

Control Packet Scheduling First for Fast Route Discovery in Tactical MANET

Bosung Kim, Juneyoung Chang, Byeong-hee Roh, and Young-Bae Ko

Graduate School of Information and Communication, Ajou University
San 5 Wonchon-dong Youngtong-gu, Suwon, Gyeonggi-do, 443-749, Korea
{kbs8354, eyeslover, bhroh, youngko}@ajou.ac.kr

Abstract— Tactical networks consisting of mobile wireless nodes with various platforms have been developed with Mobile Ad-hoc Network (MANET). The provision of Quality of Service (QoS) is still ongoing problem to be solved in MANET due to its lack of resources and harsh propagation environments. In these environments, link failure can be occurred because of frequent mobility of wireless nodes. During the route recovery, packets without route to destination is discarded because of buffer overflow and exceeded retransmission count. In this paper, we propose an algorithm that schedules the routing control packet preferentially. The performance of the proposed method is evaluated using OPNET simulator, and the simulation results show that the proposed method improves performance in terms of packet loss, delay and route discovery time performance compared to other scheduling schemes.

Keywords— MANET, Tactical Networks, Schedule, Control Packet, QoS

I. INTRODUCTION

Tactical networks may experience many different types of environmental conditions, deteriorated environments with obstacles, severe weather, and jamming/interference attacks [1]. It should consider the case of encounter with enemies and lack of resources. These tactical networks consist of all or mostly mobile node, so that their topology can be changed dynamically. These unreliable links from these networks affect the link quality and capacity to make traffic engineering management very difficult [2].

Since tactical networks are generally configured and operated on demand without infrastructure support, MANET (Mobile Ad-hoc Network) technologies are considered to be very attractive for the tactical networks [3]. MANET is constructed from a set of homogeneous or heterogeneous participants' nodes, which must interact with each other in order to accomplish common missions assigned to those nodes [4]. In tactical MANET, the concern with the provision of QoS in MANET has been growing.

Over the past few years, several studies have been made on how to maximize the QoS in tactical networks. In [5], tactical QoS frameworks are proposed based on Differentiated Service (DiffServ) and Simple Network Management Protocol (SNMP). In DiffServ, each data packet is classified into a predefined traffic classes, rather than differentiating network traffic based on requirement of an individual flow. In [6], a

scheme to provide the end-to-end QoS between heterogeneous networks is considered. In [7], stochastic model with adaptive Weighted Random Early Detection (WRED) and Class-Based Weighted Fair Queuing (CBWFQ) is provided to support the end-to-end QoS interoperability.

Although trying to support QoS as stated above studies, traffic is dropped because of buffer overflow and/or exceeded retransmission count. Harsh environment and Lack of resources in the tactical networks bring about link failure and route discovery frequently. In [8], authors mentioned that since data packets will be discarded in case the control packets cannot be processed in time, how to schedule the control packets effectively is important to support QoS. However, the general buffer scheduling didn't distinguish which traffic is data packet from the applications or control packet from the routing protocols. We will discuss this problem in detail, and propose an enhanced buffer scheduling scheme in Section II.

In this paper, we propose Control Packet Scheduling First (CPSF), which handles the control packets for route discovery preferentially rather than any other data packets in terms of buffer management. This proposed scheme secures the route when route discovery happened and reduces traffic dropped.

The rest of this paper is organized as follows. Section II states the problem and Section III explains about proposed scheme. In Section IV, we evaluate the simulation results performed with the proposed scheme. Finally, Section V concludes this paper.

II. PROBLEM STATEMENT

There are two reasons of packet loss within each wireless node itself. The first reason is buffer overflow, or tail drop. When buffer is filled to its maximum capacity, the newly arriving packets are dropped until the buffer has enough space to accept incoming packets. Another reason is retransmission threshold. In a wireless environment using the 802.11 standard, packets can be dropped because of consistent retransmission. This is because the MAC couldn't receive any ACKs for the transmitted packets and transmission attempts of packets reached the MAC's retransmission threshold. To prove this, we performs a preliminary study these cases.

To introduce briefly the implementation environment, the physical characteristic is the IEEE 802.11b with bandwidth of 2Mbps. Each flow is a Voice over IP (VoIP) with bit rate of 8Kbps. We run simulation under AODV routing protocol for 300 seconds and use the OPNET 14.5 as a simulation tool.

