Lightweight Blockchain Assisted Secure Routing of Swarm UAS Networking

Jian Wang, and Houbing Song, Ph.D.

Security and **O**ptimization for **N**etworked **G**lobe Laboratory (SONG Lab)

www.SONGLab.us

September 27, 2021

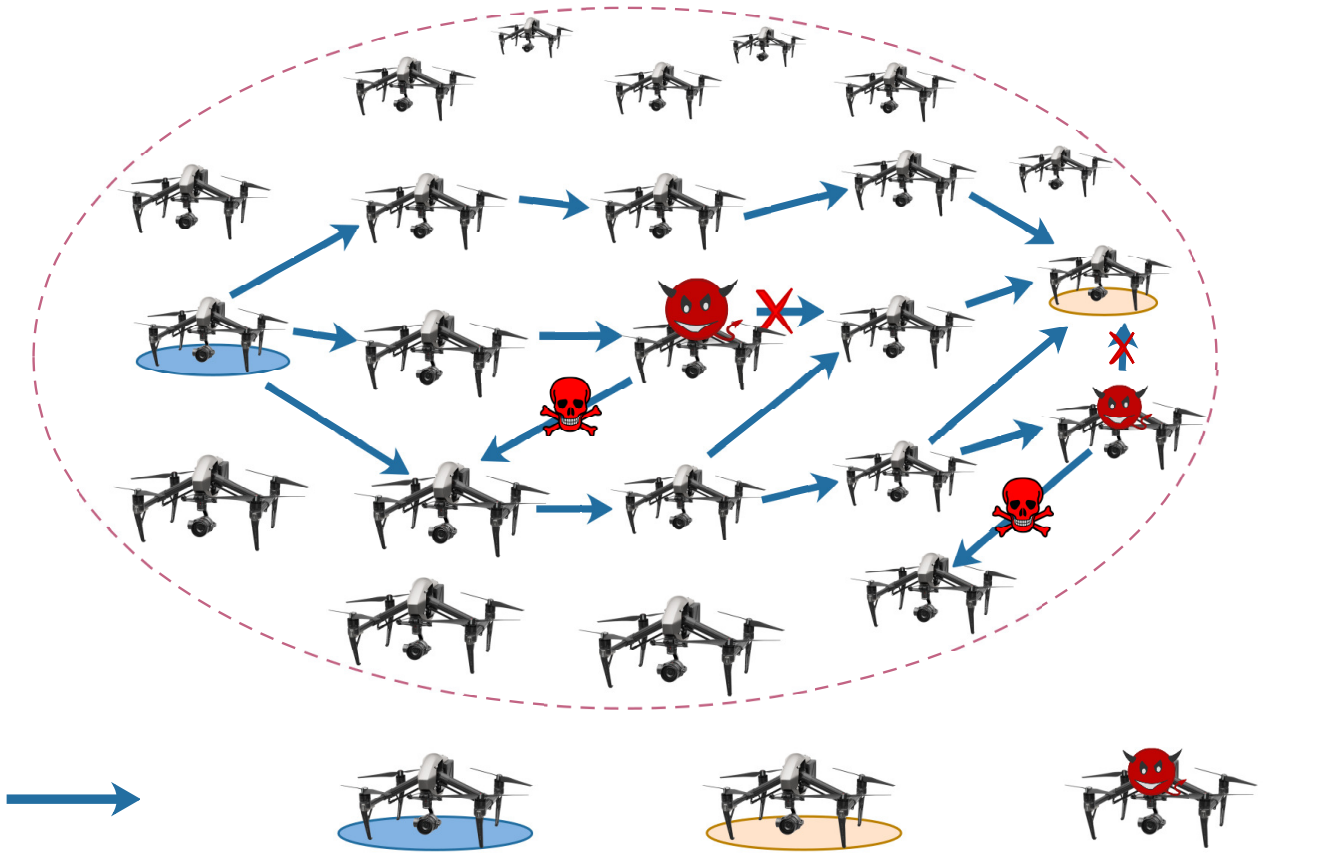
IETF Workshop on Evolving Routing Security in the Internet

