Adaptive Resource Reservation to Survive Against Adversarial Resource Selection Jamming Attacks in 5G NR-V2X Distributed Mode 2

Jason Li
CPE 490B Fall 2022
Professor Du

Intro to Direct SideLink Communications

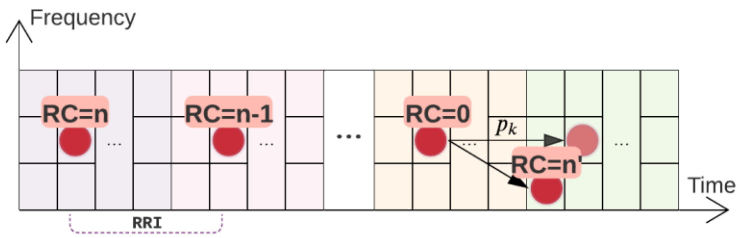
- Controls communication in order to control vehicles
- Done through radio:
  - Centralized Mode
    - Base station manages resource allocation
  - **Distributed Mode**
    - Vehicles manages resource allocations

Semi Persistent Scheduling Algorithm (SPS)

- Used in Distributed Mode
- Allocates radio resources via neighbor vehicle patterns
    - Transmits # of consecutive packets once the resource is decided via a saved frequency

Resource scheduling procedure (RSP)

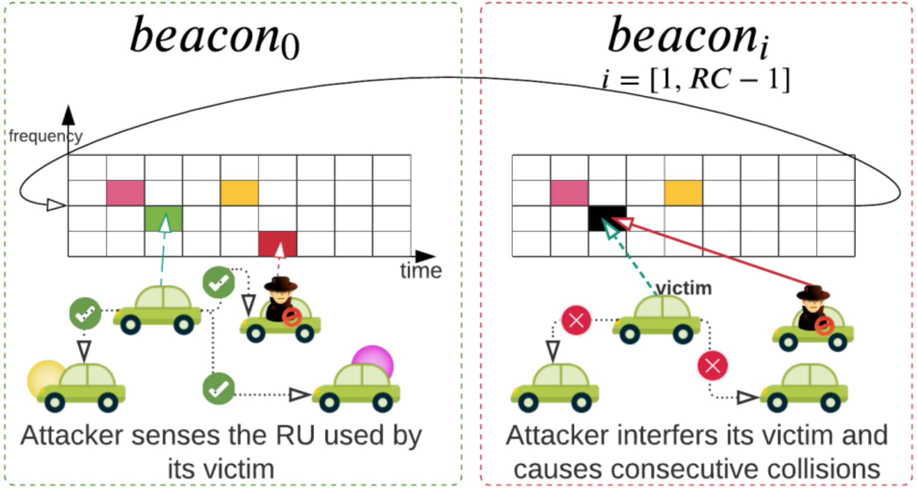
- Resource Reservation Interval (RRI)
  - Time interval between 2 consecutive packets
  - Constant value (any multiple from 100 ms to 1s)
- Re-selection Counter (RC)
  - # of transmissions before new resource is transmitted
  - Random # between 5-15
  - Value of RC decreases until 0 after each transmission



EITHER the reserved resource is kept, or a new RSP is triggered at a lower frequency

Interfering with the Signal

- Distributed allocation can minimize communication collisions in vehicular systems
- Malicious vehicles can block the distribution signal
- Adversarial resource selection: disrupt vehicle network especially for emergencies leading to accidents and fatalities



Improving the SPS Scheme

Protect SPS scheme by:

1. Developing alert system regarding collisions
2. Dynamically changing the SPS based on whether an attack happens

- Reduces attacks on packet drops
- Improves packet delivery ratio

***Attacker strategy** and intuitive solutions*

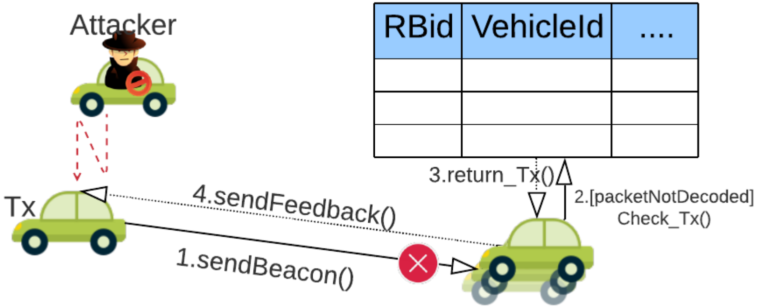
- Attacker causes mass collisions
- Tracks vehicle and follows it
- Attack can last *RC-1* times (victim transmits 1st beacon message correctly)
  - Attacker collects info needed to repeat attack
- Multiple attackers ensure victims are distinct
- Non-aggressive jammers (minor impact)

*Attacker strategy and **intuitive solutions** (cont.)*

- Enable targeted vehicles to select new resource after each sent beacon (RC = 1)
  - Makes attack useless + futile
  - Increases number of legitimate packet collisions w/ no resource reservation
- Make RC adaptive
  - If vehicle is attacked, consecutive resource reselections are made after each RRI; outcompete the attacker
  - Victim gradually increases its reservation period; repeats if new attack is detected

Attack detection strategy

- Blind re-transmission applied to ensure high reliability and handle packet collisions
- Unable to detect attacks in half duplex broadcast
- Neighboring nodes may detect transmitted beacon message (high received signal on resource) but fail to decode it, so transmitter (Tx) is unknown
- Reservation mechanism: neighboring vehicles check table of last received beacons.
    - If resource reserved before (Tx can be identified easily and confidently)



After failing to find the value in the reservation table, close neighboring vehicles (within range of victim) must provide feedback reporting collision's occurrence to the table

Attack detection strategy (cont.)

- Suppose feedback is sent in unicast mode
- Feedback is aborted if it is considered obsolete
- Assume feedback is always correctly received
- If feedback ratio of transmitted beacon is greater than threshold, vehicle considers packet as dropped and trigger resource re-selection
- Feedback ratio = $\frac{\#\ of\ received\ feedback}{\#\ of\ neighboring\ vehicles}$
  - Threshold is used for false positive alarms reduction due to infrequent legitimate collisions, and for trust concerns due to malicious nodes injecting false feedback

Algorithm 1 FeedBackListener

Input: fb: FeedBackMessage
number_feedback: Array[][]
$number\_close\_neighbors$: Integer
Output: number_feedback

if Check_RU(fb.RU$_{id}$) **then**
  number_feedback[fb.RU$_{id}$,fb.t] ++
  $\alpha \leftarrow \frac{number\_feedback[fb.RU_{id}, fb.t]}{number\_close\_neighbors}$
  if $\alpha > \phi$ **then**
    RC $\leftarrow$ 0
  end if
end if

Attack mitigation strategy

- Victim must update RC value to reselect new radio resource if attacked
- Fuzzy inference system (FIS) decides reservation period of each next selected resource
  - Powerful decision-making algo
- Four main modules of FIS:

1. Set of rules forming knowledge base
2. Fuzzy inference engine
3. De-fuzzifier
4. Fuzzifier
   - Two inputs relevant for corresponding output (RC value)

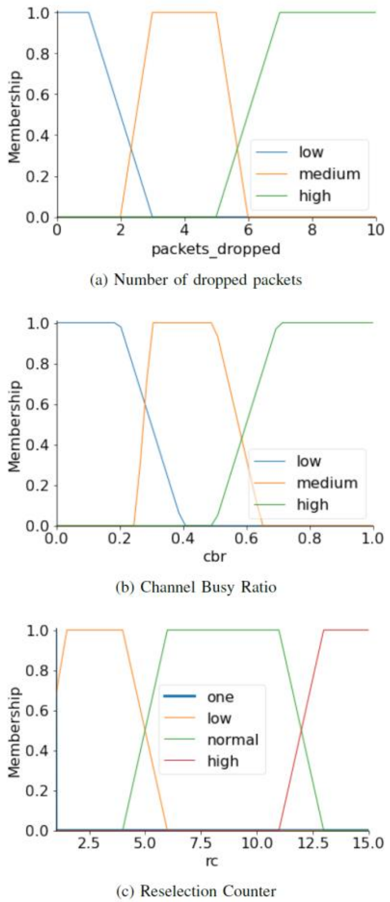
Algorithm 2 Ressource Reservation

```
Require: RC == 0
   {SPS Scheme}
   channelSensing()
   RU ← ressourceSelection()
   cbr ← calculateCBR()
   {Updating RC}
   RC ← fis(number_feedbacks[:,t-Λ:t],cbr)
```

Attack mitigation strategy (cont.)