This research was partially supported by Basic Science Research Program through NRF funded by the MEST (2010-0016938), and was completed with Ajou university research fellowship of 2010.

AODV is described as better MANET routing protocol which performs well in network with mobile nodes and dynamic mobility [9].

Figure 1 shows a relationship between the number of AODV control packets and the number of VoIP calls. As shown in the figure 1, the number of RERR and RREQ messages increases as the number of VoIP increases. This is because the node recognizes that the link failure occurs by the RERR message, and broadcasts the RREQ message for the destination [10].

Figure 2 shows the packet loss according to the number of VoIP calls. When using AODV routing protocol, there is another case of the packet loss including two cases as described above. In AODV routing protocol, data packets waiting for a route should be buffered until the source node receives the RREP message. If a route discovery has been attempted RREQ_RETRIES times at the maximum TTL without receiving any RREP messages, all data packets should be dropped [10]. This number of packets dropped from AODV routing protocol increases as the number of VoIP increases.

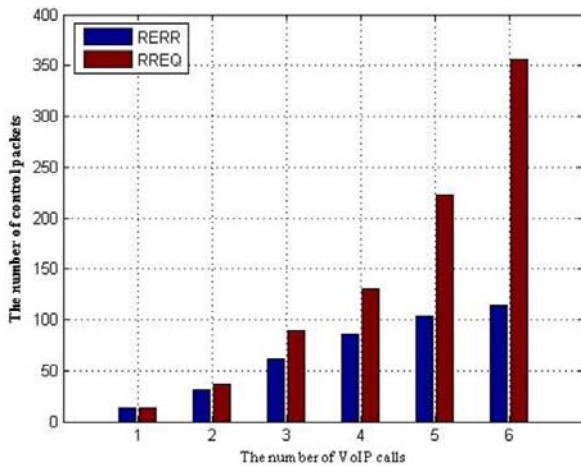


Figure 1. Number of control packets according to number of VoIP calls

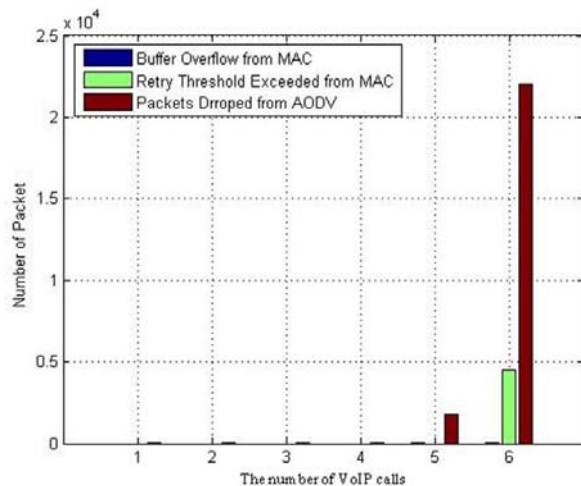


Figure 2. Packet loss according to number of VoIP calls

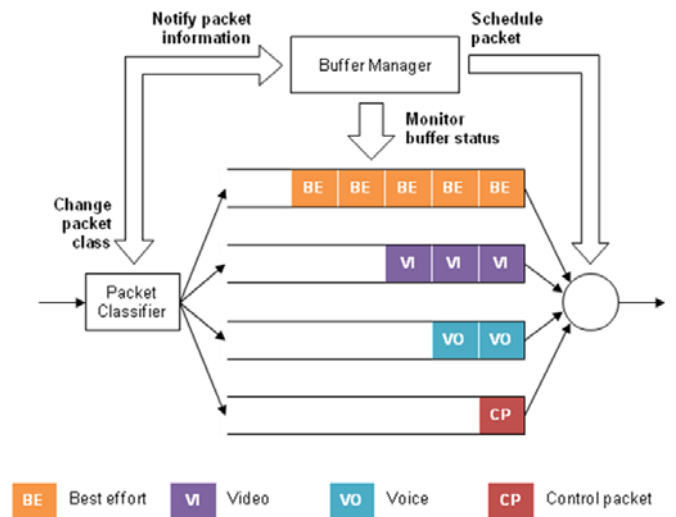


Figure 3. The proposed CPSF architecture

We can see that after more than a certain amount of traffic transmitted, packet loss occurs despite the efforts to find a route for destination. This is because the control packets for route discovery or maintenance are not treated preferentially rather than any other data packets in terms of buffer scheduling. In the following section, we will propose a buffer scheduling scheme to alleviate the above problems.