Outline

Outline

Outline

Motivation

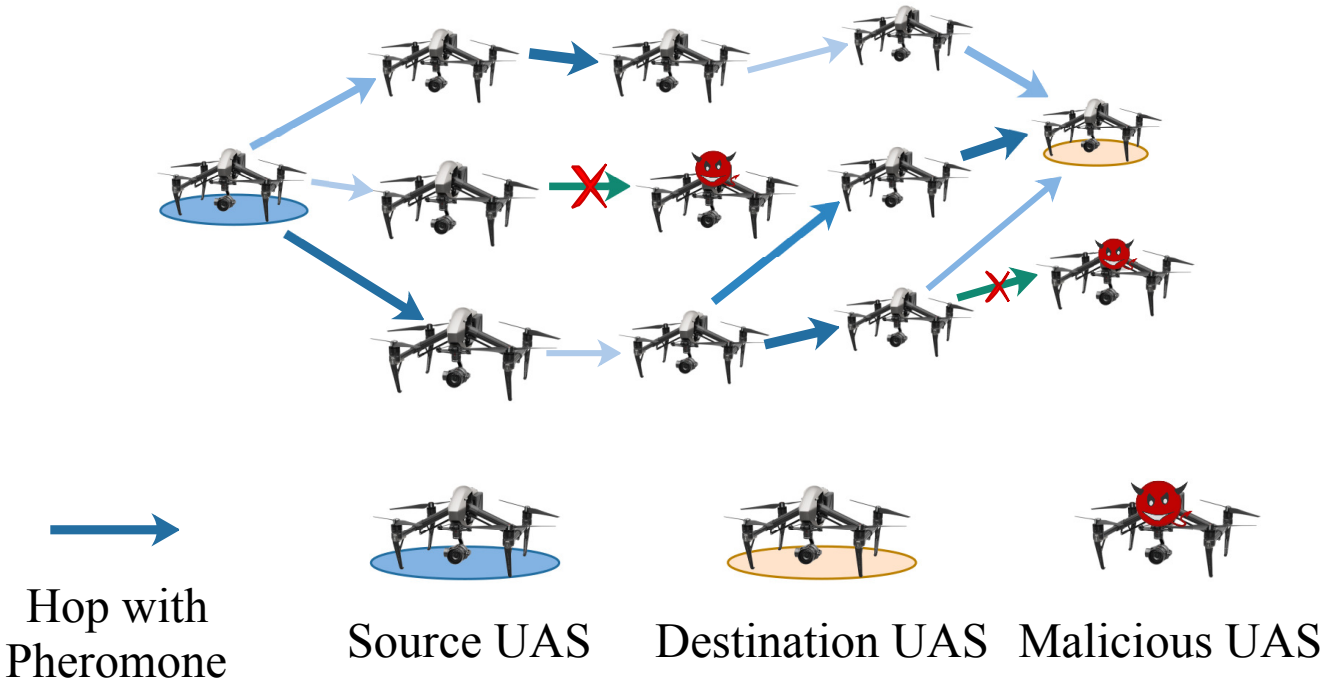


Attackers in Swarm UAS Networking

Outline

Outline

Blockchain Assisted Secure Routing



Security Routing of Swarm UAS Networking

We consider each UAS, $u_n = \{un\}$, as a block container in Blockchain which obtains its whole detailed identification, I_n, for verification and block digests, H_N, of the whole Blockchain for authentication.

The next hops, $U_{(n,\ hops)}$, for u_n is :

$$U_{(n,\ hops)} = \{u_n \mid \theta_{(\overrightarrow{V_{(s,\ d)}},\ \overrightarrow{V_{(n,\ n+1)}})} \leq \pi\} \tag{1}$$

$$Ph_n \leftarrow (1-\alpha) \times Ph_n + \sum_{k=1}^{m} \triangle Ph_n \tag{2}$$

