Defending against Flooding Attacks in the Internet of Drones Environment

Cong Pu and Pingping Zhu
Dept. of CSEE, Marshall University
Huntington, WV 25755, USA
puc@marshall.edu
zhup@marshall.edu

MARSHALL UNIVERSITY

IEEE GLOBECOM

IEEE

Outline

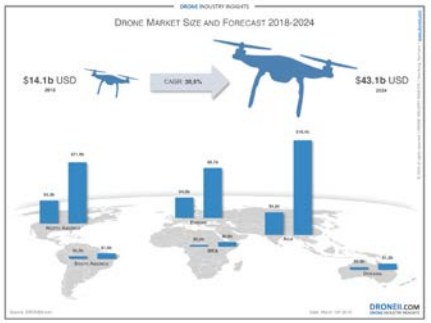
- Introduction & Motivation
- Related Work
- Proposed Flooding Attack Detection
  - System Model
  - Lightweight Distributed Detection Scheme
- Performance Evaluation
- Conclusion

Introduction

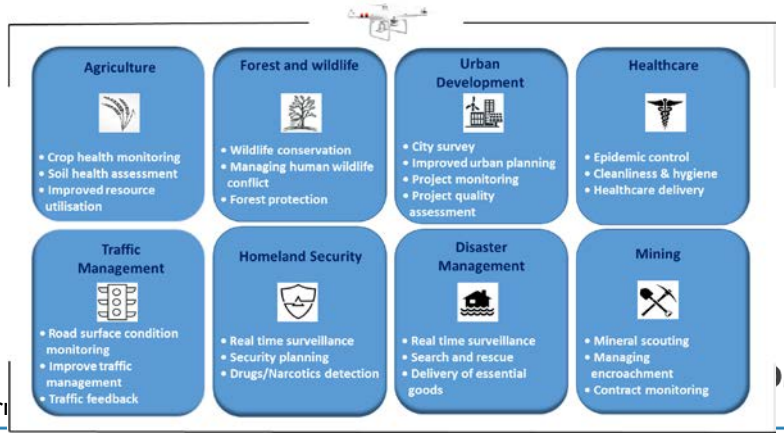
- The potential of drones is being constantly exploited…
  - a military weapon
  - an entertainment tool
  - a machinery that can revolutionize mobile networks



- "Global Drone Market Report 2020-2025"
  - the international drone market is estimated to be around $44 billion by 2024

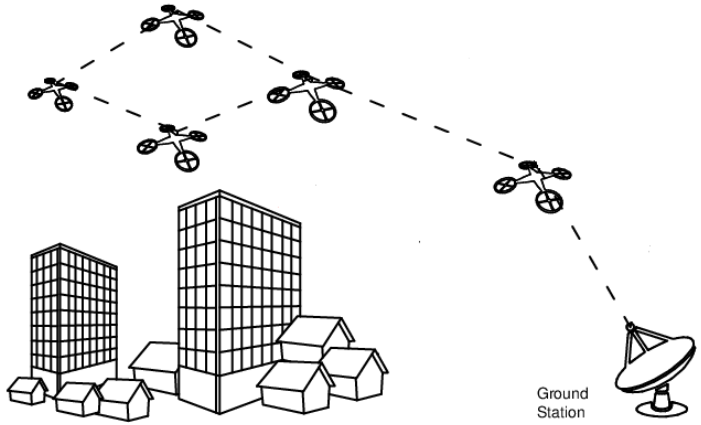


- The demand for drones by various unites is high
  - drones can be flexibly deployed for a wide range of applications



Introduction

- To fully exploit drones, Internet of Drones (IoD) is proposed
  - mobile drones
  - stationary ground stations
    - acts as access point
  - drone-to-drone (D2D) comm.
  - drone-to-ground station (D2I) comm.



