applied sciences

MDPI

Article

Situation-Aware Survivable Network Design for Tactical Environments

Sunghwa Son [1], Gwangjin Wi [2] and Kyung-Joon Park [2,*]

[1] Samsung Electronics Co., Ltd., Suwon-si 16677, Korea; sunghwa.son@samsung.com
[2] Department of Electrical Engineering & Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu 42988, Korea; wgj2050@dgist.ac.kr
* Correspondence: kjp@dgist.ac.kr; Tel.: +82-53-785-6314

Abstract: A tactical sensor network is a representative safety-critical environment that should satisfy strict guarantee of the requirements of tactical traffic. However, because of the lack of infrastructure in a military network environment, resource constraints on wireless channel and nodes can cause problems such as network congestion and packet collision. If critical tactical data is lost or does not arrive on time, it can degrade the efficiency of military operations and even threaten the survival of soldiers. To resolve this critical issue, we propose a situational backoff reset algorithm that utilizes a quality of service (QoS) field information to determine the priority of received tactical packets and control the deferral time of low-priority traffic. From a packet routing path connectivity perspective, we propose a branch node-based routing algorithm in order to provide a resilient path by excluding the isolated single path. Our simulation results demonstrate that the proposed solution can prioritize tactical traffic from the channel preemption perspective and construct a robust end-to-end path avoiding an isolated single path.

Keywords: ad hoc network; MAC protocol; quality of service; internet of battlefield things; routing protocol

Citation: Son, S.; Wi, G.; Park, K.-J. Situation-Aware Survivable Network Design for Tactical Environments. *Appl. Sci.* **2022**, *12*, 6738. https://doi.org/10.3390/app12136738

Academic Editor: Francisco Airton Silva

Received: 20 April 2022
Accepted: 1 July 2022
Published: 3 July 2022

1. Introduction

The modern military operation environment has evolved from platform centric warfare (PCW) to network centric warfare (NCW) centered on securing information superiority through networking of all battlefield environmental elements [1]. In NCW, detection, identification, sensor, commander and shooter are networked to increase command speed and reduce the operation delay to increase the survival of soldiers. However, tactical networks have an inferior environment from a communication perspective due to the lack of infrastructure, limited network resources, intermittent connections, and packet loss due to frequent mobility and competition in crowded environments [2]. Therefore, there is a need for a reliable network system that can meet the requirements of a poor tactical ad hoc network environment to improve operational efficiency and survival of soldiers in the transition to NCW.

Recently, wireless local area network (WLAN) technology has been adopted for military applications in tactical networks [3–5]. A WLAN can operate in two modes, namely, infrastructure mode and ad hoc mode. If a WLAN operates in ad hoc mode, it does not require infrastructure; thus, the WLAN can fulfill the requirements of the tactical network. Other characteristics of WLAN such as its flexibility, autonomous, self-configuring, and adaptive nature also make it suitable for military applications. Soldiers use handheld network devices and sensors, such as Internet of Things (IoT) devices attached to them, which form network nodes.

Carrier-sense multiple-access with collision avoidance (CSMA/CA) is the most widely used protocol of the IEEE 802.11 standard for WLAN. However, all the nodes in the carrier sense range have to contend with each other because of the nature of sharing the medium.

In addition, there is no notion of priority; thus, collision is more fatal to important traffic, and there is no quality of service (QoS) guarantee. IEEE 802.11e is an amendment of the IEEE 802.11 standard that enhances the QoS for WLAN applications [6]. In IEEE 802.11e, enhanced distributed channel access (EDCA) defines the level of priority, access category (AC). It gives more chance of transmission to high-priority traffic than low-priority traffic by assigning a shorter arbitration inter-frame space (AIFS) and lower contention window boundaries for higher priority traffic. Although this conventional protocol considers QoS factors, the standard just gives relative priority, which may be insufficient for a safety-critical environment, such as a tactical network.

In a tactical network, the lack of infrastructure makes it necessary for wireless nodes to be configured in a multi-hop ad hoc network. Unlike a single-hop data transmission, the multi-hop ad hoc network has several challenges to construct reliable end-to-end paths or select the best routing path for improving network performance. Many approaches have been proposed to handle those issues [7,8]. A tactical ad hoc network requires a reliable routing protocol to transmit mission-critical data such as command and control (C2) and surveillance information. The constructed end-to-end paths have to meet the requirements of tactical traffic and must be able to rapidly handle connectivity problems under harsh environments.

In this paper, we consider two problems in order to guarantee the QoS for tactical traffic and reliable end-to-end paths in a tactical network. First, we propose a situational backoff reset algorithm. The proposed scheme uses information of the QoS control field in the packet header to figure out the priority of the received packet. Based on that information, low-priority traffic determines whether the backoff reset is operated or not. The proposed algorithm avoids collision between low-priority traffic and higher priority traffic and provides efficient channel deferral time to low-priority traffic without severe performance degradation. Second, we propose a branch node-based routing algorithm. The main difference in the proposed routing algorithm in comparison to the conventional routing algorithms is that it avoids the isolated single path. We allow duplicate control message and modify the packet format to find a branch node and select a routing path toward that node. Hence, the proposed routing algorithm provides reliable connectivity to a tactical network with the link disconnection problem. Our contributions in this paper are listed as follows:

- We design and implement a situational backoff reset algorithm for meeting the requirements of military QoS (MQoS) by adjusting a length of the AIFS for avoiding priority inversion and conducting situational backoff reset for preventing collision;
- The novel branch node based routing algorithm for providing resilient connectivity by finding the branch node, which duplicates pass through when a source-destination pair discovers several end-to-end paths, is presented and analyzed.

The remainder of this paper is organized as follows. Section 2 provides the related work of media access control (MAC) protocol and routing algorithms for WLAN. The situational backoff reset algorithm and the branch node-based routing algorithm are described in detail in Section 3. Section 4 presents simulation results and evaluates the performance of the proposed schemes in a tactical network. We conclude this paper in Section 5.

2. Related Work

The military quickly adopts WLAN and commercial off-the-shelf (COTS) devices considering their benefits in deploying networks [9–12]. There have been various studies undertaken to meet the requirements of traffic and guarantee QoS [13–15]. In particular, researchers have focused on designing a MAC protocol that minimizes the transmission delay of traffic and developing a routing algorithm to ensure network recovery because of the unstable conditions of wireless networks [16–27].

With respect to the MAC protocol, the main approaches consist of optimizing the traffic transmission delay to guarantee QoS. The authors in Ref. [16] present the enhanced collision avoidance (ECA) algorithm to enhance collision avoidance ability in a saturated

network. To avoid poor performance of binary exponential backoff (BEB), such as overlapped backoff intervals, backoff interval isolation (BII), and an improved slow decrease (ISD), an algorithm was proposed in ECA. CSMA with enhanced collision avoidance (CSMA/ECA) is proposed in Ref. [17]. A deterministic backoff is defined to traffic differentiation in dense networks without killing the throughput of low priority access categories. They show that CSMA/ECA can construct collision-free periods with improvement of an overall throughput. In Ref. [18], a backoff algorithm based on self-adaptive contention window update factor for IEEE 802.11 distributed coordination function (DCF) is proposed. An optimal contention window update factor is derived based on the theoretical analysis in different situations. The results show that the proposed algorithms outperform BEB, a multiple increase multiple decrease (MIMD) and multi-channel MAC scheme (MMS) algorithm with respect to throughput by reduction of collisions and the number of time slots per contention. To improve the packet loss rate and average delay, the channel-aware contention window adaption (CA-CWA) algorithm that adapts the contention window based on the channel status is proposed [19].