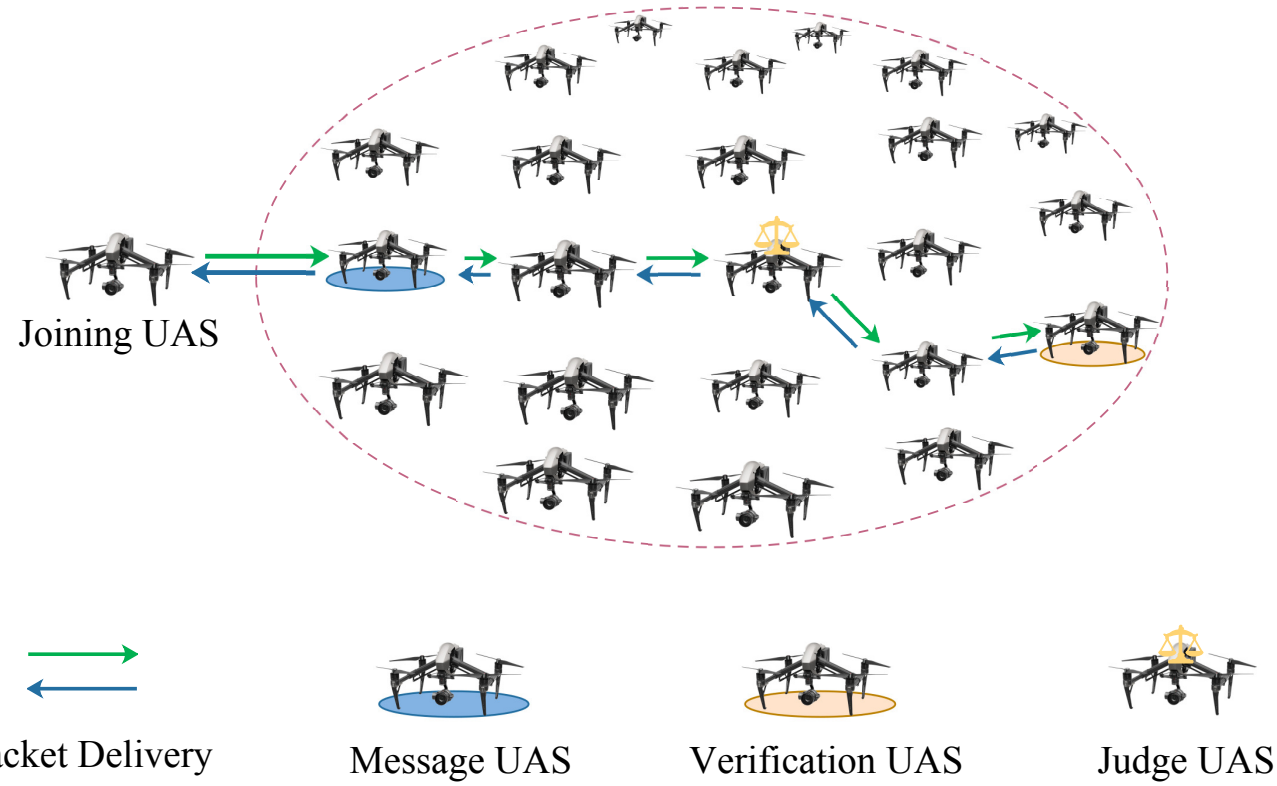
$\triangle Ph_n$ is:

$$\triangle Ph_n = \frac{1}{I_n} \tag{3}$$

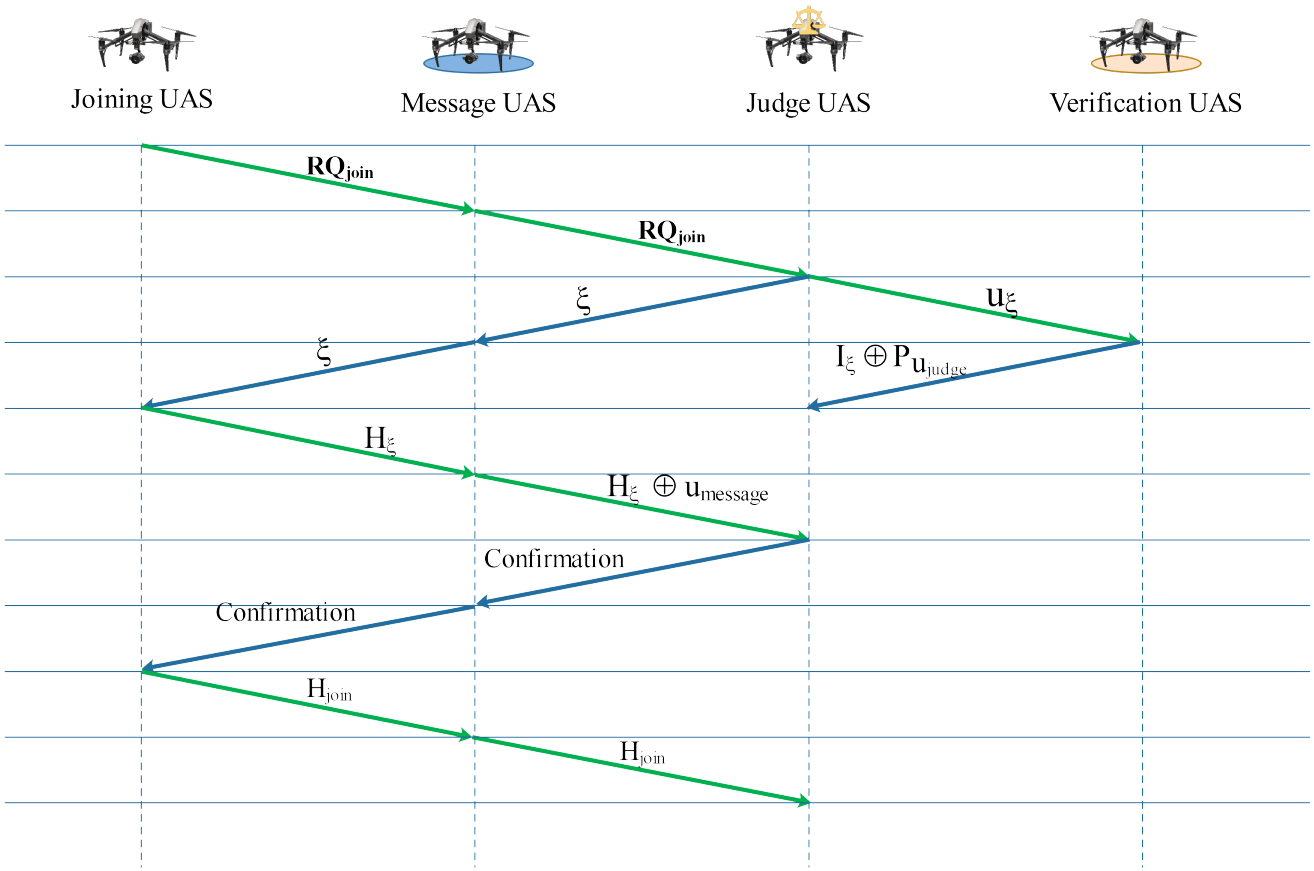
The U_n with $max(Ph_n)$ has the previlige to write a new block which is the identification digest of $U(m+1)$.

