Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 704253, 8 pages
http://dx.doi.org/10.1155/2015/704253

Research Article

An Emergency Adaptive Communication Protocol for Driver Health Monitoring in WSN Based Vehicular Environments

Young-Duk Kim,[1] Soon Kwon,[1] Woo Young Jung,[1] and Dongkyun Kim[2]

[1]*Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu 711-873, Republic of Korea*
[2]*School of Computer Science and Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea*

Correspondence should be addressed to Dongkyun Kim; dongkyun@knu.ac.kr

Received 19 December 2014; Accepted 23 March 2015

Academic Editor: Hideyuki Takahashi

Driver health and activity monitoring is one of the principal design issues for the safety provision in vehicular environments. Recently, the wireless sensor network technology is widely used to address the concerns in such applications. However, only few conventional protocols have dealt with reliable and prompt delivery of emergency packets considering the vehicular specifications. In this paper, we propose an emergency adaptive communication protocol, which treats the data packet in a discriminatory manner by investigating whether it is emergency or not. Hence, the proposed protocol defines an emergency factor for each data packet and exploits it for both route establishment and channel access procedures. In route establishment, the proposed protocol chooses a route with low delay and high reliability among the candidates by periodic calculation of emergency factor. Then, it dynamically adjusts back-off parameters before participating in the channel contention among the neighbors. In addition, an emergency aware queue management scheme and packet drop policy are proposed to improve the reliability of emergency data traffic during transmission. Our simulation results show that the proposed protocol provides a better performance compared with the existing protocol in terms of packet delivery ratio, end-to-end packet delay, and number of dropped packets.

1. Introduction

A wireless sensor network (WSN) is a network of sensor devices used in various application fields such as medicine, military, agriculture, and industry. One of the most popular applications of WSN is in development and deployment of health monitoring system to provide people with suitable, timely, and efficient safety services anytime and anywhere. In the case of vehicular environments, driver heath monitoring is significantly crucial for designing the vehicular safety because a delay in processing driver's abnormal health data may result in serious traffic accidents. However, to develop WSN based driver health monitoring systems, there are several problems. The most general problems are described as follows.

First, according to the previous research [1], between 13% and 50% of vehicular crashes are due to driver distraction and abnormal conditions. Hence, by adopting WSNs, an efficient identification of a driver's health condition and related emergency situations can mitigate the occurrence of traffic accidents. This implies that the adopted WSN should be capable of immediate packet processing and delivery for the entire emergency bionic conditions to prevent critical accidents.

Second, in addition to the low latency transmissions, the emergency information should be accurately and reliably delivered to the target system in order to prevent unexpected packet losses and misleading responses. Furthermore, the loss of the primitive data packet requires an additional network delay for the connection recovery, which may not mitigate the vehicular accidents.

Third, damages due to vehicular accidents are generally more serious in high speed driving compared to driving in compliance with speed limits. Therefore, in high speed driving, the emergency data should be delivered to the destination more promptly and reliably than other calm driving modes.

Finally, the evocation of immoderate prioritized channel access for emergency traffics may cause a monopoly problem among multiple traffics. Because of the limited channel capacity, mixed traffics can arouse severe channel contentions and packet collisions, which eventually degrade the overall network performance and negatively affect vehicle and driver's safety. Thus, each data traffic needs to find a suitable compromising mechanism for stable channel maintenance between contending nodes.

To address these problems, we propose a new protocol, called emergency adaptive communication protocol (EACP), which periodically monitors the emergency data packet and provides prioritized processing services to ensure successful delivery in a timely and reliable manner. The proposed protocol is based on the cross layer approach. Hence, it provides optimal route establishments at the network layer and allows the node to dynamically participate in the channel contention regarding the data emergency at the media access control (MAC) layer.

This paper is organized as follows. Section 2 provides a brief overview of related researches on conventional QoS support protocols for WSNs. Section 3 describes the proposed protocol in detail and Section 4 presents the performance evaluation of the proposed protocol using various performance metrics. Finally, concluding remarks and future work are provided in Section 5.