To avoid congestion and reduce the throughput problem, an adaptive virtual backoff algorithm (AVBA) is proposed in Ref. [20]. The access point (AP) generates backoff counts by AVBA, and they are sent to a synchronized centralized random backoff (CRB) node. The AVBA improves the throughput by achieving a collision-free state in comparison to the deterministic backoff algorithm. In Ref. [21], the authors present a differentiated reservation (DR) algorithm in multi-rate WLANs to improve the efficiency and fair sharing of channel resources among the contending nodes. The main contribution of the proposed algorithm is that each node sets its backoff counter as a deterministic value (DRV, deterministic reservation value) to reduce collisions. The simulation results verify that the DR algorithm significantly outperforms the legacy DCF in terms of throughput and airtime fairness. According to the existing research, most of them perform to enhance collision avoidance only without considering QoS requirements for each packet priority. However, the proposed approach is different because it provides different strategies for each priority in hierarchical structure.

With respect to routing algorithms, many studies have been conducted aiming to provide trusted link utilization and enhance network lifetime and find the optimal path. Thulasiraman and White propose an energy efficient zone routing algorithm, called EZone, for the topology control of tactical wireless sensor networks [22]. The EZone algorithm is developed based on the node die out information to increase the network lifetime. The results show that EZone algorithm offers the best opportunity to extend the tactical wireless sensor network service life while maintaining tactical control of the network. In Ref. [23], a distributed split-path routing algorithm is introduced to account for the link utilization between nodes. The scheme is designed based on the optimized link-state routing (OLSR) protocol and uses past transmission history to split the traffic into multiple paths. Simulation results show that the strategy provides a long-lasting network, while maintaining performance comparable to that of the OLSR protocol. In Ref. [24], The authors propose an energy efficient and reliable routing algorithm based on Dempster–Shafer (DS) evidence theory (DS-EERA) to achieve higher QoS. It uses DS evidence fusion rules to fuse three attribute indexes of nodes such as residual energy, traffic, and the closeness of its path to the shortest path. Using the fusion results, it selects the best next hop. Finally, each node transmits traffic through this routing strategy. However, none of the works consider link failures and environments where network topology changes.

In Ref. [25], the authors propose ad hoc on-demand multipath distance vector with the fitness function (FF-AOMDV) protocol. The FF-AOMDV uses two metrics such as the residual energy and the distance from the transmitting and receiving node to find the optimal path to reduce the energy consumption. The results demonstrate that the proposed FF-AOMDV outperforms AOMDV and ad hoc on demand multipath routing with life maximization (AOMR-LM) in throughput, packet delivery ratio, and end-to-end delay. The authors in Ref. [26] propose a topological change adaptive ad hoc on-demand multipath

distance vector (TA-AOMDV) for providing QoS in topological changing environments with high-speed nodes. In this scheme, it finds several alternative paths with better QoS performance by the alternative path selection algorithm and selects the stable path by primary path selection algorithm among the alternative path. The primary path is selected based on the Link Break Probability (LBP) and Path Stability Probability (PSP) values. Simulation results show that it can guarantee the QoS by obtaining the stable path under the dynamic topology changing networks. In Ref. [27], The authors propose a novel routing scheme named Mobility, Residual Energy, and Link Quality Aware Multipath (MRLAM). This algorithm uses a Q-learning algorithm for maintaining stability, reliability, and lifetime of the network. Through the simulation results, it performs high performance in respect to energy cost, end-to-end delay, and packet loss ratio. However, studies on providing resilient connectivity and robust end-to-end path in WLAN are insufficient. Therefore, new techniques are required to ensure the stability of network during link failure.

3. Proposed Algorithm

In this section, we describe the proposed algorithm, which comprises two parts: (i) the situational backoff reset algorithm and (ii) the branch node-based routing algorithm. The main objective of the proposed algorithms is to increase the survival in tactical networks through improvement of military operations by supporting the guaranteed delivery of important or critical messages and maintaining end-to-end network connectivity. The first scheme, the situational backoff reset algorithm, adjusts the channel access of a tactical message depending on its importance and urgency, i.e., priority of traffic. The branch node-based routing algorithm helps provide end-to-end path connectivity even in the harsh environmental conditions of a battlefield. The proposed algorithms are described in detail in the following subsections.

3.1. Situational Backoff Reset Algorithm

3.1.1. Military Quality of Service

The IEEE 802.11e EDCA is a representative standard that can improve the QoS. Generally, commercial QoS has features such that it meets performance-based requirements, static priority, and best effort service. However, these characteristics are hard to directly apply in the environment of tactical networks. In the case of MQoS, the priority may vary depending on the mission; requirements are based on importance and urgency, and MQoS should be guaranteed. The MQoS requirements defined by the U.S. Army unified capabilities (UC) reference architecture (RA) are listed in Table 1 [28]. Table 1 includes some metrics such as end-to-end delay, end-to-end packet loss, and end-to-end delay jitter, which are defined in Ref. [29]. End-to-end delay is the sum of transmission, processing, and queueing delays in routers; propagation delays in links; and end-system processing delays. End-to-end packet loss is the ratio of packets discarded or lost to total transmitted packets. End-to-end delay jitter is the variation in the delay of packets. Unlike IEEE 802.11e, in which the priority is assigned by traffic type, the priority of tactical traffic is divided into four sections based on its importance and urgency: urgent and important traffic, urgent but unimportant traffic, important but not urgent traffic, and neither urgent nor important traffic. In this work, we consider three service classes from Table 1; voice, multimedia conferencing, and short messaging.

3.1.2. The Mechanism of the Proposed Algorithm

A key feature of the situational backoff reset algorithm is illustrated in Figure 1. The basic structure of the proposed algorithm is similar to that of the commercial standard. However, the proposed algorithm has different management strategies for each priority in hierarchical structure compared to the conventional standard. The 802.11e protocol provides best effort service because it gives relative priority, which may lead to priority inversion and collisions between different priority traffic. This structure is insufficient

to transmit tactical traffic, and it raises the necessity of a new design that can guarantee appropriate priority and meet the requirements of MQoS.

Table 1. Granular service performance objectives.

Granular Service Class	End-to-End Delay (ms)	End-to-End Packet Loss (%)	End-to-End Delay Jitter (ms)
Short Messaging	1000	0.5	-
Voice (Assured/Non-Assured)	220/250	1/1	20/20
Multimedia Conferencing (Voice/Video only)	220	1	20
Broadcast Video (Voice/Video only)	1000	0.1	-
Multimedia Streaming (Voice/Video only)	250	1	20
Low Latency Data: IM/Chat, Presence	300	1	-
High Throughput Data	300	1	-

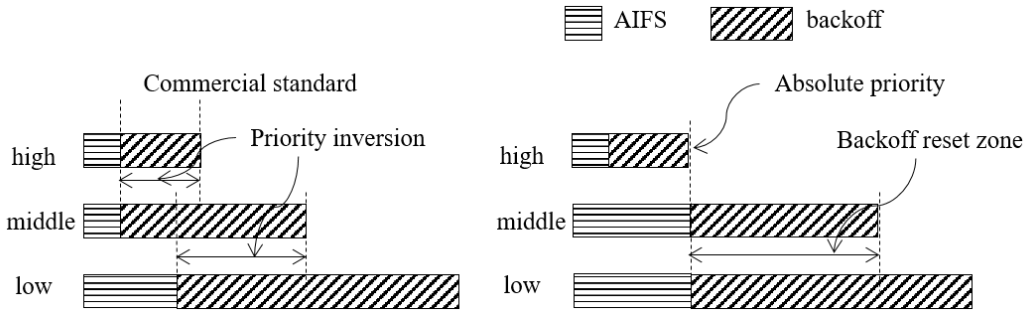


Figure 1. Conceptual comparison of IEEE 802.11e EDCA and proposed algorithm.

The proposed scheme is designed in stepwise order from high-priority to low-priority. In a tactical environment, urgent and important traffic, such as C2 communication, which corresponds to the high-priority, should be guaranteed. To address this challenge, we introduce the absolute priority scheme for high-priority traffic. The AIFS of middle-and low-priority traffic is lengthened to include the contention window size to the AIFS of the high-priority traffic. Under the proposed design, the high-priority traffic is completely excluded from channel access contention with other priority traffic as well as the priority inversion problem. Consequently, high-priority traffic is served first as an absolute priority.