- The IoD is lack of persistent connectivity
  - between drone and drone, and between drone and ground station

store-carry-and-forward strategy

the most promising candidate for delivering data in the IoD

a drone stores the received packets in the storage, carries them while flying around, and forwards them to the next-hop drone or destination (i.e., ground station)

Motivation

- As a result of high mobility and resource constraints, the IoD is vulnerable to *flooding attacks*
  - an adversary sends an excessive amount of packets (original or replica) to legitimate drones
    - draining the limited IoD resources such as communication bandwidth and drones' storage space
- *Flooding attacks* has serious consequences
  1. the link expiration time (for D2D and D2I) is short
     - a mass of attack packets waste precious commu. time
  2. the storage capacity of drones is limited
     - buffering attack packets prevent from storing genuine packets
  3. the battery energy of drones is constrained
     - receiving and sending attack packets consume energy power

Motivation (cont.)

- *Flooding attacks* are an old research topic in diverse environments
  - traditional computer network
  - named data networking
  - wireless ad hoc network
  - vehicular ad hoc network
  - etc.

  →
  - no/low mobility is considered
  - exiting schemes do not apply in IoD

- In addition, there is no available work concentrating on flooding attacks and their countermeasures in the IoD
  - our work fill this research gap

Our Contribution

- This paper
  - proposes a lightweight distributed detection scheme (Lids) to defend against flooding attacks in the IoD environment
    1. each drone counts the number of packets that it has sent within a predefined time interval and shares the self-counting report with other drones during contacts
    2. the receiving drones store the self-counting reports while flying and send them to nearby ground station which will check the consistency of self-counting reports to detect flooding attacks

Most Countermeasures in the IoD

- multi-path packet forwarding scheme against jamming attack [14]
  - select multiple paths between src. and des. based on network metrics
  - frequent metrics calculation results in computational overhead
- clustering based scheme against packet dropping attack [15]
  - the behaviors of drones are evaluated and converted into trust
  - non-negligible energy consumption from clustering maintenance
- blockchain based data management framework [17]
  - access control mechanism and secure session key
  - a consensus algorithm for the competition of adding block
  - has several serious vulnerabilities [18]

Most Countermeasures in the IoD

- RREQ flooding attack in wireless ad hoc network [20]
  - Bayesian Inference models and detects RREQ flooding attack
  - no mobility is considered
- intrusion detection system [21]
  - deep neural network technique to combat data flooding attack
  - energy consumption due to running deep neural network tech.
- flooding attack defense scheme in vehicular network [22]
  - the packet traffic of each vehicle is monitored
  - the statistics and traffic flow rules detect flooding attack
  - dense placement of road-side unites (RSU)
    - deployment and operational costs increase

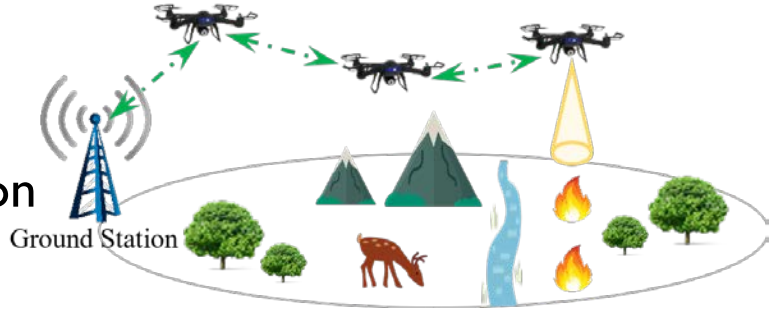
Most Countermeasures in the IoD

- Two important issues should be addressed to detect flooding attacks in the IoD
  - i. intermittent connectivity in the IoD
    - taking advantage of store-carry-and-forward strategy
  - ii. integration with off-the-shelf routing protocols
    - designing countermeasure as a network layer add-on module

- This paper provides
  - in-depth analysis of flooding attacks
  - countermeasure against flooding attack
    - Lids: Lightweight Distributed Detection Scheme
  - bridge the research gap