III. PROPOSED SCHEME: CPSF (CONTROL PACKET SCHEDULING FIRST)

To solve the problems stated above, the proposed CPSF architecture is shown as Figure 3. The CPSF architecture is composed of the buffer, packet classifier and buffer manager. The buffer has four sub-buffers. Above three sub-buffers are for data packets and sub-buffer at the bottom is for control packets. These three sub-buffers are based on Weighted Fair Queuing (WFQ) so that data packets are provided differentiated services depending on their classes; BE, VI and VO. In sub-buffer at the bottom, control packets or CP are handled preferentially rather than any other data packets. This is because if route discovery is not conducted by control packets, data packets cannot be delivered properly.

As shown in Figure 3, the packet classifier performs two functions. First, the packet classifier categorizes packets and they are stored in the sub-buffer according to their class. Second, the packet classifier brings the information of packets and notifies this packet information to the buffer manager. Since control packets created in the routing protocol were served by the best effort originally, in order to serve them preferentially, the buffer manager should know what control packets are.

The buffer manager is responsible for gathering the packet information and monitoring the buffer status. The gathered information is maintained into tables in the buffer manager. These tables are shown in Table 1 and Table 2. Table 1 has two columns; pkt_type and msg_type. The pkt_type is for checking whether incoming packet is the control packet or not. If the packet type is the control packet, the message type or msg_type is also checked. In the case of AODV, this message type can be RREQ, RREP and RERR. Table 2 also has two

columns; sub_buf and buf_len. The sub_buf is for identifying the index of each sub-buffers and the buf_len is for storing the buffer length of each sub-buffers.

Based on this information, the buffer manager treats the control packet preferentially rather than any other data packets, as shown in algorithm 1. Inputs are packet information and buffer information at current time. The buffer manager also monitors the number of RERR messages during the measurement time T. This notation is Num_RERR for judging the link failure. At first, the buffer manager initializes the Num_RERR at start time and then applies this algorithm to incoming packet. When incoming packet is the control packet, it checks the routing message type or msg_type. If msg_type is RERR message, it updates the Num_RERR. If msg_type is RREQ or RREP message, it checks the Num_RERR for judging the link failure and the length of each sub-buffer for judging the buffer overflow. Once the buffer manager knows that link failure and buffer overflow has occurred, it stores this incoming packet into sub-buffer which the control packet will be scheduled preferentially. These packets stored in this sub-buffer have a role in fast route discovery.

TABLE 1. Packet information

pkt_type	msg_type

TABLE 2. Buffer information

sub_buf	buf_len

Algorithm 1 – CPSF

Inputs: packet information and buffer information

```
#define BUFFER_OVERFLOW    N
#define RERR_THRESHOLD     M
#define MEASURE_TIME       T
```

Intialize Num_RERR at start time.

If (pkt_type = CP)

 If (msg_type = RERR)

 Update Num_RERR in T.

 Else if (msg_type = RREQ or msg_type = RREP)

 For (sub_buf)

 If (Num_RERR > M and buf_len > N)

 Store this packet into sub-buffer for CP.

 Else

 Store this packet into sub-buffer according to its class.

IV. PERFORMANCE EVALUATIONS

A. Simulation Environments

The Joint Tactical Radio System (JTRS) is developing a set of MANET, to provide the last tactical mile connectivity to the Global Information Grid (GIG). JTRS extends the GIG to the tactical edge as illustrated in Figure 4. The GIG extension is accomplished by providing an IP-based transport network infrastructure to the war-fighter from a backbone connected to a JTRS networking waveform [11][12].

These MANET-based JTRS networking waveforms are currently in development; Wideband Networking Waveform (WNW), Soldier Radio Waveform (SRW), Joint Airborne Networking-Tactical Edges (JAN-TE), and Mobile User Object System (MUOS). In this paper, we decided to consider WNW and SRW as simulation network models. The WNW network provides a secure backbone routing infrastructure that passes network traffic within and between ground and airborne domains. The SRW network is a stub network that carries traffic originating at and/or destined for internal nodes and relies on WNW for backbone routing [11][12].