Fuzzy Sets

- **Number of Dropped Packets** in observation interval helps classify collisions as legitimate or malicious, through three linguistic values: low, medium and high
- **Channel Busy Ratio** (CBR) represents time ratio channel is sensed as busy on total observation time based on SPS. Higher CBR, more vehicles will struggle in finding resource and causes channel congestion. Depends mainly on vehicle density
- **RC value** is output of FIS. 4 linguistic values: One (fuzzy singleton), Low, Normal, and High.
  - One is used when trying immediately to escape from attacker. Low represents gradual increase towards Normal state as defined in standards.
    - High: RC values are greater than 10



(a) Number of dropped packets

(b) Channel Busy Ratio

(c) Reselection Counter

Fig. 4: Fuzzy sets.

Attack mitigation strategy (cont.)

- Allow vehicles to escape by consecutively changing resources when attack occurs
- Avoid constant resource reselection when legitimate collisions are produced
  - Congested traffic has high CBR or frequent change of resource
- Fuzzy rules for decision making validation for inference systems
  - Ensures inference system finds right trade-off between necessity of consecutively changing resource to escape attacks, and staying on same resource when legitimate collisions occur

Inputs		**Output**
Dropped Packets	**CBR**	**RC**
HIGH	-	ONE
MEDIUM	HIGH	NORMAL
MEDIUM	LOW	ONE
MEDIUM	MEDIUM	LOW
LOW	HIGH	NORMAL
LOW	MEDIUM	NORMAL
LOW	LOW	HIGH

TABLE I: Fuzzy rules examples.

Attack mitigation strategy (cont.)

1. If packets dropped is high, attack is happening regardless of CBR value
2. Set RC to one in order to escape attacker
3. If packets dropped is medium, it is difficult to deduce if it came from an attack or legitimate collisions
4. Check CBR value to devise optimal strategy

- High CBR: changing RC will likely cause collisions with other neighboring vehicle since probability of finding available resource is low
- Medium CBR: available resources will allow vehicle to escape attack or avoid legitimate collisions by gradually diminishing RC to increase rate of reselection
- Low CBR: system will not suffer any side effects; therefore, it is better to put RC to one in order to clear out of any kind of collisions
- As for case of low number of packets dropped, RC is kept to normal except when CBR is low. In that event, high value is assigned to RC thereby slowing down re-selection procedure

De-fuzzification: centroid method $x^* = \frac{\int u(x) x dx}{\int u(x) dx}$ where: x* is output value, u(x) is RC membership value for point x

Simulation and Results

- 2 km road of 3 lanes per direction for 20 seconds
- Poisson distribution in positioning
- Vehicles send beacon packets at 10HZ frequency w/ transmission power of 23 dBm
- Two main 2 sub-channels per sub-frame are used by vehicles to send their packets and hence 200 resources
- Compare scheme performance to SPS according to Packet Reception Ratio (PRR)
  - PRR: ratio between # of vehicles that correctly receive beacon packets and total # of vehicles within range
- # of attackers = 0, 1, 5, 10
- Packet is presumed dropped if threshold is greater than or equal to .3
- Observation period is 20

Simulation and Results (cont.)