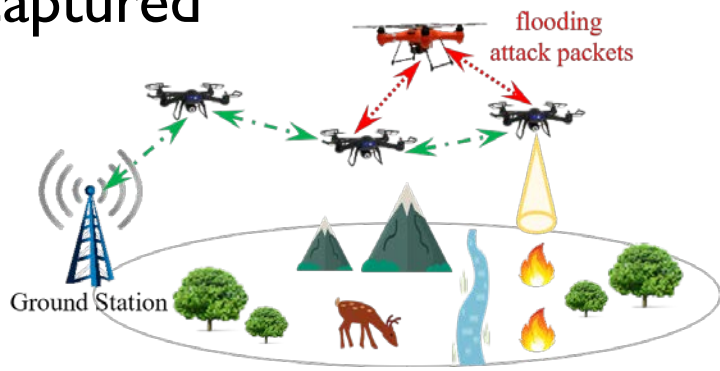
Lids:
System Model

- A genetic IoD scenario (i.e., search and rescue)
  - a set of drones is deployed in the area
  - when a drone detects an event
    - generates data packets
    - sends them to nearby ground station
      - multi-hop relays
  - end-to-end forwarding path does not always exist
    - store-carry-and-forward strategy
      - stores received packets
      - carries them while flying
      - forwards them to next-hop (i.e., drone or ground station)
  - drone has limited storage space
    - a timer is used to purge stale packets
  - public-key cryptography [23] is being utilized



Lids:
Adversary Model

- In wide-open airspace, drones can be captured
  - compromising legitimate drones
  - making them behave maliciously



- The primary goal of adversary
  - flooding a large number of original or replica packets
  - draining the limited IoD resources
    - communication bandwidth
    - drones' storage space and energy resource

Lids:
Lightweight Distributed Detection Scheme

- When the drone (i.e., ID_a) joins the IoD, it registers at the certificate authority (CA)
  - negotiate an agreement on the packet send rate, RT_a^{pkt}.
    - RT_a^{pkt}: indicates the number of packets that the drone can send within a pre-defined time period, T^{ω}.
      - if the drone sends more packets than RT_a^{pkt}, it is suspected as adversary.
  - the CA issues a digital certificate, $CERT_a$, to the drone ID_a
    - $CERT_a$ includes
      - drone's identity ID_a
      - drone's public key PU_a
      - drone's packet send rate RT_a^{pkt}
      - CA's digital signature
  - the CA also generates a private key, PR_a, and issues it to drone ID_a via a secure channel.

Lids:
Lightweight Distributed Detection Scheme

- When the drone (i.e., ID_a) contacts with another drone (i.e., ID_b)
  - the drone ID_a first sends scheduled packets to drone ID_b
  - the drone ID_a then sums up the number of sent packets, CNT^{pkt} , since the beginning of current time interval, T_i^{ω} .
  - the drone ID_a creates the self-counting report, $RPT_a^{T_x}$, and shares it with drone ID_b
    - $RPT_a^{T_x}$ contains
      - the count of sent packets CNT^{pkt}
      - the contact time T_x
      - drone ID_a's digital certificate $CERT_a$
      - drone ID_a's digital signature SIG_a
      - message authentication code MAC_{T_x}
    - $RPT_a^{T_x} = \{CNT^{pkt}, T_x, CERT_a, SIG_a, MAC_{T_x}\}$
      - $SIG_a = E(ID_a|CERT_a|PR_a)$
      - $MAC_{T_x} = H(CNT^{pkt}|T_x|CERT_a|SIG_a)$