The WNW and SRW networks are the workhorse of the communications system of Future Combat System (FCS). The WNW network supports many users with aggregate user data rates between 64Kbps to 2Mbps. The SRW network also supports many users with aggregate user data rates between 2Kbps to 2.8Mbps. Based on these data rates, we applied to 2Mbps bandwidth as simulation parameter.

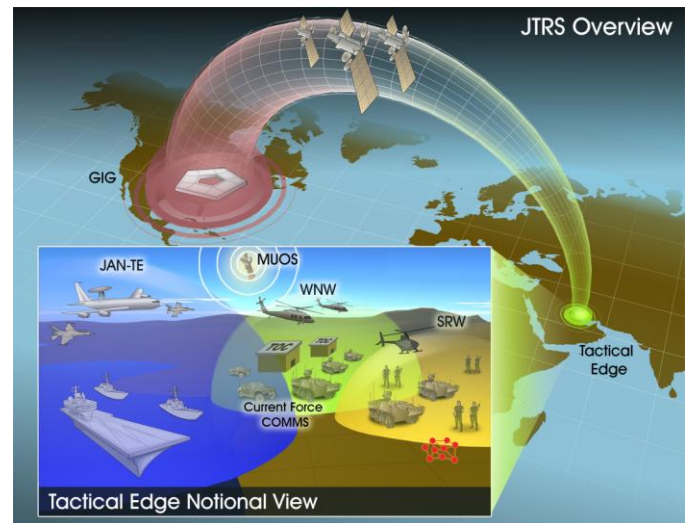


Figure 4. JTRS support of tactical edge

TABLE 3. Simulation parameters

Simulator	OPNET 14.5
Network Topology	Chain
Physical Characteristic	802.11b
Bandwidth (Mbps)	2.0
Transmission Range (m)	100
Packet Inter-arrival Time (seconds)	0.01
Packet Size (bits)	80
Routing Protocol	AODV
Mobility	Static
Simulation Times (seconds)	300

These networking waveforms described above support a various kinds of networking services. Among these networking services, VoIP will provide the war-fighter's preferred push-to-talk netted communications as well as traditional peer-to-peer communications [11]. We decided to apply this VoIP with the G.729 codec as a simulation traffic model.

The simulation environment for performance evaluation of proposed scheme is shown in Table 3. The simulator for this implementation is OPNET 14.5 [13] which is a powerful tool for network analysis. We set topology as chain networks for carrying out simulations in order to vary the number of hops. The physical characteristic is IEEE 802.11b with transmission range of 100m. As mentioned above, each flow is a VoIP with G.729 codec and the bandwidth is 2Mbps. We run simulation under AODV routing protocol for 300 seconds.

B. Results

Because our proposed scheme is implemented in the MAC layer, in order to compare the proposed scheme, we implemented two other scheduling schemes; FIFO and EDCA. The First In First Out (FIFO) scheme is based on a simple principle: The packet that first arrives in the FIFO queue will be served first. Since FIFO scheduling does not support isolation between traffic flows, it is difficult to guarantee QoS. The Enhanced Distributed Channel Access (EDCA) scheme is contention-based channel access method for differentiated QoS provision, in the Hybrid Coordination Function (HCF) Mac sub-layer.

VoIP has stringent delay requirements, thus its sound quality is sensitive to packet losses. In [14], the author mentioned that the small packet size and the number of hops together cause low throughput and long delays that are not tolerated by the VoIP traffic. To transmit the VoIP traffic, small-sized packets are generated every few milliseconds typically. The MAC protocol generates the control packets according to these packets and this can be overhead. When the number of hops is also increased, the network performance is decreased rapidly. The transmission of VoIP traffic in more than three hops causes problems on a small network because of interference of each other [14, 15].