2. Related Work

2.1. MAC Protocols for Service Differentiation. In the last decade, the pioneering MAC protocols such as SMAC [2], BMAC [3], TMAC [4], and IEEE 802.15.4 [5] were widely adopted to deploy the WSN based applications. Although these primitive schemes achieve long term fairness among the neighboring nodes that try to access the shared channel, they do not focus on designing service differentiation for emergency packets. Therefore, a number of QoS aware protocols have been proposed in WSNs. The optimized priority assignment mechanism (OPAM) [6] proposed a QoS provision scheme for medical grade packets by introducing an adaptive scheduling algorithm. It exploited a packet classifier to assign data levels and continuously monitored the packet priorities. However, such monitoring operations were considered as a burden to the resource limited sensor nodes. In U-MAC [7], the sensor nodes that generated emergency health data were given higher priority by avoiding the packet retransmissions of nonemergency data. However, this protocol did not accurately define the QoS metrics such as network delay and reliability when determining the information emergency. The authors in [8] proposed another reliable transmission protocol for emergency packets especially in congested WSNs. Each sensor node was assumed to be capable of calculating the queue length and adjusting its sending rates according to the congestion level. Although it focused on the transmission reliability in congested WSNs, it neglected to support the prioritized route discovery for emergency packet routing in multihop networks. Hybrid medium access control (HMAC) [9] was defined as a combined protocol for carrier sense multiple access (CSMA) and time division multiple access (TDMA) approaches. When a node with delayed sensitive data wanted to access the channel, HMAC reserved a channel with high-priority assignment. Then, it reduced possible queuing delay. However, this scheme strictly required precise time synchronization between the neighboring nodes, which was a computational burden to WSNs. In our previous work [10], using the cross-layer channel access and routing (CCAR) protocol, we introduced a QoS factor to monitor the channel condition and provide differentiated channel access at both network and MAC layers. Although it provided adaptive backoff tuning operations according to the QoS level, it did not exploit the vehicular features such as vehicle's velocity and acceleration during data transmission. In Section 4, we plan to conduct simulations and compare the proposed protocol with the CCAR to identify its performance.

2.2. Routing Protocols for Service Differentiation. Since conventional on-demand routing protocols such as AODV [11] and DSR [12] were not aware of the priority level of the data packet, extensive research efforts have been devoted to provide service differentiated routing methods over resource limited WSNs. AQOR [13] was one of the well-known QoS aware protocols that computed the available bandwidth and end-to-end delay per flow QoS requirement. In addition, other enhanced routing protocols [14–16] that dealt with QoS services have explored various routing metrics such as interference, power consumption, and traffic levels. However, they were generally operated in wireless local area network (WLAN) environments such as IEEE 802.11 DCF and IEEE 802.11e, which was not directly applicable to WSNs. There were a number of location based routing protocols to improve the service differentiations. Localized multiobjective routing (LOCALMOR) [17], SPEED [18], and MMSPEED [19] were a few examples where they generally assumed that each node could acquire its position information and forward the emergency packet to the neighboring location with the minimum distance and latency. Although they could calculate the location information in a timely manner, the management and cost overhead to maintain location-assisted devices such as a global positioning system (GPS) was still a potential burden to the sensor node. The CCAR [10] also proposed a priority aware routing scheme with an efficient MAC algorithm. In CCAR, the measured QoS factor of each node was employed to reflect the degree of emergency and congestion level during the route discovery procedure. However, it did not consider how long the emergency packet traveled from source to destination during the routing process. Thus, it might suffer from significant packet losses especially in high propagation delay environments.

In this paper, to overcome the aforementioned problems, we propose a combined routing and channel access protocol to support emergency data transmissions over WSN based vehicular applications.

3. Emergency Adaptive Communication Protocol

3.1. Overview. In general, the conventional IEEE 802.15.4 standard uses the CSMA/CA channel access mechanisms

where all sensor nodes should contend for the wireless medium with equal opportunities. Although it provides long term fairness among all neighboring nodes, it does not guarantee emergency data transmissions in situations with high possibility of vehicular accidents. To resolve this problem, emergency adaptive communication protocol (EACP) is proposed by introducing a new dynamic channel access scheme according to the degree of data emergency. The EACP defines a noble data emergency factor called EF(i) at every data packet i, which is represented as follows:

$$\mathrm{EF}(i) = \frac{D^i_{\mathrm{cur}(t)}}{D_{\mathrm{avg}(\theta,t)}} + \frac{J^i_{\mathrm{cur}(t)}}{J_{\mathrm{avg}(\theta,t)}} + \frac{V^i_{\mathrm{cur}(t)}}{V_{\mathrm{avg}(\theta,t)}}, \quad (1)$$

where $D^i_{\mathrm{cur}(t)}$ is the accumulated packet delivery delay between the source node and current relaying node, which are located in the identical routing path at current time t. $D_{\mathrm{avg}(\theta,t)}$ is the average packet delivery delay among currently neighboring nodes during the predefined period θ, that is, $[t-\theta, t]$. Thus, the value of $D^i_{\mathrm{cur}(t)}$ divided by $D_{\mathrm{avg}(\theta,t)}$ represents the delay performance ratio to calculate EF(i). Furthermore, $D^i_{\mathrm{cur}(t)}$ is concretely calculated using the following expression:

$$D^i_{\mathrm{cur}(t)} = D^i_{\mathrm{sense}} + D^i_{\mathrm{queue}} + D^i_{\mathrm{backoff}} + D^i_{\mathrm{trans}} + D^i_{\mathrm{prop}}. \quad (2)$$