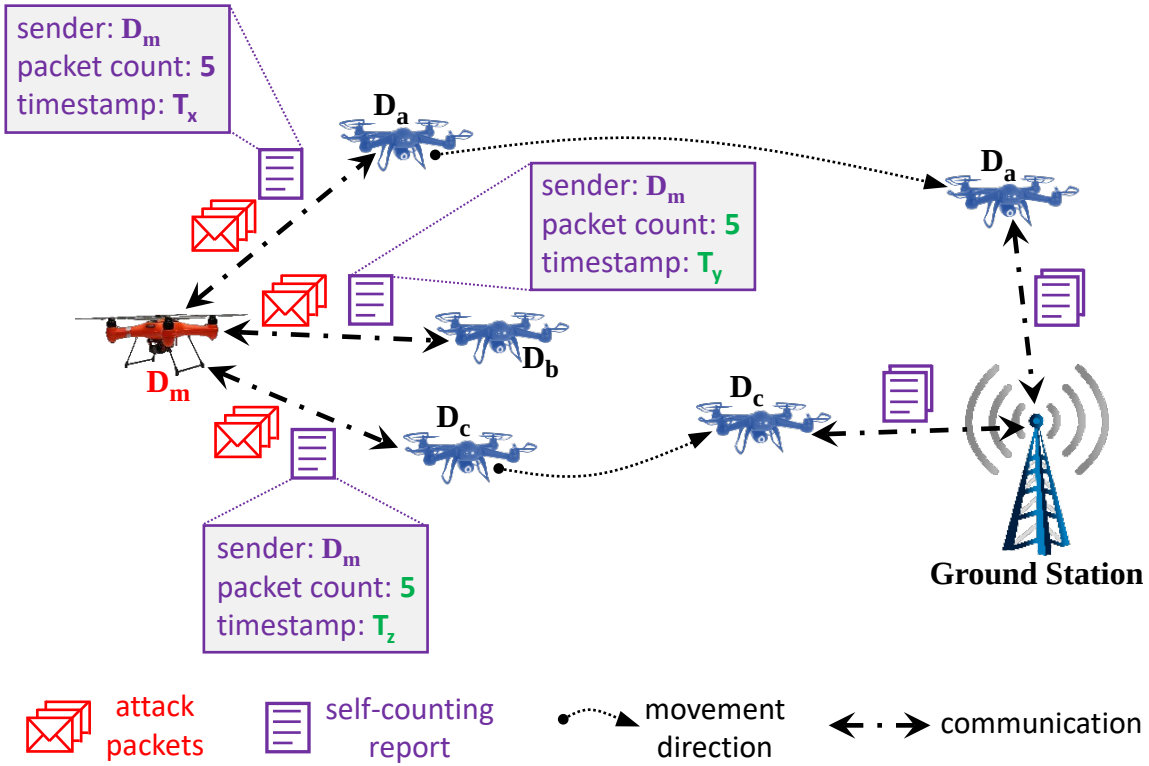
Lids:
Lightweight Distributed Detection Scheme

- After receiving the report $RPT_a^{T_x}$, drone *ID*$_b$ verifies MAC_{T_x}.
  - if MAC_{T_x} is valid, drone *ID*$_b$ verifies SIG_a
    - if SIG_a is valid, drone *ID*$_b$ retrieves the packet send rate RT_a^{pkt} and the digital certificate $CERT_a$, and compares it with the count of sent packets CNT^{pkt}
      - if $CNT^{pkt} > RT_a^{pkt}$
        - drone *ID*$_a$ sends more packets than permitted
        - drone *ID*$_b$ discards all received packets
          - save $RPT_a^{T_x}$ for ground station to detect flooding attack
      - if $CNT^{pkt} \leq RT_a^{pkt}$
        - drone *ID*$_b$ carries received packets and delivers them to next-hop drone or ground station

Lids:
Lightweight Distributed Detection Scheme

- When drone ID_b reaches the ground station, it submits all received self-counting reports
- The ground station will compare the newly received reports with the already obtained reports
  - identify whether a drone issues multiple reports with inconsistent information
    - an adversary may disloyally report a false packet count to avoid detection
    - however, this misbehavior can be easily detected
      - the false packet count must have been reported before by adversary;
      - or the false packet count is smaller than or equal to a packet count which was reported in an earlier self-counting report
  - detect flooding attack