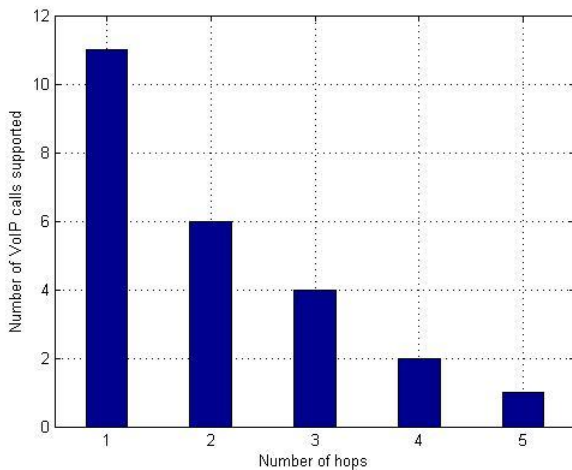


Figure 5. Capacity degrades with the number of hops

Figure 5 also shows that the network performance is sensitive to the number of hops. We implemented a simple experiment by the simulator with VoIP calls with G.729 codec. This experiment indicates that the number of VoIP calls decreases with the number of hops for a chain network.

We have already mentioned that the performance of VoIP including the number of calls is affected by the number of hops. So, we have focused on 2-hop and 3-hop networks, since the VoIP cannot achieve the performance with more hops [14, 15]. Our proposed scheme was compared with other schemes, FIFO and EDCA for each performance metric. We evaluated our proposed scheme with increasing the number of VoIP calls until the link failure occurs like in tactical networks. Figure 6 shows the performance of 2-hop networks and Figure 7 shows the performance of 3-hop networks.

Because FIFO cannot guarantee the QoS, it can transmit VoIP up to the number of VoIP calls as illustrated in Figure 5. However, CPSF and EDCA can support the QoS up to 8 calls of 2-hop case and 5 calls of 3-hop case. In order to verify how quickly the route is generated, we extracted total route discovery time as shown in Figure 6(a) and Figure 7(a). Our proposed scheme shows that it takes less time than other schemes even when the link failure occurs because CPSF serves control packet first.

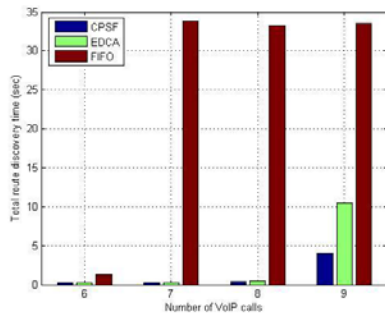
We could not compare the performance of CPSF with EDCA because FIFO has much worse performance than others. So, we summarized the numerical results for our proposed scheme separately corresponding 2-hop and 3-hop networks in comparison with EDCA as shown in Table 4. There is significant difference between CPSF and EDCA in 2-hop networks. However, in 3-hop networks, CPSF shows a better performance than EDCA. When the link failure occurs, CPSF also shows the better performance. In tactical network where the network fault such as link failure can be occurred, CPSF can alleviate this phenomenon.

V. CONCLUSIONS

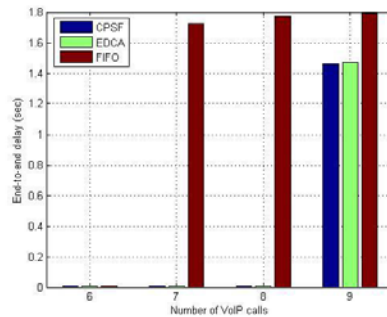
We have already discussed problem that during the route recovery, packets without route for destination can be discarded in terms of buffer management. In this paper, we propose the scheme so called Control Packet Scheduling First (CPSF), which handles the control packets for route discovery preferentially rather than any other data packets. We model the tactical networks similarly and the simulation results show that proposed scheme has advantages limited less than 3-hop range networks. For multi-hop transmission of VoIP traffic more in-depth study needs to be conducted to support QoS in tactical networks.