As the next step to the absolute priority scheme, we propose the situational back-off reset algorithm for the middle-priority traffic. If the middle-priority traffic adopts a differentiation strategy as the absolute priority scheme does, it may obtain advantages from channel access contention but a long deferral time is ineffective, and performance degradation is inevitable. To distinguish between middle- and low-priority traffic, the low-priority traffic resets the current backoff counter when it senses the transmission of a higher priority traffic and the current backoff counter is in the range of a backoff reset zone (BRZ). We use a traffic identification (TID) value in the QoS control field as a trigger of the backoff reset. Figure 2 shows the QoS data frame structure, and the QoS control field is included in the MAC header. Accordingly, any node can access the TID value, even if the received packet is not destined to this node. As described in Algorithm 1, only in the case of a node that has low-priority traffic to transmit, it checks the condition of the TID value from the received packet and whether its current backoff counter is in BRZ or not. If the condition is satisfied, the corresponding node conducts backoff reset to prevent collision and give channel access preference to middle-priority traffic. Otherwise, that node can keep its backoff counter and transmit when it terminates backoff. In summary, the proposed algorithm effectively prioritizes traffic based on the situation-aware information without an undesirably long deferral time.

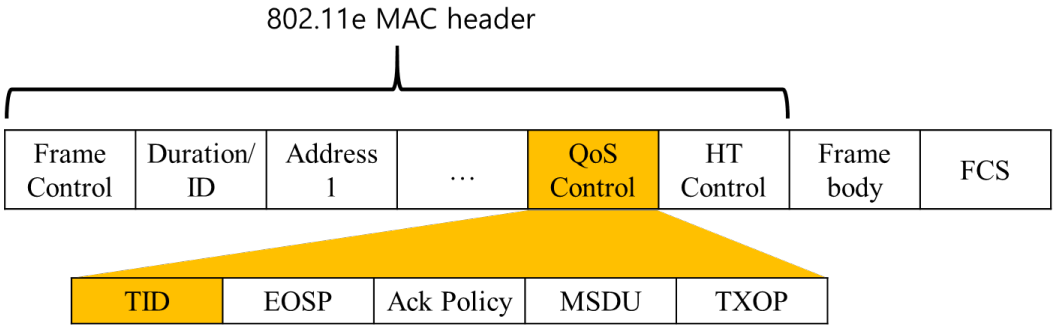


Figure 2. QoS data frame structure.

Algorithm 1 Pseudocode of situational backoff reset

```
/* High-priority has an "ac" value of 3*/
/* The length of AIFS setting */
if ac == 3 then
    AIFS[ac] = default;
else
    AIFS[ac] = AIFS[3] + CW_max[3];
end if
/* situational backoff algorithm */
/* when a node senses transmission */
tid = qos_info_ptr → tid;
recv_ac = ac_mapping_array[tid];
if (my_ac ≠ 3)&(recv_ac > my_ac) then
    if my_BC < BRZ then
        while my_BC < BRZ do
            my_BC = rand % my_CW;
        end while
    end if
end if
```

3.2. Branch Node Based Routing Algorithm

3.2.1. Branch Node Detection

The environment of a tactical network is challenging because of the absence of infrastructure, limited network resource, mobility, and network disconnection. Therefore, a reliable network system in a tactical network is essential, and a possible solution is to build a robust end-to-end path. In this subsection, we introduce the branch node-based routing algorithm, which is modified from the ad hoc on-demand distance vector (AODV) routing algorithm to cope with the network connectivity problem. Typical routing protocols search for one path that has the best performance, whereas the proposed routing algorithm investigates several paths to find the branch node. We define the branch node as a node that duplicates the pass through when a source-destination pair discovers several end-to-end paths, as shown in Figure 3. The advantage of forwarding a packet through the path that includes the branch node is that when a connectivity problem occurs on the main path, the packet can be promptly handled with an alternative path.

Before introducing the proposed algorithm, we briefly explain the process of constructing a path in the conventional AODV routing algorithm. At a node, after a packet is generated, it checks the destination address and the existence of a path to the destination. If there is no path, before transmitting the packet, the node has to construct a path by using control packets, such as a route request (RREQ) message and a route reply (RREP) message. Figure 4 shows the RREQ message format for the AODV model [30]. A source node broadcasts the RREQ message to investigate a path to reach the destination node. In the case of the intermediate nodes that are not the destination node and do not have a

path to the destination node, they re-broadcast the RREQ message and store reverse paths towards a node originating the RREQ in the route table. The destination node unicasts an RREP message in response to the RREQ message, and a forward path is set up through this process.

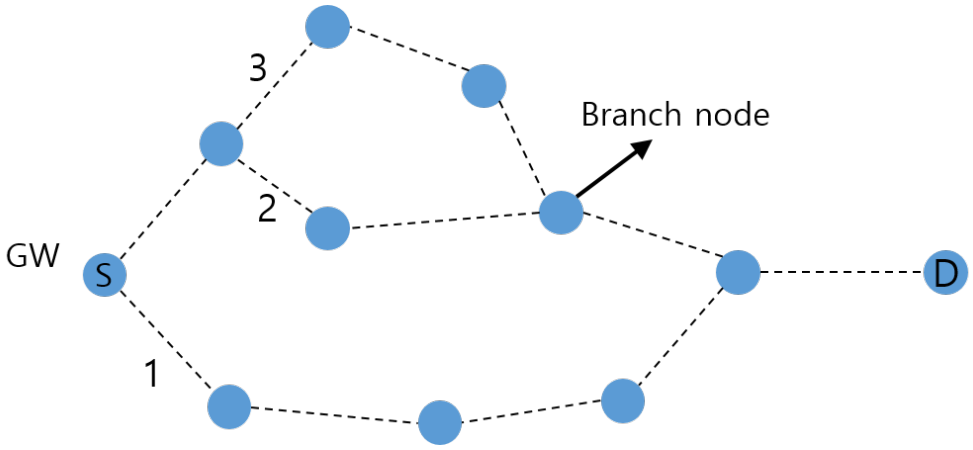


Figure 3. A branch node and the rank of each path in the network.

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Figure 4. RREQ message format.

As a first step to specify the branch node, we need to permit the receipt of multiple RREQ messages that have the same RREQ ID as that of the last received RREQ message. The source code in Algorithm 2 helps to forward the RREQ message, which should be originally discarded, and investigate the branch node. In addition, the destination node can reply in an RREP message to construct a forwarding path including the branch node by receiving multiple RREQ messages. Next, we modify the RREQ message format and add new fields, forwarder IP address and RREQ count, as shown in Figure 5. A forwarder IP address field is added to avoid loop formation, and the RREQ count field is for specifying the branch node. When a node receives an RREQ message with the same RREQ ID already stored, it increments the RREQ count value by 1 and re-broadcasts. If a node receives an RREQ message for which the RREQ count is more than 1, it means that this RREQ message has passed through the branch node. Then, that node stores the previous hop as a route table entry—next hop. The next hop information is used as the direction for forwarding a unicast RREP to build the end-to-end connection.

3.2.2. Operation Process

Figure 6 shows a simple example network to illustrate the operation process of the proposed algorithm. The branch node-based routing algorithm searches the top-k ($k = 3$ in our example) paths that meet the requirement of a tactical packet by broadcasting an RREQ message. The number on each path indicates its ranking, and the existence of the branch node in the upper side is verified by depending on the value of the RREQ count field. The nodes behind the branch node receive the RREQ message with the RREQ count value of 2; therefore, the destination node can recognize the existence of the branch node and forward

the RREP message toward it. However, in case of the conventional routing algorithm, the destination node forwards the RREP message toward the path of rank 1 because it discards a duplicate RREQ message.

