Secure, Robust, and Energy-Efficient Authenticated Data Sharing in Drone to Vehicles Communications

Atefeh Mohseni

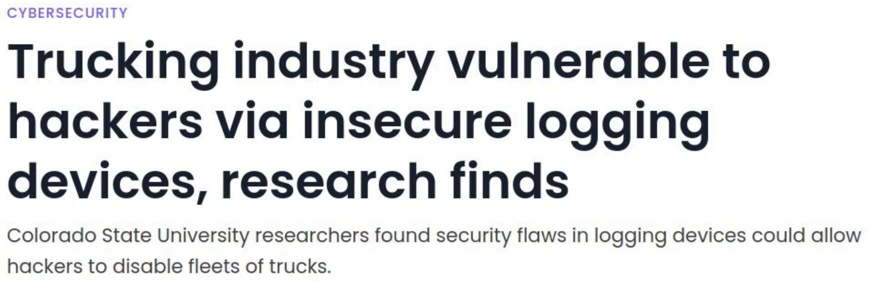
University of California, Santa Barbara, USA

ACWS July 2024

The Potential of UAVs in B5G

- Beyond 5G networks offers unprecedented speed and minimal latency.
- Drones (UAVs) can extend network coverage and enhance communication in challenging environments.
- UAV-assisted Vehicular Ad-hoc Networks (VANETs) can improve traffic management, safety, and connectivity.

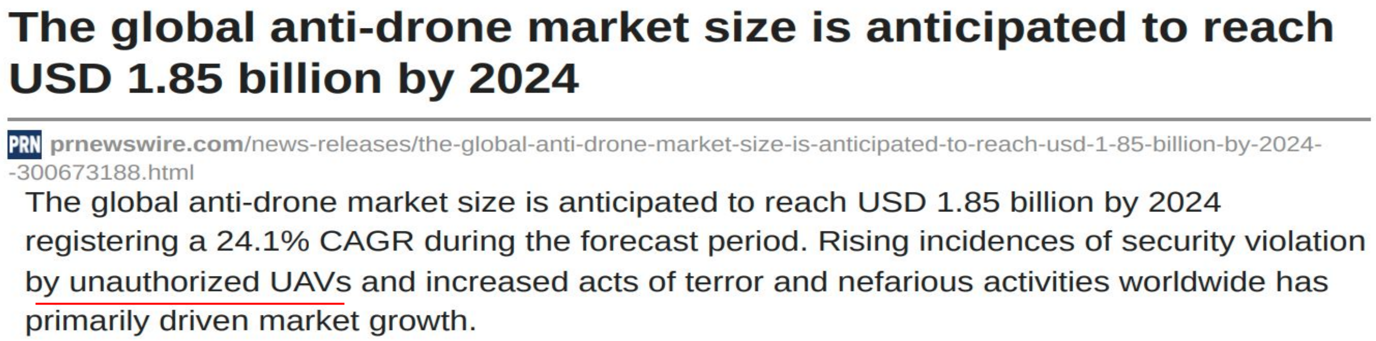
Security Challenges



CYBERSECURITY

Trucking industry vulnerable to hackers via insecure logging devices, research finds

Colorado State University researchers found security flaws in logging devices could allow hackers to disable fleets of trucks.



The global anti-drone market size is anticipated to reach USD 1.85 billion by 2024

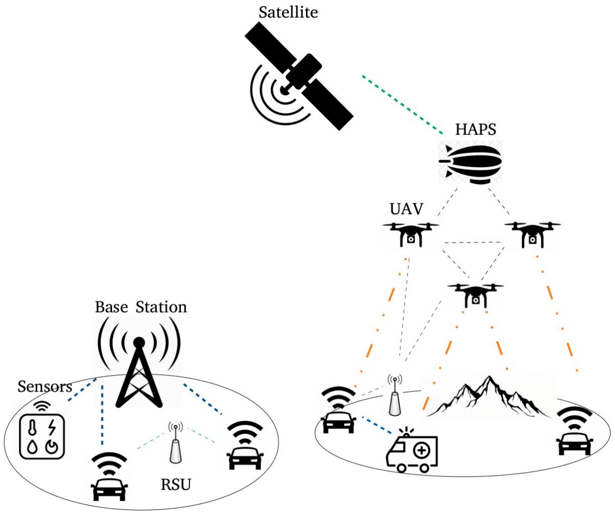
PRN prnewswire.com/news-releases/the-global-anti-drone-market-size-is-anticipated-to-reach-usd-1-85-billion-by-2024--300673188.html