Outline

Blockchain based Authentication



Consensus Construction for Joining Swarm UAS Networking



Operation of Authentication for Swarm UAS Networking

Outline

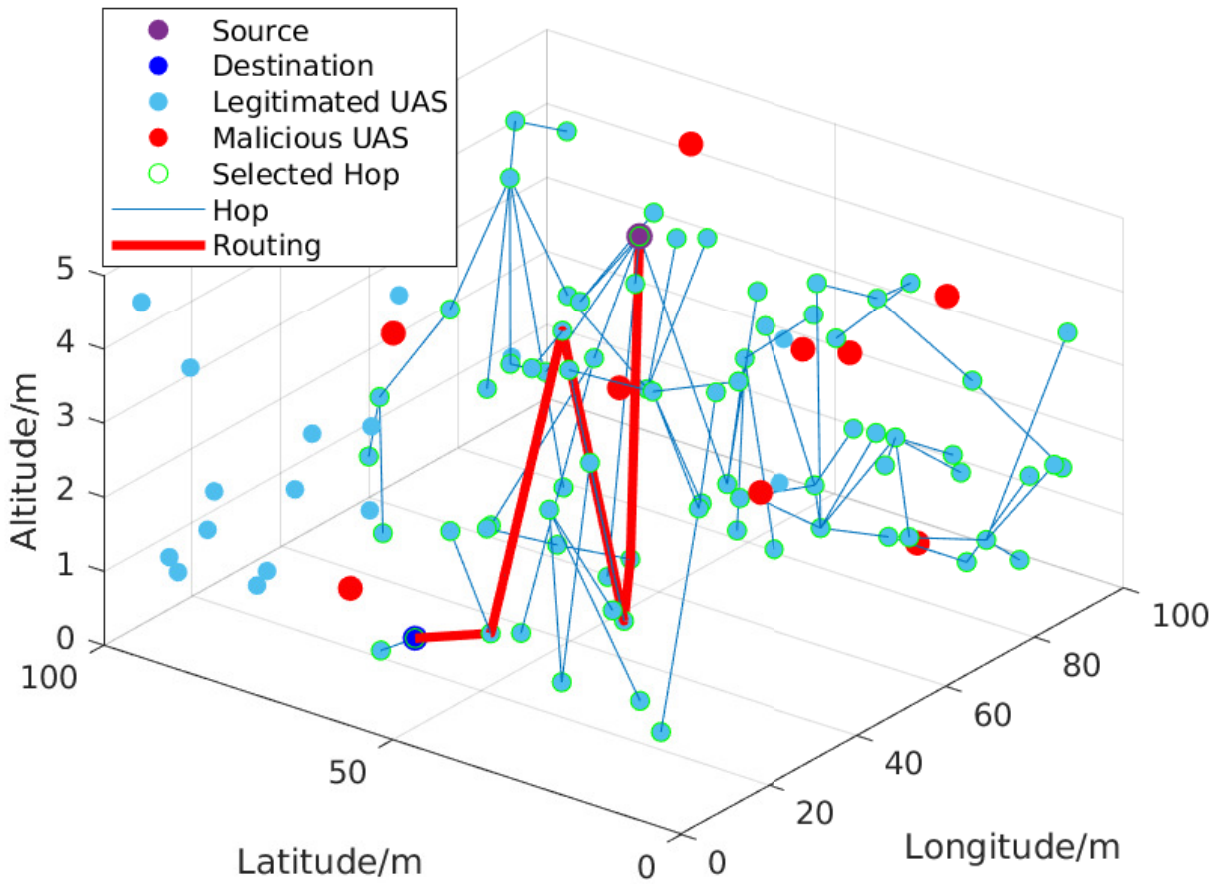
Passive synchronization

For the synchronization of Blockchain, we adopt a passive approach to broadcast the updated blocks with the communication of the swarm UAS networking.

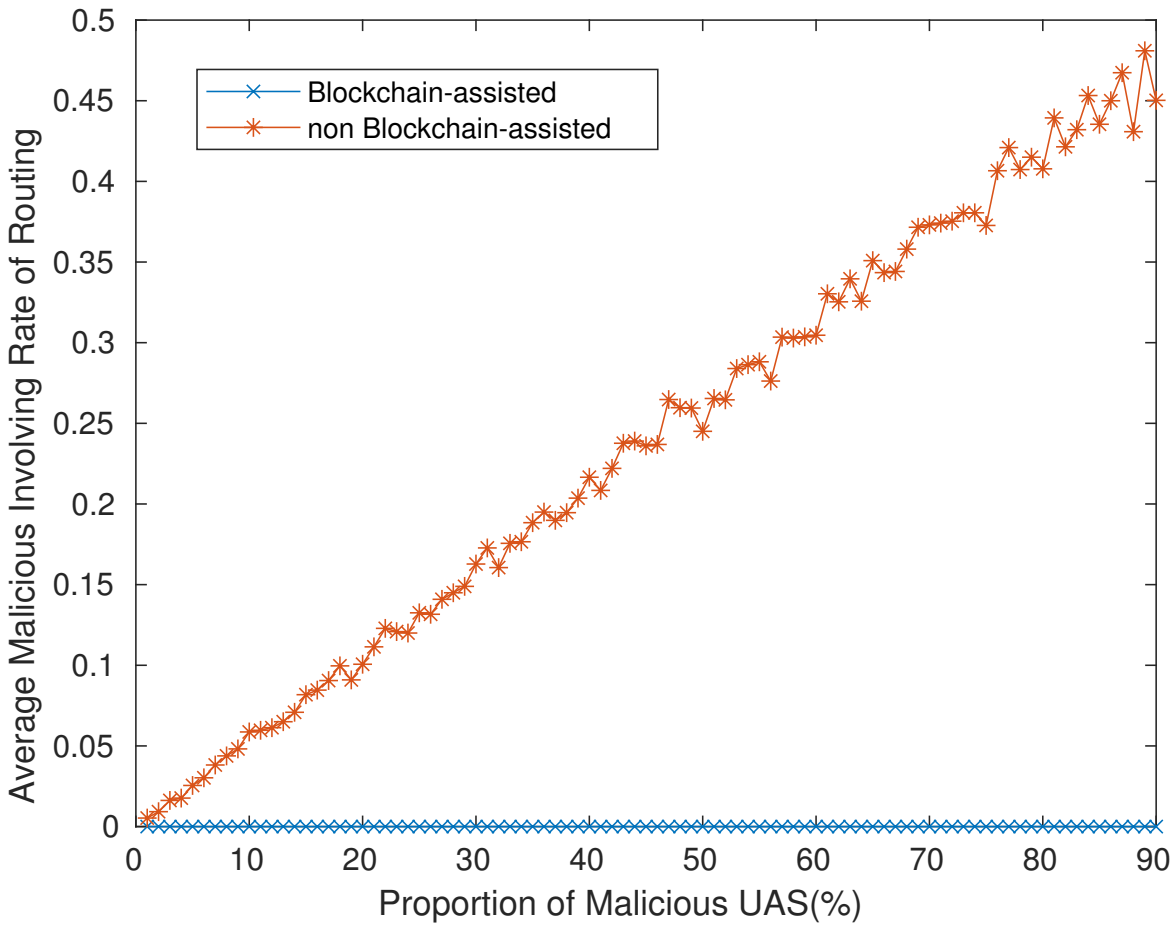
1. The updated blocks, H'_n is stored in u_{judge} which has main traffic streams.
2. Each packet p_μ passes through u_{judge} will be attached to the updated blocks to synchronize the its neighbors $U_{neighbors}$.
3. The updated $u_{neighbors}$ will be marked in $U_{updated}$.
4. The updated UAS will check its neighbors $U'_{neighbors}$ and deliver the updated H'_n when p_μ passes through.