Algorithm 2 Pseudocode of branch node-based routing

```
/* RREQ packet arrival part */
/* 1. Check prev_addr is my_addr */
if addr_equal(my_addr, prev_addr) == true then
    recv_pkt_destroy();
    FOUT;
end if
/* 2. Increment the RREQ count value at branch node */
/* and update route table for branch node at dest_node*/
if addr_equal(my_addr, dest_addr) == true then
    route_table_update(next_hop_addr, hop_count);
else
    if my_count ≥ rreq_count then
        rreq_ptr → rreq_count++;
        route_entry_ptr → rreq_count
        = rreq_ptr → rreq_count;
    else
        route_entry_ptr → rreq_count
        = rreq_ptr → rreq_count;
    end if
    broadcast_rreq();
end if
/* RREP packet arrival part */
/* 3. Update route table for branch node at src_node */
if (reached_src)&(rreq_count > 1) then
    route_table_update(next_hop_addr, hop_count);
end if
```

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							
Forwarder IP Address							
RREQ Count							

Figure 5. Modified RREQ message format.

The path repair process with the branch node-based routing algorithm is illustrated in Figure 7. If a node on the primary path senses that connection is lost to the next hop, it starts the route repair process. If local repair is attempted, the proposed routing scheme can easily and quickly find an alternative route near the primary path. However, in the case of the conventional routing scheme, it may fail to recover an end-to-end path with local repair because it constructs a single path. Consequently, the source has to construct a new path after it receives a route error (RERR) message. Because this takes a long time, it causes inevitable performance degradation, such as long delays or packet drop. Even if local

repair is successful, it is hard to guarantee that the new path can satisfy the requirements of tactical traffic.

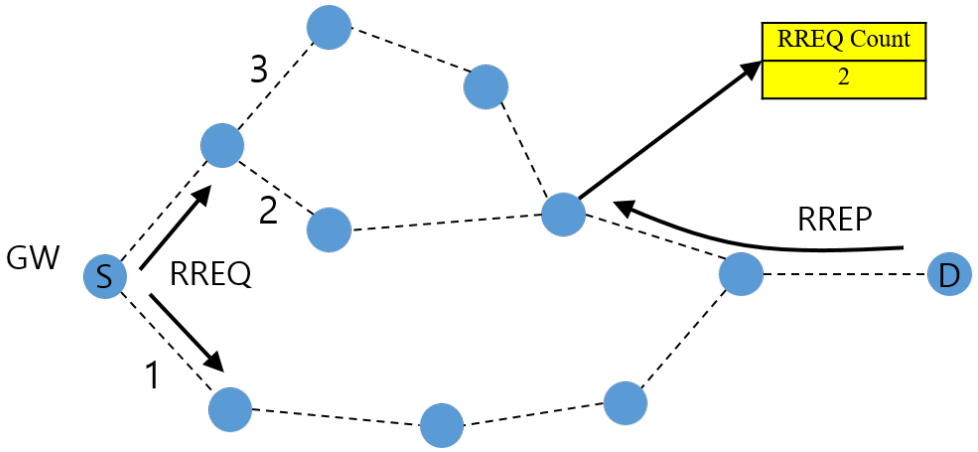


Figure 6. Routing path construction with the proposed routing algorithm.

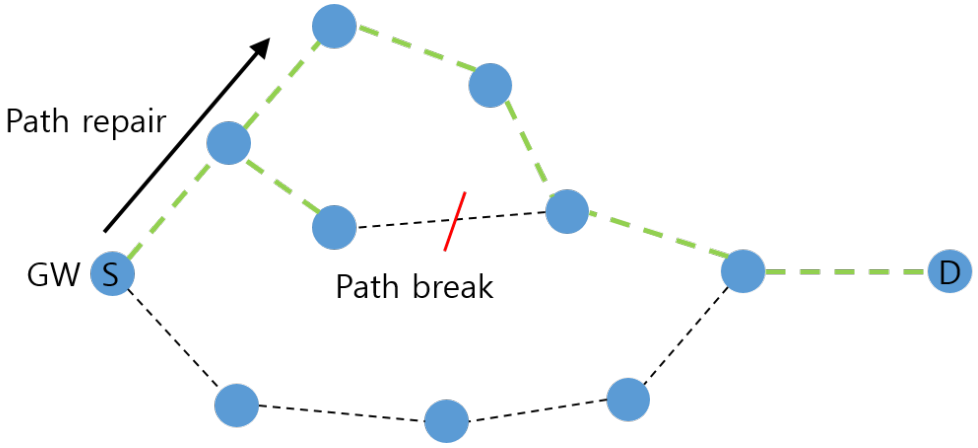


Figure 7. Path repair process with the proposed routing algorithm.

4. Performance Evaluation

In this section, we evaluate and compare the performance of the proposed algorithm and the conventional algorithm via a simulation study.

4.1. Situational Backoff Reset Algorithm

We conduct a simulation using Riverbed modeler, known as OPNET simulator [31] and set the simulation parameters as shown in Table 2. As previously mentioned, we consider three service classes, namely, voice, multimedia conferencing, and short messaging. In the simulation, voice traffic represents C2; therefore it is assigned high-priority. Video surveillance traffic is mapped to middle-priority, and data traffic, such as short messages and low-resolution images are considered low-priority. For the tactical wireless network setup, the IEEE 802.11e protocol, 1 Mbps data rate, and AODV routing protocol are used. Figure 8 shows the node configuration for that tactical network simulation. The total 15 nodes include 1 gateway node, 2 high-priority traffic, and 3 middle-priority traffic, while the rest are low-priority traffic and are distributed in an 800 m by 400 m field.

Table 2. Simulation parameters setup.

Parameters		Value
Simulator		OPNET 18.7
Simulation time		300 s
Number of nodes		15
Routing protocol		AODV
Traffic type	High	VoIP G.723.1
	Middle	Video conferencing (10 frame/s)
	Low	Short message (1000 byte/s)
MAC protocol		802.11e EDCA
Data rate		1 Mbps

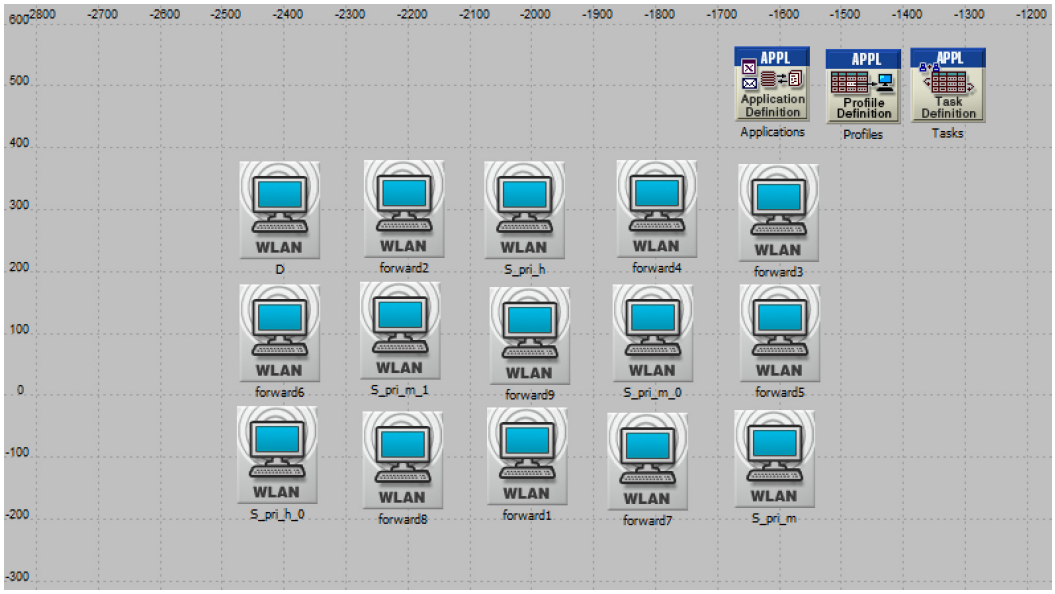
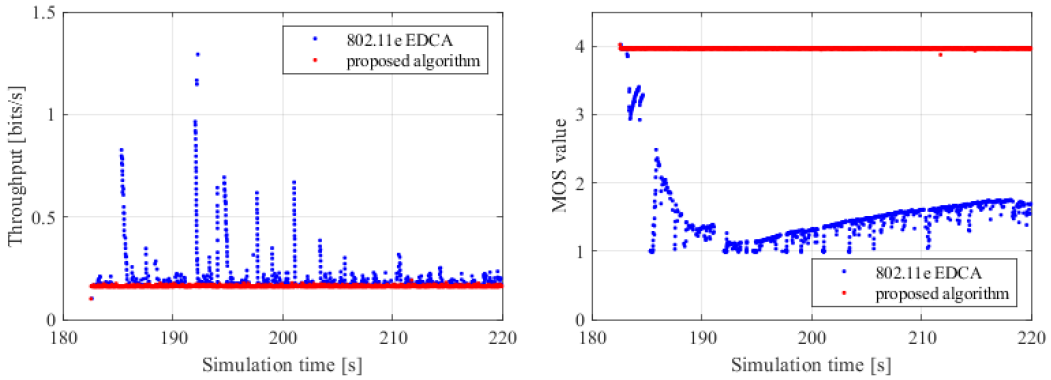