Lids:
Lightweight Distributed Detection Scheme



Performance Evaluation

- Performance metrics
  - Detection Ratio
  - Miss Detection Ratio
  - Detection Latency
  - Energy Consumption

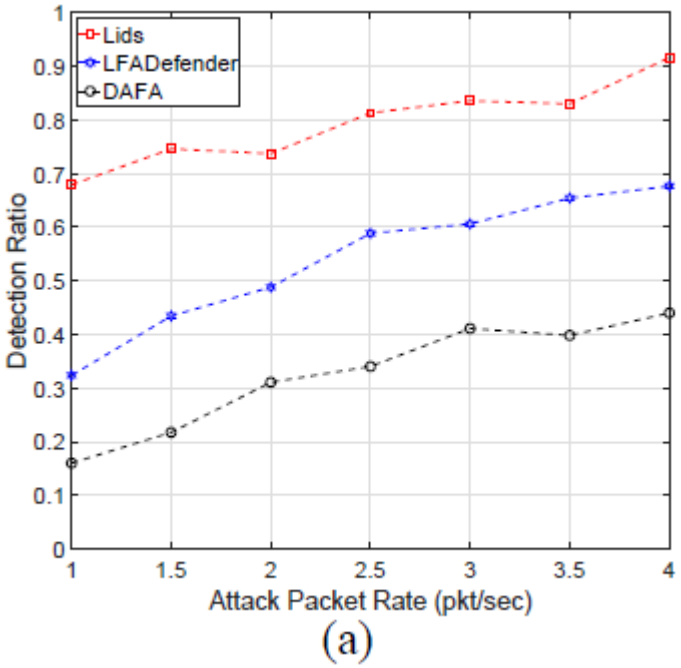
TABLE I
SIMULATION PARAMETERS

Parameter	Value
Network area	$150 \times 150\ m^2$
Number of legitimate drones	35
Number of malicious drones	5
Number of ground stations	3
Moving speed	15 meter/sec
Mobility model	Random waypoint
Communication range of drone	12.59 meters
Communication range of ground station	50 meters
Radio data rate	3 Mbit/sec
Packet size	127 bytes
Attack packet rate	1.0 - 4.0 pkt/sec
Simulation time	10,000 seconds

- Benchmark schemes
  - DAFA [12]
    - packet transmission rate
  - LFADefender [13]
    - packet loss rate, round-trip time, and available bandwidth

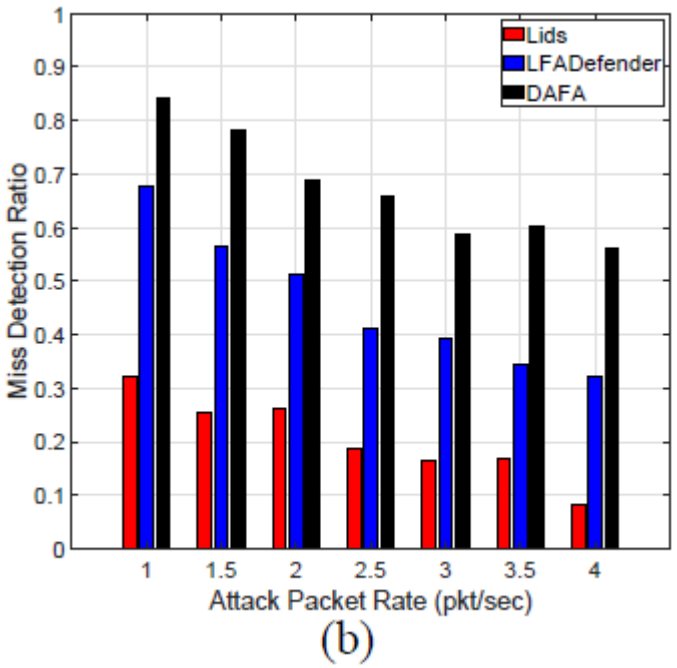
Performance Evaluation (cont.)