In this equation, D^i_{sense} denotes the sensing delays in packet i for the emergency data acquisition and includes both measuring and urgency estimating delays. Although the measuring delay requires relatively short latency to abstract the raw data value from the sensor device, the urgency estimating delay highly depends on the medical decision methods and it may take more time than a simple measuring process. For example, the measurements of body temperature and blood pressure are obtained in a short time and are typically consistent values. Meanwhile, the measurements of electroencephalography (EEG), electrocardiography (ECG), or heart rate to make decisions for abnormal conditions cannot be obtained immediately and they are considered as variable values depending on medical applications. Thus, it is important to identify both sensing delay factors in order to support emergency data traffics. D^i_{queue} denotes the packet queuing delay which is the time a packet waits in a node's queue until it can be transmitted, D^i_{backoff} is the backoff delay for wireless medium competition between neighbors, and D^i_{trans} is the transmission delay which is the amount of time required to forward all of the packet's bits and is calculated using the number of bits divided by bits per second. D^i_{prop} denotes the propagation delay over the physical channel and it is the amount of time required for the physical signal of the packet to travel from the sender to the receiver. Although all these delay factors can significantly affect the network performance, the sensing, queuing, transmission, and propagation delay factors are considered to be consistent when all sensor nodes are assumed to have identical network interfaces and processing capacity. Therefore, other delay factors such as queuing and backoff delay should be carefully investigated when dealing with the transmission of emergency data packets.

Another main evaluation component for EF(i) is the packet journey ratio that consists of $J^i_{\mathrm{cur}(t)}$ and $J_{\mathrm{avg}(\theta,t)}$. $J^i_{\mathrm{cur}(t)}$ denotes the degree of packet's journey through the route between the source node and current relaying node at the current time t and its calculation details are shown as follows:

$$J^i_{\mathrm{cur}(t)} = J^i_{\mathrm{hops}} + J^i_{\mathrm{retry}}, \quad (3)$$

where J^i_{hops} and J^i_{retry} denote the number of journey hops for packet i from the source node and the number of retrials to successfully forward the packet after it detects transmission failures at the MAC layer, respectively. $J_{\mathrm{avg}(\theta,t)}$ indicates the average degree of journey packets among currently neighboring nodes during the period θ. These two metrics represent the duration that the data packet has traveled and suspended along the route; therefore, when the calculated journey ratio is high, it should be dealt with higher emergency priority than others. Hence, when the packet is dropped or undelivered, the network delay is significantly increased for retransmitting the relayed packets. This increases the possibility of the occurrence of vehicular accidents due to delayed responses.

The other component for EF(i), $V^i_{\mathrm{cur}(t)}$ divided by $V_{\mathrm{avg}(\theta,t)}$, is the velocity ratio of the vehicle, where $V^i_{\mathrm{cur}(t)}$ denotes the vehicular velocity at the current time t and $V_{\mathrm{avg}(\theta,t)}$ denotes the average vehicular velocity during the period θ. Typically, it is important to note that the emergency data packet should be delivered with high priority during high velocity situation because an abrupt acceleration may increase the vehicular accident rate.

Meanwhile, in order to accurately calculate the EF(i) value and determine the average factors such as $D_{\mathrm{avg}(\theta,t)}$, $J_{\mathrm{avg}(\theta,t)}$, and $V_{\mathrm{avg}(\theta,t)}$, each node should investigate the data priority of neighboring nodes. Thus, each node defines and maintains a neighbor emergency table (NET) that includes the following information set:

> {Neighbor ID, Neighbor's Emergency Flag, Neighbor's $D_{\mathrm{avg}(\theta,t)}$, Neighbor's $J_{\mathrm{avg}(\theta,t)}$, Neighbor's $V_{\mathrm{avg}(\theta,t)}$, and T_{EX}}.

The NET is periodically updated with recent information whenever it receives or overhears beacon frames from hop neighbors. As shown in Figure 1, the beacon frame also contains the average delay, journey, and velocity factors of the node.

The other information field of the NET is T_{EX}, which indicates the expiration time of each data entity. If the timer is expired, the node regards the entity as stale information and immediately removes it from the table.