TABLE 4. Detailed results of proposed scheme

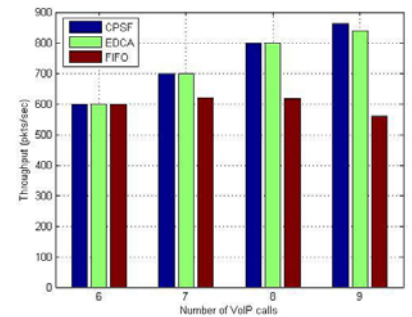
Hops	Calls	CPSF		EDCA	
		Delay	Throughput	Delay	Throughput
2	6	0.0055	600	0.0055	600
	7	0.0066	700	0.0068	700
	8	0.0085	800	0.0183	800
	9	1.4593	860	1.4731	839
3	4	0.0083	400	0.0106	400
	5	0.0147	496	0.0371	490
	6	2.8211	503	2.6965	443
	7	2.9675	528	3.3478	383



(a) Route discovery time (sec)

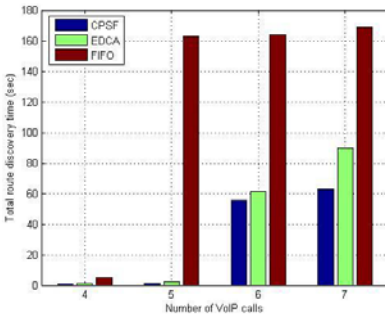


(b) End-to-end delay (sec)

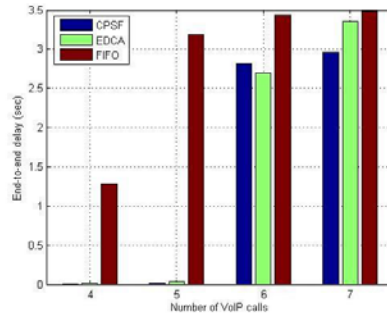


(c) Throughput (pkts/sec)

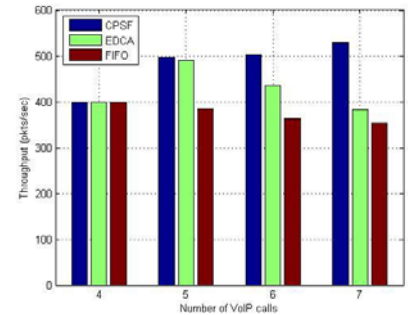
Figure 6. Performance according to number of VoIP calls in 2-hop range networks



(a) Route discovery time (sec)



(b) End-to-end delay (sec)



(c) Throughput (pkts/sec)

Figure 7. Performance according to number of VoIP calls in 3-hop range networks

REFERENCES

- [1] Ji Yong Choi, et al., "A Dual-path On-demand Routing Protocol for Tactical Wireless Networks," IEEE ICACT 2010, Feb. 2010.
- [2] Sherry Wang, et al., "QoS Management In Disadvantaged Tactical Environments," IEEE MILCOM 2007, Oct. 2007.
- [3] Burbank, J.L., et al., "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," IEEE Communication Magazine, Nov. 2006.
- [4] Bosung Kim, et al., "Label-Switched Multi-Path Routing for Mission Critical Tactical Message Delivery," IEEE CUTE 2010, Dec. 2010.
- [5] Bong Chan Kim, et al., "A QoS Framework design based on DiffServ and SNMP for Tactical Networks," IEEE MILCOM 2008, Nov. 2008.
- [6] Hye-Lim Koo, et al., "Data delivery with end-to-end QoS guarantee in tactical network interconnected with Wireless Ad-hoc Network and heterogeneous networks," IEEE ICACT 2009, Feb. 2009.
- [7] Ming-Jye Sheng, et al., "Analysis of adaptive WRED and CBWFQ algorithms on tactical edge," IEEE MILCOM 2008, Nov. 2008.
- [8] Jianxin Wang, et al., "QoS supporting control packet scheduling strategy in optical burst switched networks," SPIE 2003, Sept. 2003.
- [9] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, Jan. 1999.
- [10] C. Perkins, et al., "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.
- [11] Stephen, D.R., et al., "Network programming of Joint Tactical Radio System radios," IEEE MILCOM 2008, Nov. 2008.
- [12] North, R., et al., "Joint Tactical Radio System – Connecting the GIG to the Tactical Edge," IEEE MILCOM 2006, Oct. 2006.
- [13] <http://www.opnet.com/>
- [14] Vanhatupa, T., et al., "Multihop IEEE 802.11b WLAN Performance for VoIP," IEEE PIMRC 2005, Sept. 2005.
- [15] Armenia, S., et al., "Transmission of VoIP traffic in multihop ad hoc IEEE 802.11b networks: experimental results," IEEE WICON 2005, July 2005.