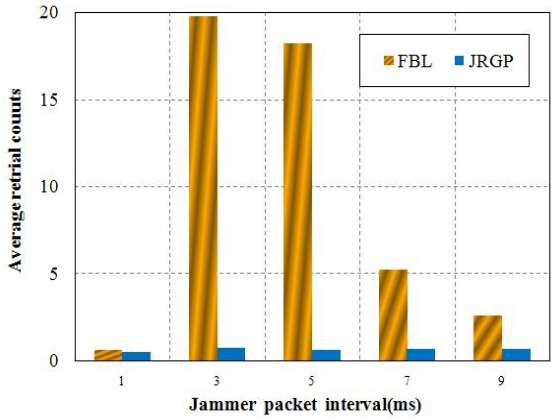

Figure 10: Average retrial counts

the geocast region. It increases, as we decrease the jamming interval because link failure is encountered frequently when packet is transmitted through the jammed region. However, in case when jamming interval is 1ms retrial counts become very less due to the same reason that make nodes in the jammed region non-functional due to frequent jamming signals. Thus, packets are automatically routed avoiding the jammed region.

V. CONCLUSION

In this paper, we proposed jamming resilient geocasting protocol that can be applied in tactical networks for delivering emergency and C2 messages in presence of the jamming attack by the adversaries. Our first scheme "Failure-Based Learning" uses repeated transmission attempt to go through the jammed region to reliably deliver the packet, however at the cost of increased latency and overhead. Another scheme "Detour by Anchor Point" operates when boundary nodes become aware of the jammed nodes. JRGP including FBL and DAP can deliver messages reliably and reduce control overhead of jammer related messages and latency. Recently the use of smart phones is increasing rapidly. Since commercial smart phones are enabled with the GPS, our proposed schemes can also be applied in commercial ad hoc networking by smart phone. In future work, we simulate further to evaluate the performance considering several jammer nodes that exist in the networks and the mobility of jammer nodes.

ACKNOWLEDGEMENT

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 (2010-0016189), and 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)).

REFERENCES

[1] H.L. Chen, C.C. Tseng, S.H. Hu, "An adaptive handshaking-based geocasting protocol in MANETs", in: Proceedings of the IWCMC, 2006.

[2] S.H. Lee, Y.B. Ko, "Efficient geocasting with multi-target regions in mobile multi-hop wireless networks", Wireless networks, vol. 16, no. 9, pp. 1253-1262, 2010.

[3] M.R. Frater and M. Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, 2001.

[4] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in Proc. MobiHoc, pp.46-57, 2005.

[5] H. Liu, W. Xu, Y. Chen, and Z. Liu, "Localizing Jammers in Wireless Networks", in Proc. IEEE PERCOM, Mar. 2009.

[6] D. Chen, P.K. Varshney, "A survey of void handling techniques for geographic routing in wireless networks," IEEE Communication Survey & Tutorials, vol. 9, no. 1, 2007.

[7] Mpitziopoulos. A, Gavalas. D, Konstantopoulos. C, Pantziou. G, "A survey on jamming attacks and coun-termeasures in WSNs", IEEE communications surveys & tutorials, vol. 11, no.4 2009.

[8] D. son, A Helmy, G. Krishnamachari, "The effect of mobility-induced location errors on geographic routing in mobile ad hoc and sensor networks", IEEE transactions on mobile computing, vol. 3, No 3 2004.

[9] A. Wood, J. Stankovic, and S. Son, "JAM: A jammed-area mapping service for sensor networks," in 24th IEEE Real-Time Systems Symposium, 2003.

[10] J.H. Lee, J.W Jung, JS Lim, "Jamming-Aware Direction Disjoint Multi-Path Routing in Tactical Network," in Proc. JCCI 2009.

[11] The VINT Project, The network simulator–ns-2. A collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC.

[12] S.J. Yoon, S.H. Lee, Y.B. Ko, "Reliable dual-path geoasting for tactical ad hoc networks," in proc. MILCOM, 2009.