The global anti-drone market size is anticipated to reach USD 1.85 billion by 2024 registering a 24.1% CAGR during the forecast period. Rising incidences of security violation by unauthorized UAVs and increased acts of terror and nefarious activities worldwide has primarily driven market growth.

Proposed Protocols for Secure Data Sharing

- **SeGDS**: Secure Group Data Sharing among drones.
- **SeDDS**: Secure Direct Data Sharing between drones

  and vehicles.



System Model

Threat Model

01 Adversaries can intercept messages, and impersonate entities.

02 Collisions among adversaries are possible.

03 Service Provider (Cloud) and Road Side Unit (RSU) are trusted entities.

04 UAVs are rational entities with limited resources, acting maliciously for perceived benefit.

SeGDS: Secure Group Data Sharing Phases

System Initialization: The Authentication Server Function (AUSF) sets up the cryptographic parameters.

Registration: UAVs register with the AUSF, obtaining their keys.

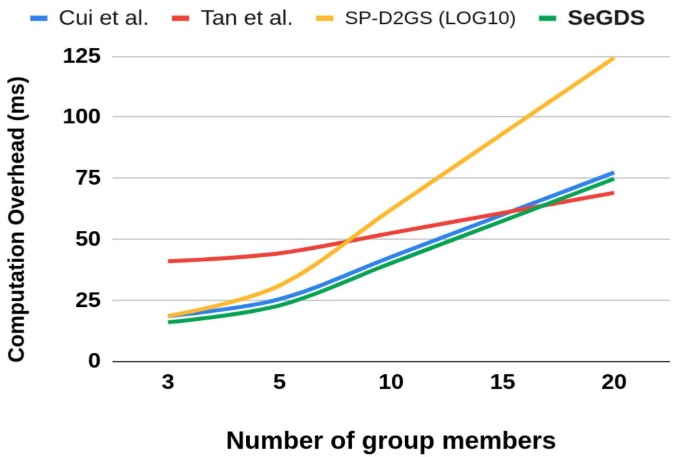
Session Setup: The Road Side Unit (RSU) establishes a secure session with the content service provider.

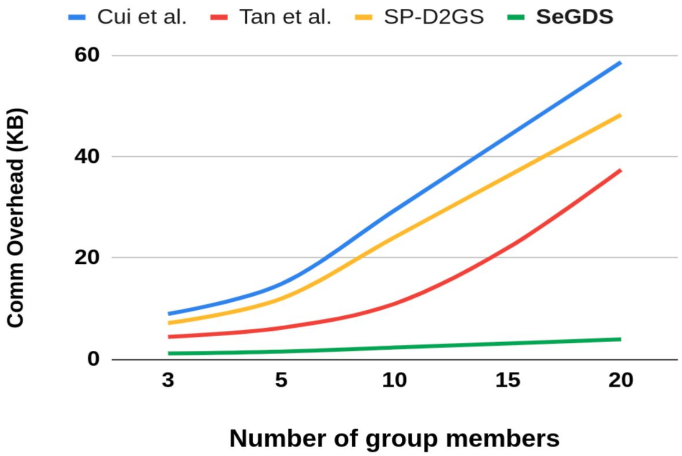
Task Assignment and Cooperative Download: The RSU divides the data into segments and assigns them to UAVs for download.

Data Sharing: UAVs share their downloaded segments with each other.

Data Consolidation: The RSU consolidates the data and distributes the decryption key to the UAVs.