Figure 8. Node configuration in OPNET.

Figure 9a,b compares the performance of high-priority traffic for the conventional protocol and the proposed algorithm. In each figure, the blue dots show the performance of the conventional protocol, and the red dots show that of the proposed algorithm. In Figure 9a, the end-to-end delay of voice traffic is presented. With the conventional protocol, a large delay is observed occasionally, while the proposed algorithm maintains small latency because the proposed algorithm can provide absolute priority for high-priority traffic. Considering that the service performance objective for the voice is 220 ms and 250 ms, as seen in Table 1, the conventional protocol does not guarantee MQoS of the voice traffic while the proposed algorithm does. To evaluate voice traffic more clearly, we introduce the mean opinion score (MOS) [32], which is a metric related to the quality of experience (QoE), which is shown in Figure 9b. The MOS represents a quality satisfaction level from 5 to 1, and the meaning of the score is excellent, good, fair, poor, and bad in descending order. In the case of the conventional protocol, the MOS value is 4 at first; however, it decreases shortly to 1 and fails to recover in poor quality level. However, the proposed algorithm is verified to provide guarantee of absolute priority to voice traffic by maintaining an MOS value to good quality level.

As for voice traffic, we measure the end-to-end delay of a video surveillance application, as shown in Figure 10. The performance requirement for video defined by the U.S. Army UC RA is 220 ms. A node transmits video traffic during 60 s at 2 min and 40 s in simulation time. In the case of the conventional protocol, the end-to-end delay increases to 3.5 s between 190 s and 200 s, the time when the voice application is also activated in simulation time. However, the performance of the proposed algorithm does not degrade because it can avoid collisions between low-priority and higher priority traffic. Such a long

end-to-end delay as observed in voice traffic means the conventional protocol not only fails to distinguish the priority of tactical applications but also do not meet the requirements. Contrary to the poor performance of the conventional protocol, the proposed algorithm can handle video traffic without a delay problem.



(**a**) (**b**)

Figure 9. Performance comparison of voice application. (**a**) End-to-end delay. (**b**) MOS value.

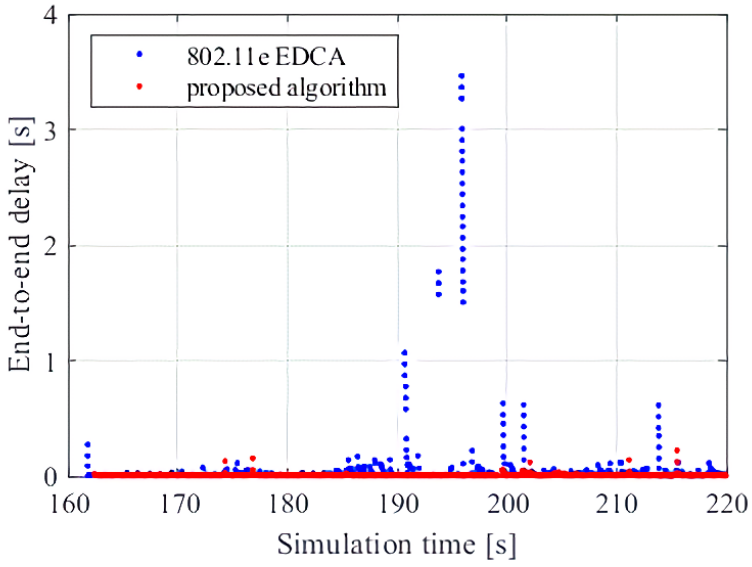


Figure 10. End-to-end delay comparison of video application.

Finally, we evaluate the throughput performance for a short message application and the total application as presented in Figure 11. Figure 11a compares the throughput of a short message, which corresponds to low-priority traffic. Compared to the conventional protocol, low-priority traffic of the proposed algorithm has relatively long channel access time, and less chance to transmit is presumed because it resets backoff when it senses higher-priority transmission. However, contrary to our expectation, the throughput of low-priority traffic in the proposed algorithm is comparable to that of the conventional protocol without severe performance degradation. This may be attributed to the fact that, with the proposed approach, the tactical traffic is distinguished well by prioritization. The conventional protocol supports a relative priority that can intensify congestion among different priorities and increase collisions, consequently. As a result, the proposed algorithm shows better performance for total throughput as seen in Figure 11b.

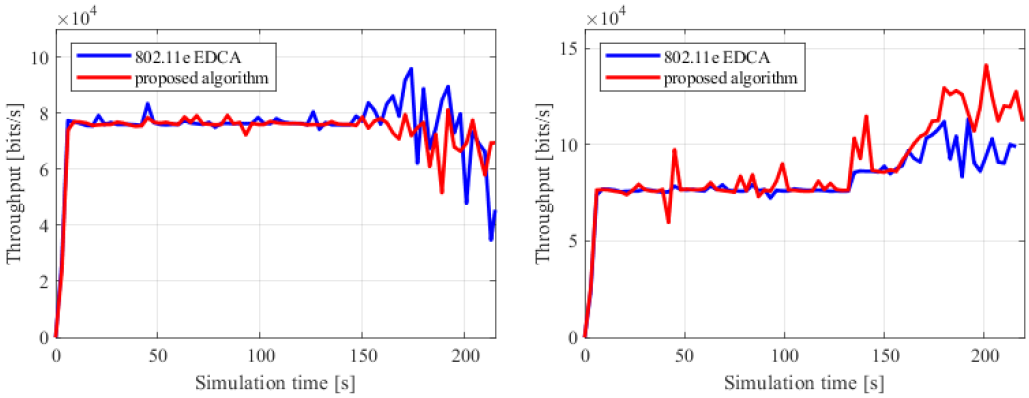


Figure 11. Throughput performance comparison. (**a**) Short message. (**b**) Total throughput.

These simulation results are used to compare the performance of the conventional protocol and that of the proposed algorithm according to the simulation time. In addition, we conduct 100 simulations and gather the results to investigate the average performance of the algorithms. The end-to-end delay distribution of voice traffic according to each simulation number is presented in Figure 12. For each simulation number, the end-to-end delay of voice traffic is plotted as a type of box plot; the upper graph is for the conventional protocol, and the lower one is for the proposed algorithm. In certain cases, we can observe a large delay for the conventional protocol, such as 21.78 s in simulation run 68 due to the fact that high-priority traffic exists longer than other simulation runs. In these two simulations, none of the voice packets are received. From these results, we can conclude that the conventional protocol is not appropriate for tactical environments and it fails to meet the required QoS level. On the other hand, however, except some simulation cases, the end-to-end delay of the proposed algorithm is small.