3.2. Proposed Routing Scheme. The main contribution of the proposed protocol is to guarantee emergency data transmissions for prioritized packets in order to mitigate the vehicular accidents due to the driver's abnormal physical conditions. Although the diagnosis of personal health condition is one of the most important issues, the proposed protocol assumes that each sensor device for driver's health or distraction monitoring accurately decides whether the measured data is currently a normal or abnormal condition for safe driving. After

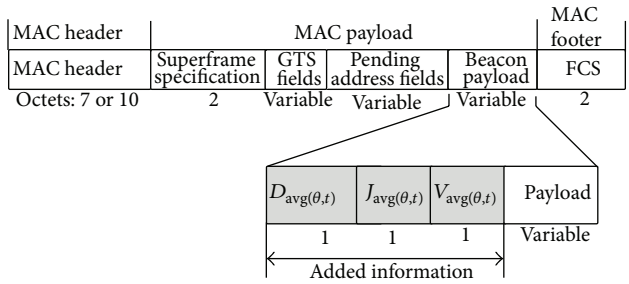

Figure 1: Beacon frame structure.

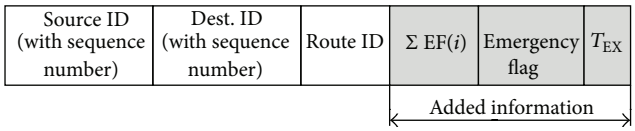

Figure 2: RREQ packet structure.

Table 1: Adaptive backoff for data packet.

Type	Adaptive backoff
Emergency data	If $((2^{MinBE} - 1) - EF(i)) > 0$ Adaptive Backoff = $(2^{BE} - 1) - EF(i)$ Else Adaptive Backoff = 1 macMaxCSMAbackoff = macMaxCSMAbackoff + EF(i)
Best effort data	Default backoff

Sacrifice data	Adaptive Backoff = $(2^{BE} - 1) + EF(i)$
	If (macMaxCSMAbackoff − EF(i)) > 0
	macMaxCSMAbackoff =
	macMaxCSMAbackoff − EF(i)
	Else
	macMaxCSMAbackoff = 1

the system identifies such abnormal condition, it is required to transmit the urgent packet as soon as possible through the network. Therefore, the proposed protocol simultaneously provides both routing and MAC schemes which are tightly coupled for data communication efficiency. To support the routing level, EACP attaches additional information to the route request (RREQ) packet header to indicate such an emergency condition if the sensor node detects any abnormal values. The designed header structure is shown in Figure 2.

As shown in Figure 1, one of the main functional superiority aspects of the proposed scheme is the fact that a data route is established to minimize the unnecessary network delay and provide prompt delivery to the destination nodes. That is, EACP chooses the route with the lowest EF values among all candidate routes while the conventional on-demand routing protocols merely pursue the shortest route without considering the data emergency. The detailed expression is shown as follows:

$$\min_{R} \left[\sum_{i \in R} \mathrm{EF}(i) \right], \tag{4}$$

where R is a candidate route and consists of multiple intermediate nodes ($R = \{N_0, N_1, \ldots, N_n\}$). Here, N_n depicts the nth node along the route R. Although the source node may have several candidate R routes to the destination, the route with minimum delay and high reliability is selected. First, to discover such candidate, the source node measures its EF(i) and broadcasts the RREQ packet as described in Figure 1. Then, every neighboring node accumulates its own measured EF value to the received instance from the previous node and performs rebroadcasting until it is delivered to the destination.

In addition to the accumulated EF(i), a source node defines and inserts emergency flag bit onto RREQ to reserve the channel by indicating that the data packet of the source node contains emergency data when the bit is set to "1". After finishing the route establishment process, this flag will enable all intermediate nodes along the route to locally adjust their backoff parameters during the medium access time. This reserved channel access will be released when a node receives a new RREQ packet with a clear flag bit (e.g., "0") or a predetermined timer (T_{EX}) expires.

Finally, once the destination receives multiple RREQs through multiple candidate routes, it chooses the optimal route and replies with the route reply (RREP) packet via the established route, which is a similar operational flow with an ordinary on-demand routing method. However, during the route discovery procedure with RREQ flooding, the proposed protocol intentionally prohibits intermediate nodes to perform proxy responses with the RREP packet using their own route cache, because all RREQ packets have to be delivered to the destination to check the emergency factors of the entire route. Although the route cache reply of the intermediate node can mitigate the route discovery latency, it has disadvantages because the route obtained from the route cache may be stale, especially when the positions and channel status of nodes are frequently changed. This may significantly result in additional network delay due to route failures and repeated attempts of the route discovery process. Thus, the suppression of RREP packets from intermediate nodes can help the source node to obtain newer and more accurate route information.