Detection Ratio



(a)

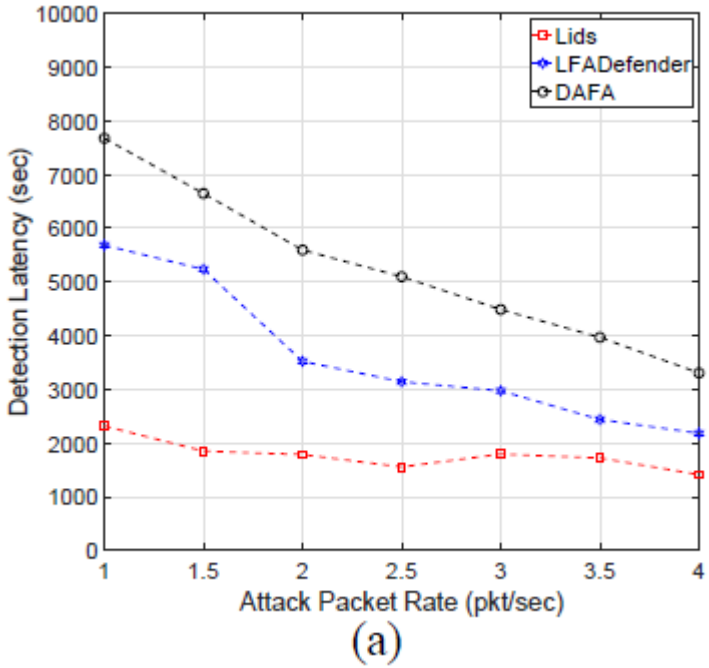
Miss Detection Ratio



(b)

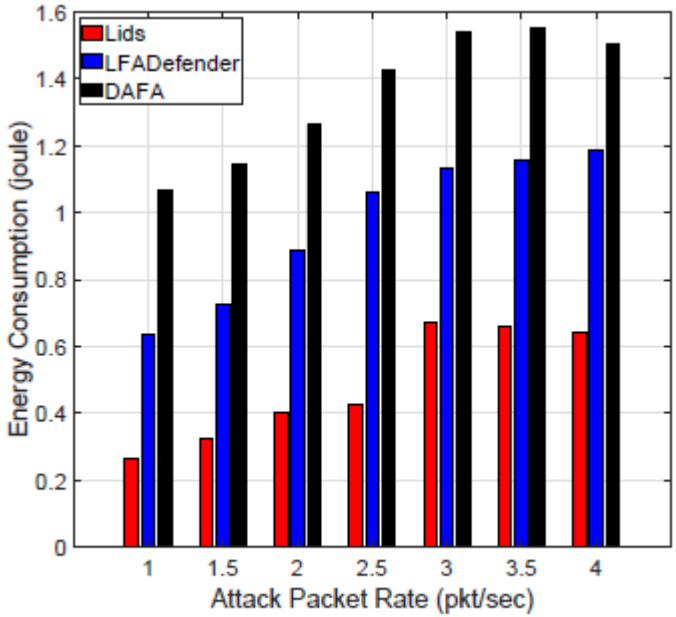
Performance Evaluation (cont.)

Detection Latency



(a)

Energy Consumption



(b)

Concluding Remarks

- Develop a lightweight distributed detection scheme to defend against flooding attacks in the IoD environment
  - each drone counts the number of sent packets and shares the self-counting report with other drones
  - the receiving drones store the self-counting reports and send them to the nearby ground station
  - the ground station evaluates all self-count reports to detect flooding attack

- Under investigation…
  - a large number of self-counting reports to be exchanged
  - data reduction strategy
  - a real-world testbed to explore the full potential of *Lids*

Any Questions?