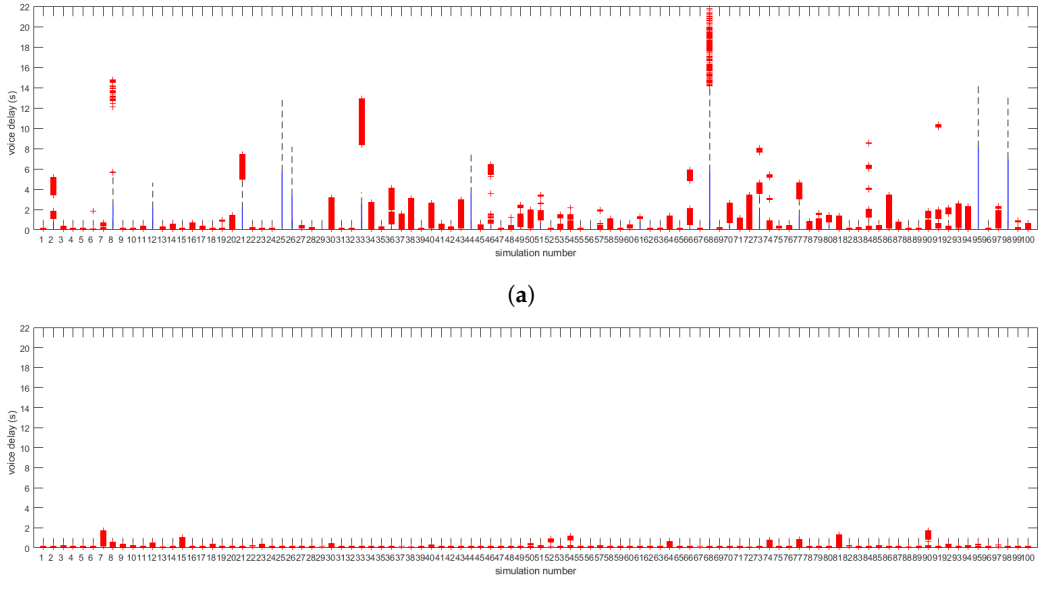


Figure 12. End-to-end delay distribution of voice traffic of 100 simulations. (**a**) 802.11e EDCA. (**b**) Situational backoff reset algorithm.

We calculate the average delay from every 100 simulations, and the cumulative distribution function (CDF) for the average delay of voice traffic is presented in Figure 13. The vertical red line is the reference line of the service performance objective for voice traffic, 220 ms, as shown in Table 1. In the CDF of the conventional protocol, about 58%

of the average delay is below the reference line (57 cases of the total 98 cases). From the total 100 simulations, 101,591 voice packets are received by the conventional protocol, and 9190 packets corresponding to around 9% are delayed. However, there is only one case with the proposed algorithm in which the average delay of voice traffic exceeds the reference line. In other words, 99% of the measured average delay is below the reference line. With the proposed algorithm, a total of 126,020 voice packets are received, and the delay of 391 voice packets, 0.3% of the received packets, exceeds 220 ms.

Figure 14 shows the end-to-end delay distribution of video traffic, measured from 100 simulations. The box plots of video traffic for the conventional protocol and the proposed algorithm have a similar aspect to the result of voice traffic. In the case of the conventional protocol, the end-to-end delay of video traffic is measured from only 66 cases among 100 simulations. Compared to the voice traffic, there are more cases that fail to receive video traffic because of the congested wireless network condition. On the other hand, the proposed algorithm receives video traffic from the overall simulations. The numbers of cases in which the delay exceeds the service performance objective are 65 out of 66 and 18 out of 100 for the conventional protocol and the proposed algorithm, respectively.

We also investigate the average delay CDF for video traffic for the two algorithms, as shown in Figure 15. In the case of the CDF graph for the conventional protocol, 68% of the results meet the required QoS for video traffic. However, if we consider 34 simulations in which none of the video packets are received, 45% from the measured average delay of video traffic is below the reference line. In 66 simulations out of the total 100 simulations, 27,142 video packets are received, and 1765 packets are received but are delayed. In the case of the proposed algorithm CDF, it meets the required QoS of video traffic in 100% of the simulations. The average video traffic of both the conventional protocol and the proposed algorithm show a relatively small delay compared to the voice traffic. This difference may be attributed to the fact that the voice traffic delay includes encoding and decoding delay. A total of 54,319 video packets are received with the proposed algorithm, and 143 packets, corresponding to 0.26%, are delayed.

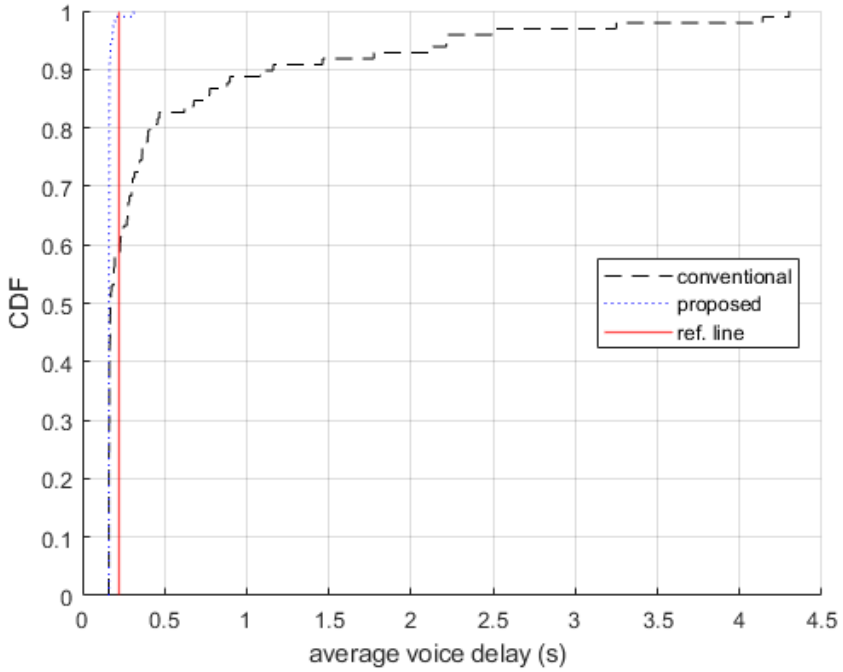


Figure 13. Average delay CDF for voice traffic of 100 simulations.

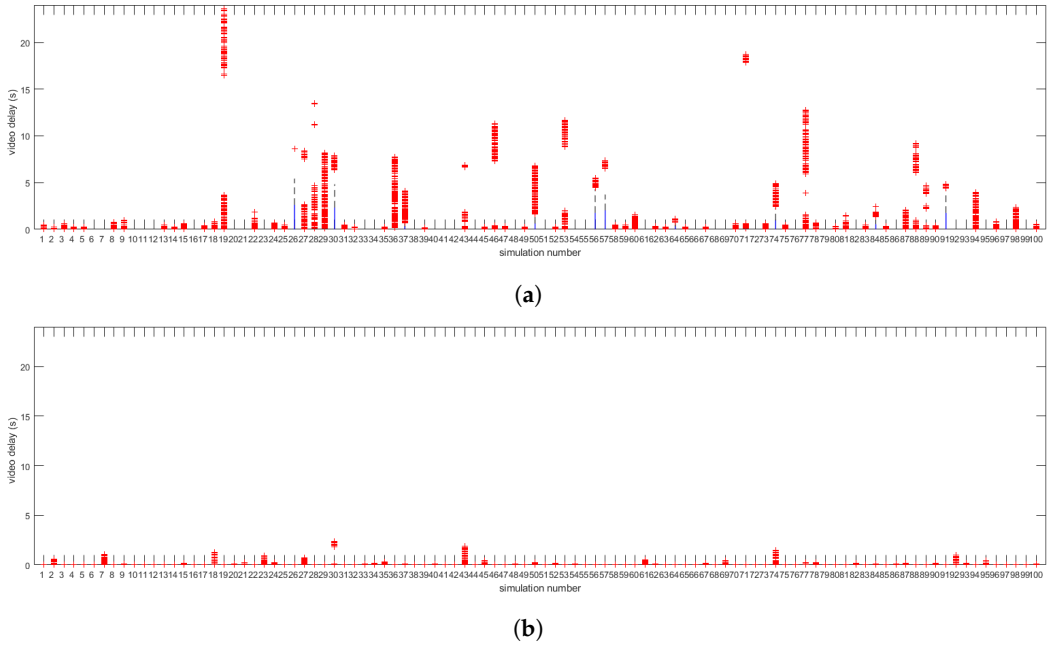


Figure 14. End-to-end delay distribution of video traffic of 100 simulations. (**a**) 802.11e EDCA. (**b**) Situational backoff reset algorithm.