3.3. Proposed Channel Access Scheme. As mentioned in the previous section, the source node can establish the optimal route with the lowest EF values. However, in order to transmit the data frame through the medium, each intermediate node cannot help suffering from channel access delay at the MAC layer. Furthermore, the conventional MAC protocols merely compel every node to contend with neighbors without providing any prioritized access mechanisms for emergency traffics. To tackle this problem, EACP suggests an emergency adaptive backoff tuning scheme according to each packet priority level as shown in Table 1.

The emergency data type depicts the most important data packet that requires to be transmitted more promptly and reliably compared with the other packets in order to

prevent severe vehicle accidents. Expression (2) represents that the backoff operation is one of the major delay factors at the MAC layer. Therefore, EACP uses a new adaptive backoff value when the emergency packet i accesses the channel with higher probability by subtracting EF(i) from the default backoff value. In addition, the emergency packet has more retransmission opportunities compared with others by adding EF(i) to the existing macMAXCSMAbackoff which denotes the maximum number of backoff attempts before declaring a channel access failure. It should be mentioned that the packet with higher EF value should be treated with higher priority than others, because it has experienced a higher network delay and longer journey distance.

The best effort data represents nonemergency data traffic and its backoff operations are identical to those of the conventional IEEE 802.15.4 standard. Finally, the basic operation of sacrifice data is that its packet transmission is intentionally suppressed by providing opposite operations compared with the emergency traffics. Because the network bandwidth resource is strictly limited, the unreciprocated prioritized channel access of the emergency packet may result in severe packet collisions and link failures especially when the network encounters burst traffics at a certain period. To mitigate such conditions, EACP suggests that a node with the best effort traffic immediately changes its data transmission policy into sacrifice data if it detects any neighbors with emergency flag in the NET as described in previous section.

Although the complementary operations between emergency and sacrifice data provide the prioritized channel utilization, some packets will be dropped because of the limited queue length and channel capacity. In conventional First-In-First-Out (FIFO) queue, all packets are placed in a single queue and processed in the same order in which they arrived. When a buffer overflow occurs, the node drops the newly arrived packets at the queue and this is called a drop tail method. However, this simple method does not provide differentiated packet scheduling service and some heavy flow can consume the entire queue space. Since this drawback can result in severely increased delay, jitter, and packet loss of emergency data, EACP suggests a new packet drop policy as follows.

(i) All packets are classified into three classes and are separately enqueued according to the NET and upper layer as shown in Figure 3.

(ii) When a buffer overflow occurs, nonemergency packets are immediately dropped regardless of their arriving sequences. Although the nonemergency packet may suffer from starvation problem [20], the purpose of EACP is to guarantee the successful delivery of emergency packet for the vehicle safety.

(iii) If all remaining packets are emergency data, the packet with lowest EF value is the first to be dropped.

4. Performance Verification

To validate the performance of our proposed protocol, we undertook experimental evaluation via the ns-2 simulator [21].

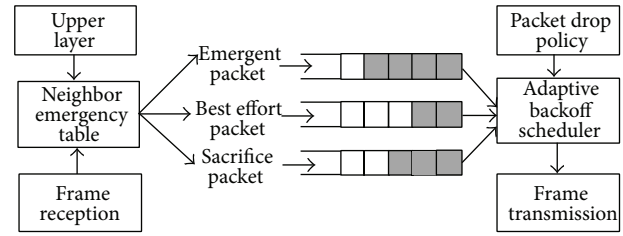

Figure 3: Structure of the proposed MAC module.

All the performance results are an average of five different simulation trials. The proposed EACP protocol is compared with the CCAR, which is another QoS provisioning protocol as mentioned in Section 2. The target network is configured with 150 nodes that are randomly placed in a rectangular place of 100 m × 100 m. We assume that all sensor nodes are capable of routing and have identical specifications regardless of their assigned role. All nodes are assumed to be located in a vehicle, which can accelerate to 100 km/h in a predefined period θ. The radio propagation range and the interference range for each node are set to 9 m and 18 m, respectively. The packet length is set to 50 bytes, and the total number of data connections between the source and destination is set to 30 (emergency connections: 10, non-emergency connections: 20). All source nodes are assumed to generate a user datagram protocol (UDP) packet with constant bit rate (CBR) traffic instead of a transmission control protocol (TCP) packet because TCP may perform its additional congestion control operations, which make it difficult to investigate the results of the actual network delay. For the network traffic variation, the degree of packet journey, that is, the sum of packet traveled hops and retransmission attempts, is used by configuring the range from 5 to 12. In our experiments, the maximum queue length of the node is set to 50. This means that it will be faced with buffer overflows if the node receives more than 50 requests. The θ and T_{EX} used to calculate the EF value are set to 10 s, which is the general timeout value to maintain the route information according to our previous work [22]. Although the dynamical tuning method for θ may somewhat affect the overall performance of the proposed protocol, it is beyond the scope of this paper.