SeGDS Performance Analysis



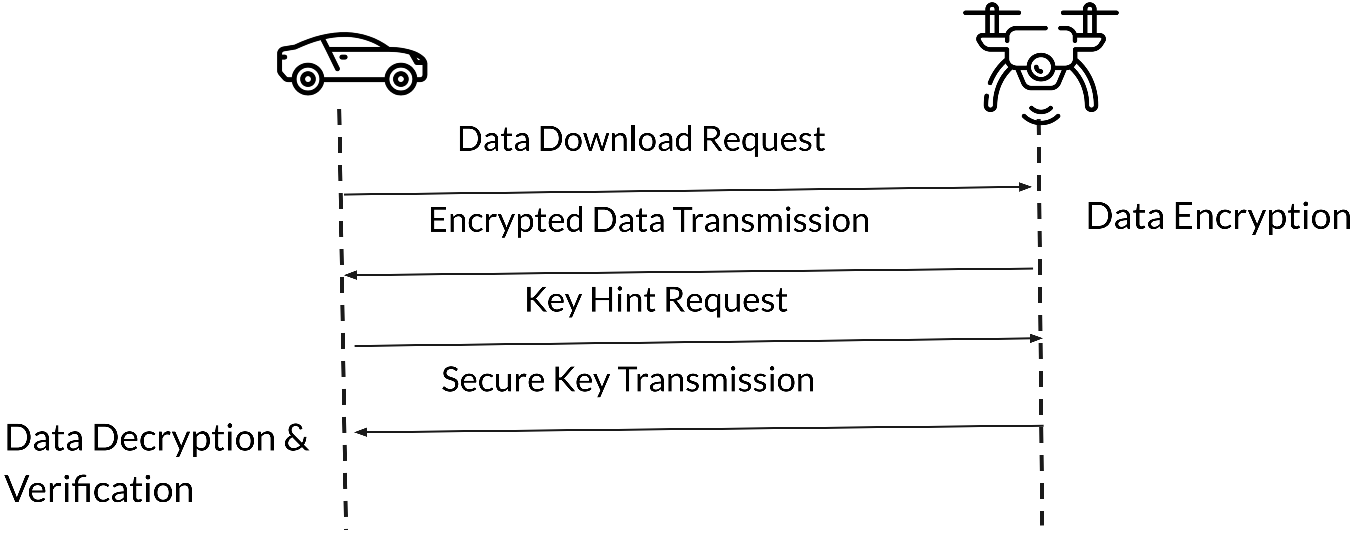


Cui, Jie, et al. "Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme." *IEEE Journal on Selected Areas in Communications*, (2020).

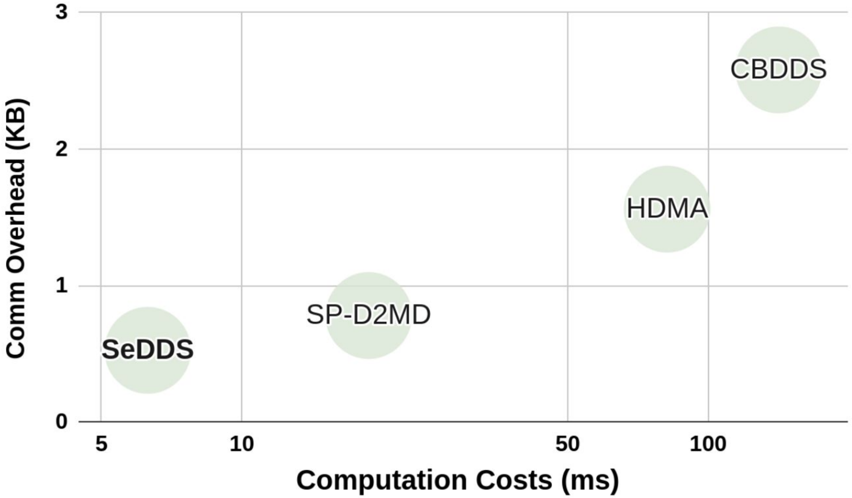
Tan, Haowen, et al. "Rsu-aided remote v2v message dissemination employing secure group association for uav-assisted vanets." *Electronics* 10.5 (2021).