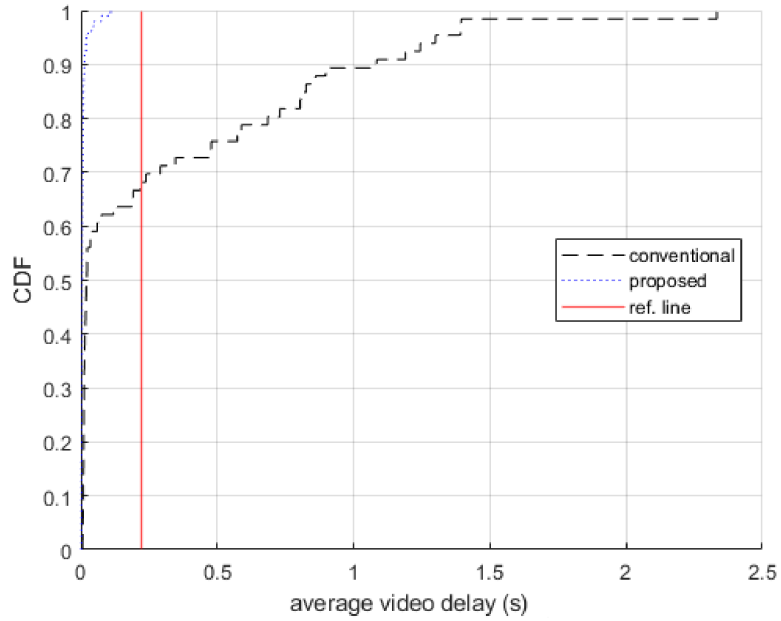


Figure 15. Average delay CDF for video traffic of 100 simulations.

4.2. Branch Node Based Routing Algorithm

We conduct a simulation study to evaluate the performance of the routing protocol in a tactical network. For the performance comparison with the proposed algorithm, we consider AODV, which is the representative routing protocol. Figure 16 shows the network configuration used for the simulation study. A total 14 nodes are distributed in a 2000 m by 1500 m space including source node S and destination node D. The branch node is positioned in the upper part of the network topology. In our scenario, we move away one of the nodes that is a part of the main route for the comparison of the network connection maintenance ability.

The results of the performance comparison of end-to-end delay for the AODV routing algorithm and the branch node-based routing algorithm are presented in Figure 17. As we mentioned in a previous section, the proposed routing algorithm constructs a path through

a branch node, and the AODV routing algorithm selects a path at the bottom of the network topology, the same path that the first RREP message passes through. In the simulation result of AODV routing algorithm, we observe that the end-to-end delay of the proposed algorithm is much lower than that of the AODV routing algorithm during 45 s to 50 s of the simulation time. The reason for increasing end-to-end delay is that when a link break occurs, there are no nodes near the main route to attempt local repair, and a substantial amount of time passes in the series of processes that forward the RERR message to the source node and discover the route at the source node. However, the proposed branch node-based routing algorithm shows quick packet forwarding through an alternative path without performance degradation.

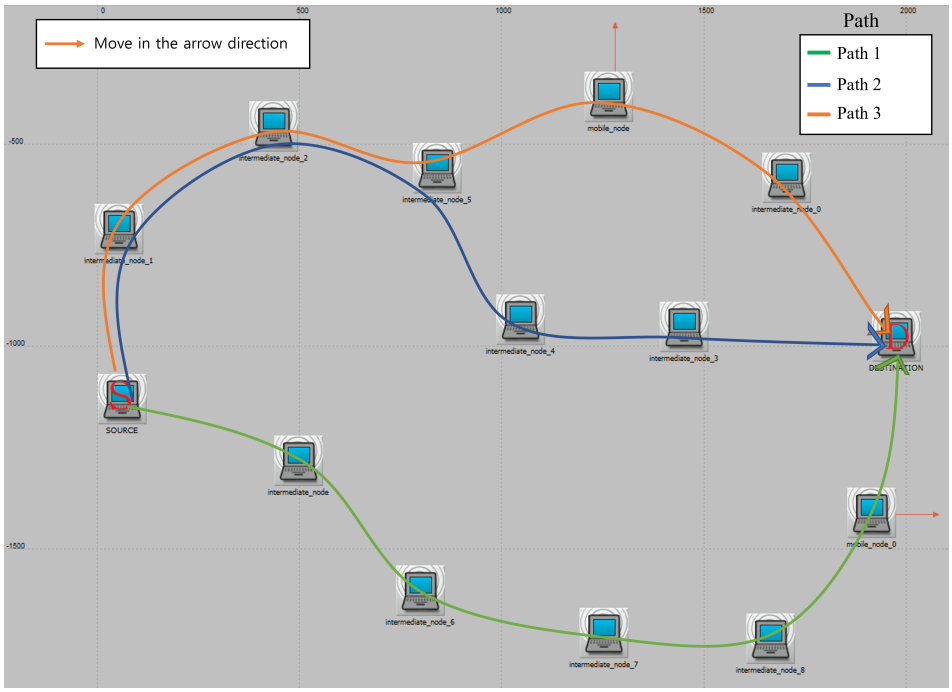


Figure 16. Network configuration for the simulation study.

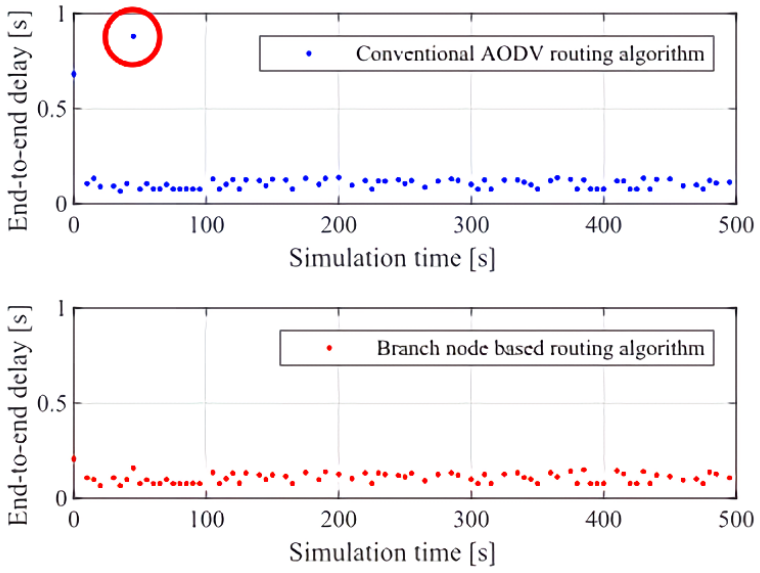


Figure 17. Performance comparison of end-to-end delay.