In the simulation study of the proposed protocol, we explore the following three performance metrics.

(i) Number of dropped packets: this is the total number of dropped packets due to link failures, buffer overflows, and collisions during the simulation periods. This parameter identifies whether the target protocol is reliable to transmit and receive data. Dropping of packets acts as an implicit signal that the network is congested or broken. Thus, in order to detect such packet losses and diagnose the network reliability, the number of dropped packets should be monitored.

(ii) End-to-end packet delivery ratio: this is the average number of data packets that are actually received by the destination node over the number of data packets originated by the source nodes. This parameter

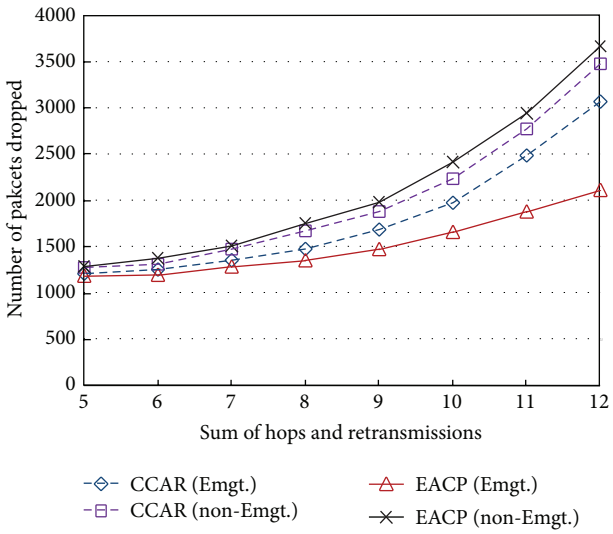

Figure 4: Number of dropped packets.

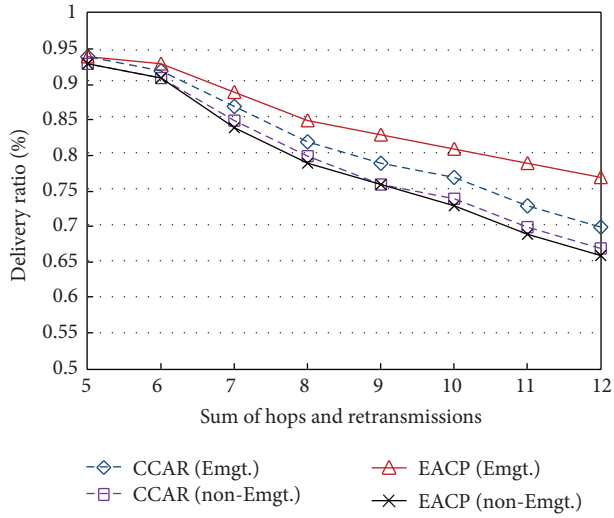

Figure 5: Delivery ratio.

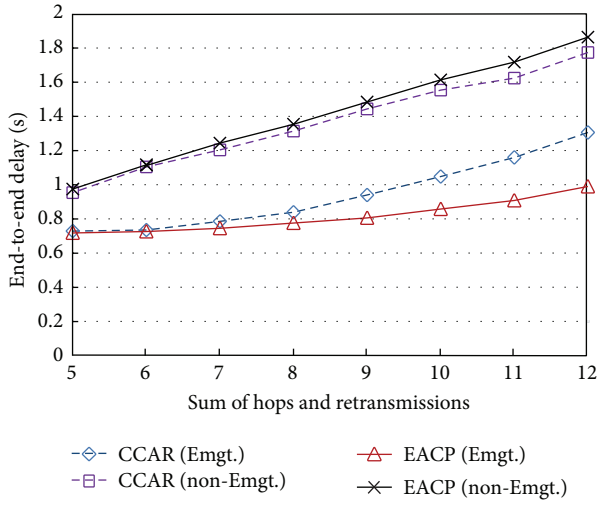

Figure 6: End-to-end delay according to the packet journey degree.

illustrates the level of successfully delivered data to the destination. In general, because the higher value of delivery ratio means a better performance from the protocol, this parameter should be monitored for the performance validation.

(iii) End-to-end delay: this is the average time that elapses from the time a data packet is transmitted by a source node to when it is successfully received by the destination node. This parameter is calculated between synchronized source and destination nodes in order to identify the acceptable delivery latency to ensure the QoS requirements of user applications (e.g., driver's preference or request).