Ko, Yongho, et al. "Drone secure communication protocol for future sensitive applications in military zone." *Sensors* 21.6 (2021).

SeDDS: Secure Direct Data Sharing Steps



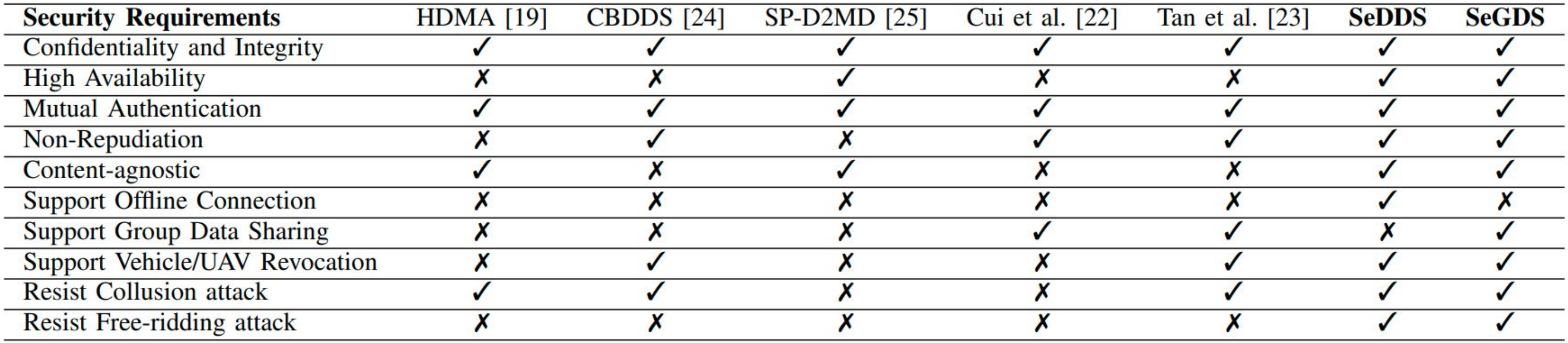
SeDDS Performance Analysis



Wang, Peng, et al. "**HDMA**: Hybrid D2D message authentication scheme for 5G-enabled VANETs." *IEEE Transactions on Intelligent Transportation Systems* 22.8 (2020).

Zhang, Jing, et al. "**CBDDS**: Secure and revocable cache-based distributed data sharing for vehicular networks." *IEEE Transactions on Mobile Computing* (2023).

Security Comparison



Security Requirements	HDMA [19]	CBDDS [24]	SP-D2MD [25]	Cui et al. [22]	Tan et al. [23]	**SeDDS**	**SeGDS**
Confidentiality and Integrity	✓	✓	✓	✓	✓	✓	✓
High Availability	✗	✗	✓	✗	✗	✓	✓
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓
Non-Repudiation	✗	✓	✗	✓	✓	✓	✓
Content-agnostic	✓	✗	✓	✗	✗	✓	✓
Support Offline Connection	✗	✗	✗	✗	✗	✓	✗
Support Group Data Sharing	✗	✗	✗	✓	✓	✗	✓
Support Vehicle/UAV Revocation	✗	✓	✗	✗	✓	✓	✓
Resist Collusion attack	✓	✓	✗	✗	✓	✓	✓
Resist Free-ridding attack	✗	✗	✗	✗	✗	✓	✓

Conclusion and Future Work

- SeGDS and SeDDS are secure and efficient protocols for UAV-assisted VANETs.
  - SeGDS reduces communication costs by 2.5x
  - SeDDS reduces computation overhead by 1.5x.
- Future work
  - Focus on energy efficiency optimization
  - Support threat model with malicious RSUs

Thank you

For more information or questions, please contact:

atefeh@ucsb.edu amohseni.ejiyeh@gmail.com

https://atefehmohseni.github.io/