5. Conclusions

In this paper, we have discussed the unstable environment of tactical networks caused by the lack of infrastructure, limited network resources, intermittent connections, and frequent mobility. To overcome this problem and provide reliable communication in the military domain, we proposed two algorithms. The situational backoff reset algorithm adjusts the backoff counter value of low-priority traffic by using situation-aware information. A node, which has low-priority traffic to transmit, resets its backoff counter based on the priority of the received packet without performance degradation. The branch node-based routing algorithm avoids an isolated single path and provides resilient connectivity in the event of a link break. The simulation results indicate that the proposed algorithms outperform the conventional schemes in tactical networks. The contribution of our paper can be extended into various fields. Our research is not limited to military domains but can be applied to medical fields that require strict QoS guarantee for medical application and smart factories that require reliable communication. One possible direction of future research is to consider the timeliness of packet delivery on top of the reliability. As future work, we will extend our survivable network design to guarantee robust communication while satisfying the delay requirements of the networks.

Author Contributions: Conceptualization, S.S. and K.-J.P.; methodology, investigation, S.S. and G.W.; simulation, validation, S.S. and G.W.; writing—original draft preparation, S.S.; writing—review and editing, K.-J.P.; visualization, S.S.; supervision, K.-J.P.; project administration, K.-J.P.; funding acquisition, K.-J.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported by the Future Combat System Network Technology Research Center program of Defense Acquisition Program Administration and Agency for Defense Development. (UD190033ED).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not available due to the confidentiality issue with the funding agency.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kim, K.D.; Kumar, P.R. Cyber-physical systems: A perspective at the centennial. *Proc. IEEE* **2012**, *100*, 1287–1308.
2. Aschenbruck, N.; Gerhards-Padilla, E.; Martini, P. A survey on mobility models for performance analysis in tactical mobile networks. *J. Telecommun. Inf. Technol.* **2008**, *2008*, 54–61.
3. Crow, B.P.; Widjaja, I.; Kim, J.G.; Sakai, P.T. IEEE 802.11 wireless local area networks. *IEEE Commun. Mag.* **1997**, *35*, 116–126. [CrossRef]
4. Zhao, Q.; Du, P.; Gerla, M.; Brown, A.J.; Kim, J.H. Software defined multi-path tcp solution for mobile wireless tactical networks. In Proceedings of the MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 1–9.
5. Keum, D.; Lim, J.; Ko, Y.B. Trust based multipath qos routing protocol for mission-critical data transmission in tactical ad-hoc networks. *Sensors* **2020**, *20*, 3330. [CrossRef] [PubMed]
6. std. 802.11 e 2005, I. Wireless LAN Medium Access Control (MAC) and PHYsical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. 2005. Available online: https://standards.ieee.org/ieee/802.11e/3131 (accessed on 30 June 2022).
7. Cengiz, K.; Dag, T. Energy aware multi-hop routing protocol for WSNs. *IEEE Access* **2017**, *6*, 2622–2633. [CrossRef]
8. Zhang, A.; Sun, M.; Wang, J.; Li, Z.; Cheng, Y.; Wang, C. Deep reinforcement learning-based multi-hop state-aware routing strategy for wireless sensor networks. *Appl. Sci.* **2021**, *11*, 4436. [CrossRef]
9. Fraga-Lamas, P.; Castedo-Ribas, L.; Morales-Méndez, A.; Camas-Albar, J. Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN. In Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016; pp. 1–8.
10. Al-Shehri, S.M.; Loskot, P.; Numanoğlu, T.; Mert, M. Comparing tactical and commercial MANETs design strategies and performance evaluations. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 599–604.

11. Komulainen, A.; Grönkvist, J.; Sterner, U. On the performance of using CSMA for broadcast traffic in tactical ad hoc networks. In Proceedings of the 2018 International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, 22–23 May 2018; pp. 1–7.
12. Pradhan, M.; Gökgöz, F.; Bau, N.; Ota, D. Approach towards application of commercial off-the-shelf internet of things devices in the military domain. In Proceedings of the 2016 IEEE 3rd world forum on internet of things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 245–250.
13. Felemban, E.; Lee, C.G.; Ekici, E. MMSPEED: Multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks. *IEEE Trans. Mob. Comput.* **2006**, *5*, 738–754. [CrossRef]
14. Park, K.J.; Kim, J.; Lim, H.; Eun, Y. Robust path diversity for network quality of service in cyber-physical systems. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2204–2215. [CrossRef]
15. Kim, D.; Won, Y.; Eun, Y.; Park, K.J. Resilient architecture for network and control co-design under wireless channel uncertainty in cyber-physical systems. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3499. [CrossRef]
16. Cheng, H.; Yan, X.; Lian, H.; Weng, L.; Zhang, Q.; Feng, Z. A novel collision avoidance algorithm for IEEE 802.11 wireless LANs. In Proceedings of the 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 6–8 October 2014; pp. 879–884.
17. Sanabria-Russo, L.; Bellalta, B. Traffic differentiation in dense collision-free WLANs using CSMA/ECA. *Ad Hoc Netw.* **2018**, *75*, 33–51. [CrossRef]
18. Zhang, C.; Chen, P.; Ren, J.; Wang, X.; Vasilakos, A.V. A backoff algorithm based on self-adaptive contention window update factor for IEEE 802.11 DCF. *Wirel. Netw.* **2017**, *23*, 749–758. [CrossRef]
19. Cheng, Y.; Zhou, H.; Yang, D. Ca-CWA: Channel-aware contention window adaption in IEEE 802.11 ah for soft real-time industrial applications. *Sensors* **2019**, *19*, 3002. [CrossRef] [PubMed]
20. Kim, J.D.; Laurenson, D.I.; Thompson, J.S. Adaptive centralized random access for collision free wireless local area networks. *IEEE Access* **2019**, *7*, 37381–37393. [CrossRef]
21. Lei, J.; Tao, J.; Huang, J.; Xia, Y. A differentiated reservation MAC protocol for achieving fairness and efficiency in multi-rate IEEE 802.11 WLANs. *IEEE Access* **2019**, *7*, 12133–12145. [CrossRef]
22. Thulasiraman, P.; White, K.A. Topology control of tactical wireless sensor networks using energy efficient zone routing. *Digit. Commun. Netw.* **2016**, *2*, 1–14. [CrossRef]
23. Regis, P.A.; Sengupta, S. Distributed split-path routing strategy for multi-hop mesh networks. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 575–580.
24. Tang, L.; Lu, Z.; Fan, B. Energy efficient and reliable routing algorithm for wireless sensors networks. *Appl. Sci.* **2020**, *10*, 1885. [CrossRef]
25. Taha, A.; Alsaqour, R.; Uddin, M.; Abdelhaq, M.; Saba, T. Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. *IEEE Access* **2017**, *5*, 10369–10381. [CrossRef]
26. Chen, Z.; Zhou, W.; Wu, S.; Cheng, L. An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. *IEEE Access* **2020**, *8*, 44760–44773. [CrossRef]
27. Tilwari, V.; Dimyati, K.; Hindia, M.; Fattouh, A.; Amiri, I.S. Mobility, residual energy, and link quality aware multipath routing in MANETs with Q-learning algorithm. *Appl. Sci.* **2019**, *9*, 1582. [CrossRef]
28. Capabilities (UC) Reference Architecture (RA). Version 1.0. 11 October 2013. Available online: https://docplayer.net/2665571-U-s-army-unified-capabilities-uc-reference-architecture-ra-version-1-0-11-october-2013.html (accessed on 26 June 2022).
29. Kurose, J.F. *Computer Networking: A Top-Down Approach Featuring the Internet, 3/E*; Pearson Education India: Noida, India, 2005.
30. Perkins, C.; Belding-Royer, E.; Das, S. *RFC3561: Ad Hoc on-Demand Distance Vector (AODV) Routing*; RFC Editor: Fremont, CA, USA, 2003.
31. Network Simulation (Riverbed Modeler Suite) Web Site. Available online: https://www.riverbed.com/sg/products/steelcentral/steelcentral-riverbed-modeler.html (accessed on 29 March 2022).
32. Cole, R.G.; Rosenbluth, J.H. Voice over IP performance monitoring. *ACM Sigcomm Comput. Commun. Rev.* **2001**, *31*, 9–24. [CrossRef]