Outline

Evaluation

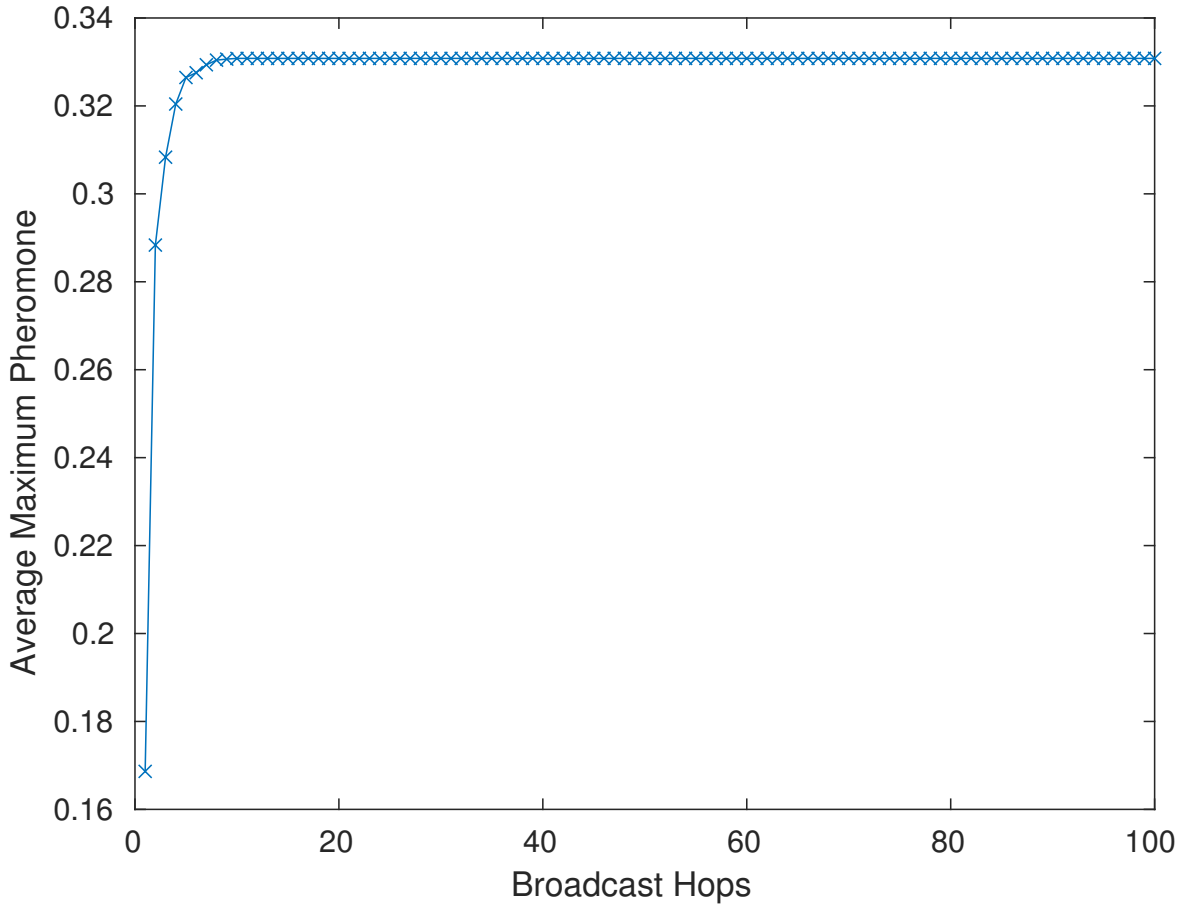


Routing Processing

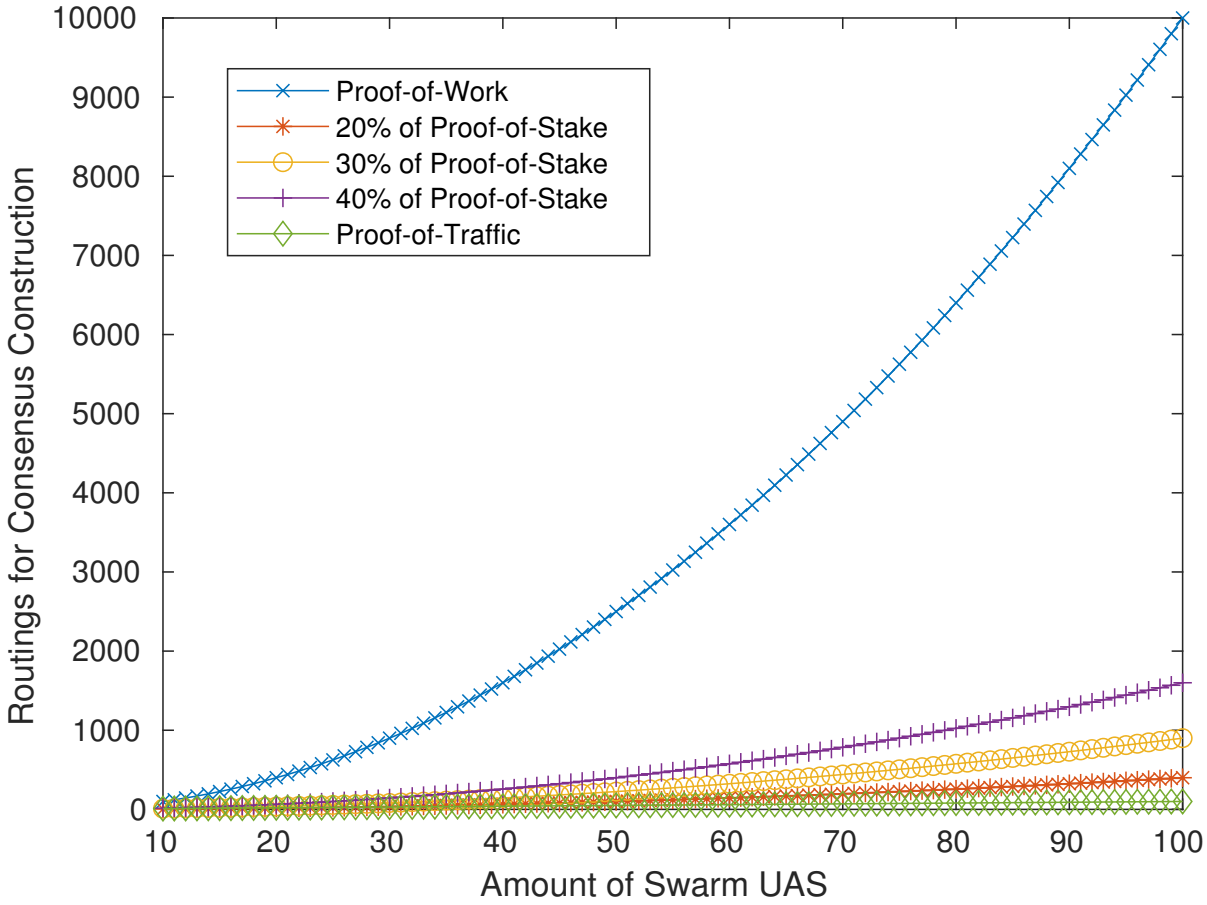


Average Malicious Involving Rate of Routing

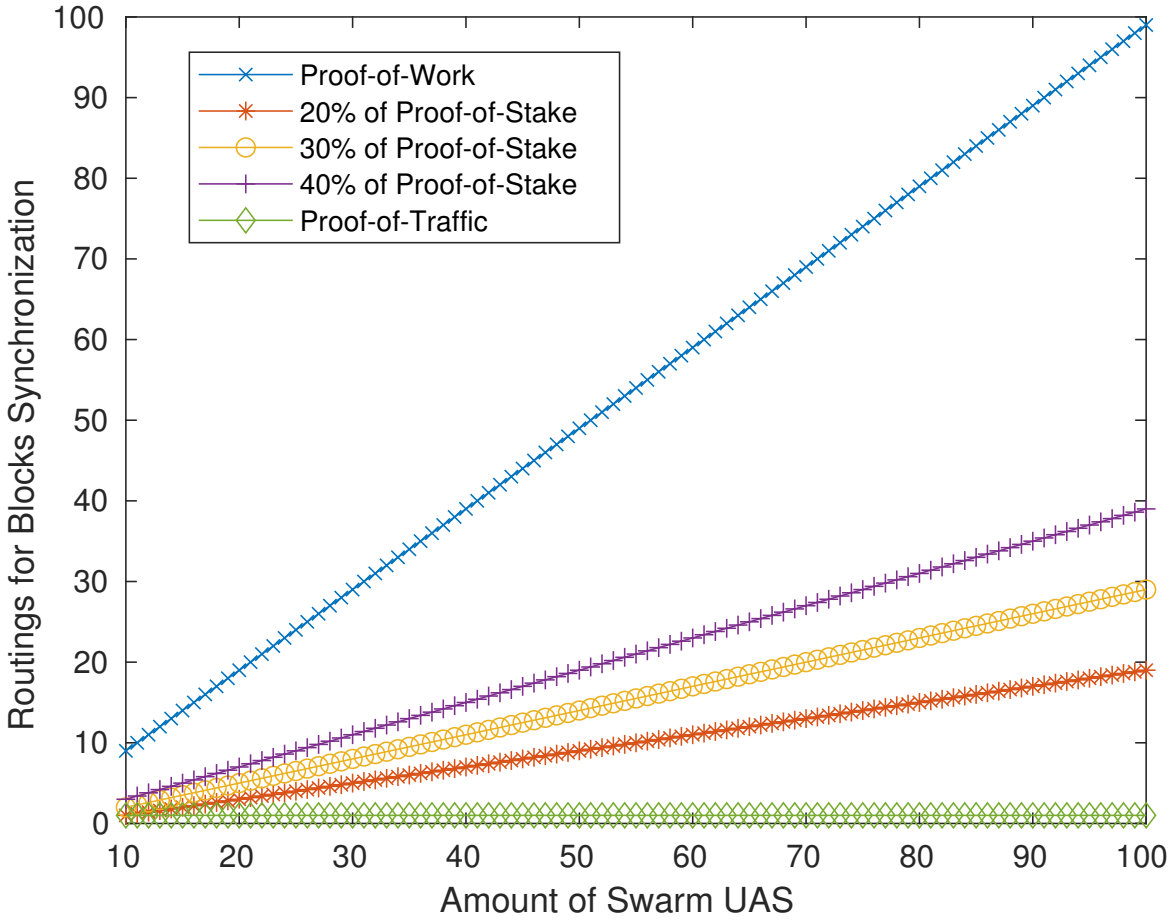
η_ζ (bits)	64	128	256	512
$Pr_{bruteForce}$	$5.4210e^{-20}$	$2.9387e^{-39}$	$8.6362e^{-78}$	$7.4583e^{-155}$



Average Broadcast Pheromone



Routing for Consensus Construction



Routing for Synchronization

Outline

Conclusions

- We leverage lightweight Blockchain to assist the swarm UASs to improve the security of routing with constraint computation resources.
- With lightweight Blockchain, swarm UASs can prevent the malicious UAS connection to the swarm UAS networking and mitigate the attacks from malicious UASs.
- Different from PoW and PoS, we leverage pheromone to mark the traffic status of each UAS in swarm UAS networking. To save routing construction, PoT synchronizes the updated blocks with the passive broadcast.

Thank you! & Questions?

Security and **O**ptimization for **N**etworked **G**lobe Laboratory (SONG Lab)
www.SONGLab.us
WANGJ14@my.erau.edu; Houbing.Song@erau.edu