Figure 4 describes the number of dropped packets during the simulation as a function of the sum of the traveled hops and retransmission attempts. This figure represents the degree of unsuccessful packet delivery, which is significantly related to the vehicle safety because of the loss of emergency data. For all kinds of data traffics, it was observed that the number of dropped packets was significantly increased as the packet traffic degree increased. This happened because the possibility of packet loss (e.g., collision, congestion, route failure, and physical channel error) increased as the packet traveled longer. In this figure, it can be observed that the nonemergency data traffic suffers more from packet losses than emergency traffic because each QoS aware protocol can provide nodes with differentiated packet treatments among traffics. However, it is important to note that the emergency traffic with EACP showed less packet losses compared with the traffic with an existing CCAR. This showed that EACP reflected the packet journey factor while CCAR only considered the network congestion status during the excursion of emergency packets. Meanwhile, in case of nonemergency packets, the traffic with EACP showed slightly more packet losses compared with the CCAR traffic. It was realized that when the clear channel assessment (CCA) operation of the node failed, EACP allowed the emergency packet to acquire more retransmission opportunities instead of merely dropping the packet. In addition, the nonemergency traffic provided more sacrifices than the CCAR when it performed the dynamic backoff tuning. Although it was considered as a trade-off relationship between two traffics, the reliable delivery of the emergency packet was more important to provide overall safety especially in vehicles with high velocity.

Figure 5 illustrates the end-to-end packet delivery ratios of the CCAR and EACP data flows that consist of emergency and nonemergency data packets. Although all data flows showed similar performance in shortly traveled situations, the performance gap was sharply increased as the degree of packet journey increased (see Figure 4). That is, when more nodes experienced packet losses, fewer nodes achieved packet delivery ratio.

In Figure 6, the end-to-end delay performance is described as a function of the degree of the packet journey.

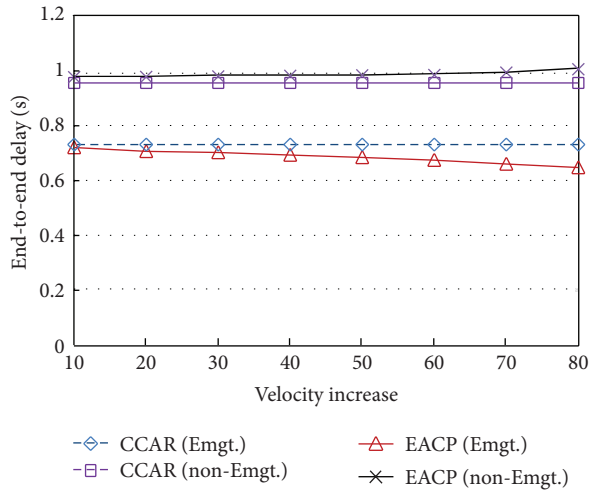

Figure 7: End-to-end delay with respect to the velocity increase.

As explained in previous figures, the emergency traffic of EACP showed better end-to-end delay performance than that of CCAR because EACP guaranteed more prompt channel accesses than other traffics by shrinking the backoff slots especially when the packet experienced a long journey. In addition, the proposed queue scheduling method mitigated the packet delivery delay while the nonemergency traffic relatively suffered from more frequent packet drops at the queue. Meanwhile, although CCAR could mitigate the network congestion and provide relatively prompt packet transmissions compared to nonemergency traffics, it did not efficiently cope with data losses of long traveled packets, which required additional invocation of the route rediscovery procedure and eventually increased the packet end-to-end delay.

Figure 7 shows the end-to-end delay performance as a function of vehicle accelerations to identify the effects of the velocity ratio parameter. As we assumed that the higher velocity increase means the vehicle encounters higher level of emergency, EACP provided improved end-to-end delay while the data traffics with CCAR were unchangeable. Thus, it can be realized that EACP was more suitable to provide vehicle safety than the other protocol especially under the high acceleration situations.

However, the proposed protocol had some disadvantages compared with existing protocols. As shown in all simulation results, there were few performance enhancements especially when the degree of packet journey was less than five. This means that the network does not have to adopt EACP instead of conventional protocols over WSNs with simple and sparse network topology. Furthermore, in such uncomplicated networks, the proposed protocol may suffer from unexpected performance degradations because of computational overheads for unnecessary network operations. Further research on the performance weakness and its countermeasures are part of our future work.

