

# Byzantine Generals: OM(2) with Traitor Commander

$N = 7$  generals,  $t = 2$  traitors. Commander  $G_0$  is a traitor.

- Commander:  $G_0(\mathcal{T})$
- Lieutenants:  $G_1(\mathcal{T}), G_2(\mathcal{L}), G_3(\mathcal{L}), G_4(\mathcal{L}), G_5(\mathcal{L}), G_6(\mathcal{L})$

Traitor Strategies:

- $G_0(\mathcal{T})$ : Sends A to  $G_2, G_4, G_6$ . Sends R to  $G_1, G_3, G_5$ .
- $G_1(\mathcal{T})$ : (Received R from  $G_0$ ) When sending/relaying: sends A to  $G_2, G_4, G_6$ ; sends R to  $G_3, G_5$ .

## Round 1: Commander $G_0$ (Traitor) Sends Commands

$G_0$  sends its chosen messages to the lieutenants.

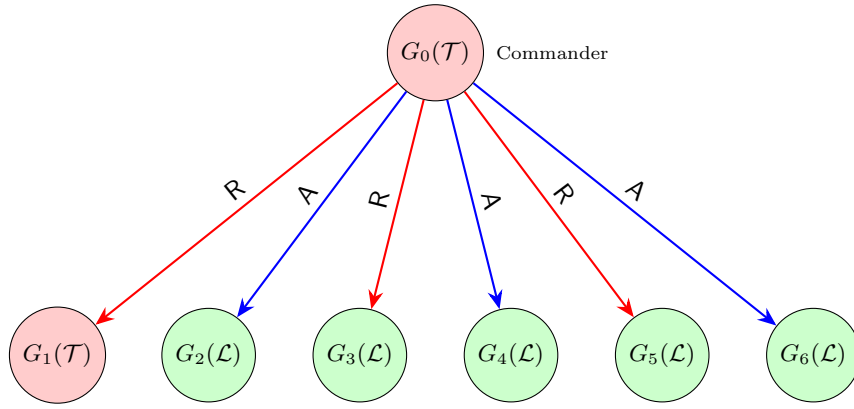


Figure 1: Round 1: Traitor Commander  $G_0$  sends messages.

$G_1(\mathcal{T})$	$G_2(\mathcal{L})$	$G_3(\mathcal{L})$	$G_4(\mathcal{L})$	$G_5(\mathcal{L})$	$G_6(\mathcal{L})$
R					
	A				
		R			
			A		
				R	
					A

The grid above shows the initial values  $v_i$  that each lieutenant  $G_i$  (represented by row and column headers) receives from Commander  $G_0$  and stores. This value is placed on the diagonal cell  $(G_i, G_i)$ . Off-diagonal cells are empty, to be filled by messages exchanged between lieutenants in later algorithm phases (e.g., OM(m-1) rounds).

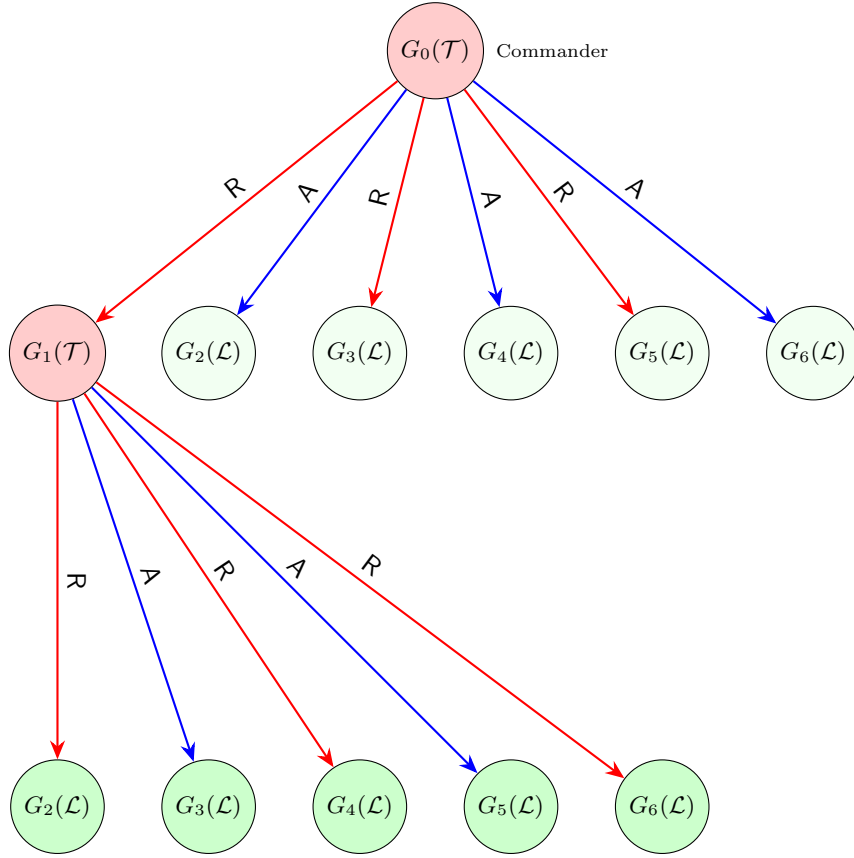


Figure 2: Round 2: Traitor Lieutenant  $G_0$  sends conflicting messages. Lieutenants now communicate with each other.

		Receiver				
		$G_2$	$G_3$	$G_4$	$G_5$	$G_6$
Sender	$G_2$	<b>R</b>	R	R	R	R
	$G_3$	A	<b>A</b>	A	A	A
	$G_4$	R	R	<b>R</b>	R	R
	$G_5$	A	A	A	<b>A</b>	A
	$G_6$	R	R	R	R	<b>R</b>
Majority		<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>

**Legend:** Rows (left) are senders, columns (top) are receivers. Each cell shows the message the sender tells the receiver that it received from  $G_1$ . Yellow diagonal: sender's own message from  $G_1$ . Blue = Attack (A), Red = Retreat (R).

$G_1(\mathcal{T})$	$G_2(\mathcal{L})$	$G_3(\mathcal{L})$	$G_4(\mathcal{L})$	$G_5(\mathcal{L})$	$G_6(\mathcal{L})$
<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>
	<b>A</b>				
		<b>R</b>			
			<b>A</b>		
				<b>R</b>	
					<b>A</b>

The grid above shows the initial values  $v_i$  that each lieutenant  $G_i$  (represented by row and column headers) receives from Commander  $G_0$  and stores. This value is placed on the diagonal cell  $(G_i, G_i)$ . Off-diagonal cells are empty, to be filled by messages exchanged between lieutenants in later algorithm phases (e.g., OM(m-1) rounds).