5. Conclusion

In WSN based driver's bionic data monitoring systems, there are multiple and different sensing data units to support vehicle safety. However, because of the limited channel capacity, some emergency data packet may not be delivered to the destination node in a timely and reliable manner. In this paper, we proposed a new emergency traffic aware communication protocol termed EACP to provide a more reliable and prompt packet delivery for emergency data in vehicular environments. Based on predefined data emergency factors, which included packet delay, journey, and velocity degrees, EACP could establish an efficient routing path for emergency packets during the route discovery process. Then, it performed adaptive backoff operations for each data traffic according to its emergency level. EACP allowed the emergency traffic to have relatively short backoff delay and more retransmission attempts compared with nonemergency traffics. In addition, a novel scheme for separated queue management and drop policy was proposed to improve the successful delivery in traffic concentrated situations. We used simulation to evaluate the performance. It was revealed that EACP for emergency data traffics performed better than the existing CCAR especially when the packet experienced a long journey.

As part of our ongoing research, we plan to study and test other QoS operations for vehicle and driver's safety. Moreover, we will consider possible ways to reduce the computational overheads in multihop forwarding.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by Daegu Gyeongbuk Institute of Science and Technology (DGIST) and was funded by Ministry of Science, ICT, and Future Planning (MSIP) of Korea.

References

[1] J. C. Stutts and W. W. Hunter, "Driver inattention, driver distraction and traffic crashes," *ITE Journal*, vol. 73, no. 7, pp. 34–45, 2003.

[2] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493–506, 2004.

[3] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 95–107, November 2004.

[4] T. V. Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proceedings of the International Conference on Embedded Networked Sensor Systems*, pp. 171–180, November 2003.

[5] Draft IEEE Std. 802.15.4; Part 15.4, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)," 2006.

[6] I. Raza, S. R. Chaudhry, S. A. Hussain, S. A. Abid, and H. Raza, "Optimised priority assignment mechanism for biomedical wireless sensor networks," *IET Wireless Sensor Systems*, vol. 2, no. 2, pp. 92–102, 2012.

[7] K. A. Ali, J. H. Sarker, and H. T. Mouftah, "Urgency-based MAC protocol for wireless sensor body area networks," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC '10)*, May 2010.

[8] L. Liang, D. Gao, H. Zhang, and V. C. M. Leung, "A novel reliable transmission protocol for urgent information in wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '10)*, pp. 1–6, IEEE, Miami, Fla, USA, December 2010.

[9] H. Wang, X. Zhang, F. Naït-Abdesselam, and A. Khokhar, "Cross-layer optimized MAC to support multihop QoS routing for wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2556–2563, 2010.

[10] Y.-D. Kim, K.-R. Cho, H.-S. Cho, and D. Kim, "A cross-layer channel access and routing protocol for medical-grade QoS support in wireless sensor networks," *Wireless Personal Communications*, vol. 77, no. 1, pp. 309–328, 2013.

[11] C. E. Perkins, E. Royer, and S. Das, "Ad-hoc on-demand distance vector routing," IETF RFC 3561, 2003.

[12] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4," IETF RFC 4728, 2007.

[13] Q. Xue and A. Ganz, "Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 63, no. 2, pp. 154–165, 2003.

[14] M. Wang and G.-S. Kuo, "An application-aware qos routing scheme with improved stability for multimedia applications in mobile ad hoc networks," in *Proceedings of the IEEE 62nd Vehicular Technology Conference (VTC-Fall '05)*, pp. 1901–1905, September 2005.

[15] Z.-K. Lee, G. Lee, H. R. Oh, and H. Song, "QoS-aware routing and power control algorithm for multimedia service over multihop mobile ad hoc network," *Wireless Communications & Mobile Computing*, vol. 12, no. 7, pp. 567–579, 2012.

[16] T. Liu and W. Liao, "Interference-aware QoS routing for multi-rate multi-radio multi-channel IEEE 802.11 wireless mesh networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 166–175, 2009.

[17] D. Djenouri and I. Balasingham, "Traffic-differentiation-based modular QoS localized routing for wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 6, pp. 797–809, 2011.

[18] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: a stateless protocol for real-time communication in sensor networks," in *Proceedings of the 23th IEEE International Conference on Distributed Computing Systems (ICDCS '03)*, pp. 46–55, May 2003.

[19] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath Multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 6, pp. 738–754, 2006.

[20] H. N. Elmahdy and M. H. N. Taha, "The impact of packet size and packet dropping probability on bit loss of VoIP networks," *ICGST-CNIR Journal*, vol. 8, no. 2, pp. 25–29, 2009.

[21] S. McCanne and S. Floyd, "NS network simulator," http://www.isi.edu/nsnam/ns.

[22] C. Richard, C. Perkins, and C. Westphal, "Defining an optimal active route timeout for the AODV routing protocol," in *Proceedings of the IEEE SECON*, September 2005.