- 0 attacker case: decreasing PRR due to legitimate collisions
- No great difference between 0 and 1 attacker (difference noticeable for low-density scenarios of 50 to 75 vehicles)
  - PRR value decreases as density increases
- High-density scenarios: difference in PRR becomes truly small (~2% for 0-5 attackers, 4% for 0-10 attackers in each scenario)
- Average PRR value stays above 87% for all
- Low effectiveness of attacks on entire system (non-aggressive)

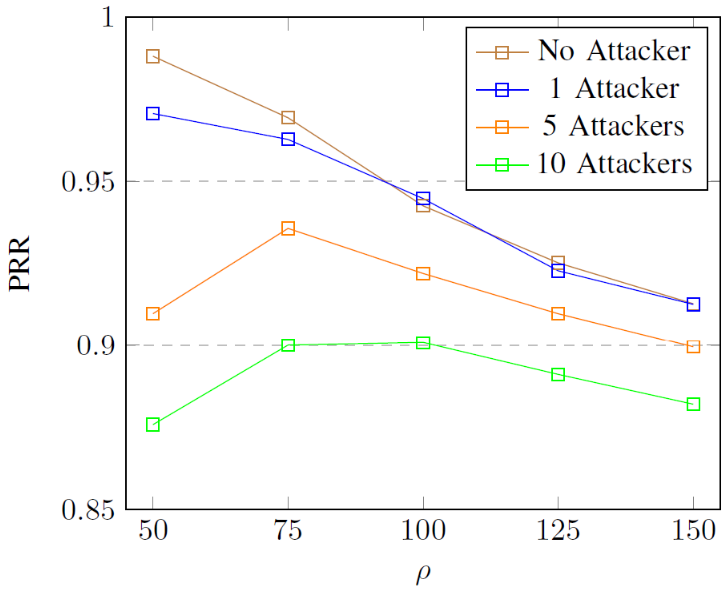


Fig. 5: Impact of adversarial resource selection attacks on PRR.

Simulation and Results (cont.)

- Vehicle density = 150 vehicle/km
- PRR of 3 vehicles:
  i. Vehicle A: safe (not attacked)
  ii. Vehicle B: attacked and does not implement approach
  iii. Vehicle C: attacked and approach implemented
- Cumulative distribution function (CDF) shows 10% of packets sent by vehicle B have PRR equal to one, extremely low compared to vehicles A and C (60% & 55%)
- Vehicle B most impacted 85% of packets have PRR less than 20% (vehicle basically isolated)
  - PRR of Vehicle C is close to safe vehicle A (65% of packets have PRR higher than 80% [77% for safe vehicles])

Higher PRR compared to SPS means its effective in defending adversarial resource selection attacks; improved due to feedback and RC adaptability

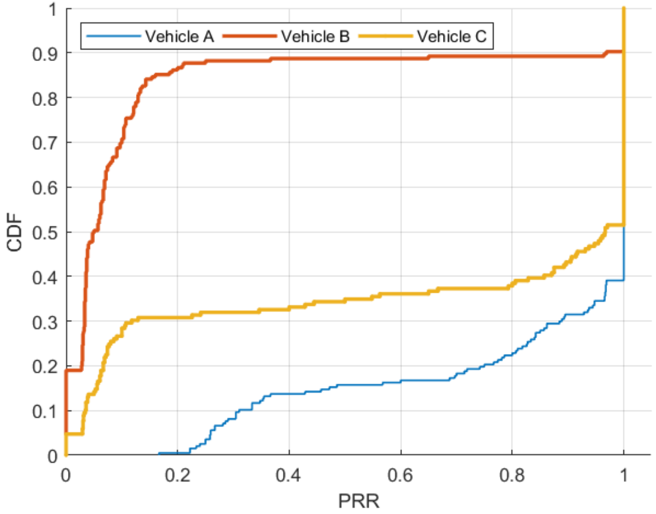


Fig. 6: Cumulative distribution function of PRR

Conclusion

- Improved version of SPS algorithm to deal with adversarial resource selection jamming attacks
- Feedback mechanism alerts vehicle when packets fail to transmit
- Optimal defense strategy against packet-dropping attacks using fuzzy logic
  - Dynamically adjust re-selection counter value as key parameter in semi persistent schemes
- Simulation: scheme can significantly reduce effectiveness of stacks, even if there are many
- Outperforms SPS scheme via PRR by minimizing number of legitimate collisions
- Investigate other decision-making techniques (machine and reinforcement learning)

Works Cited

T. Eddine Toufik Djaidja, B. Brik, S. Mohammed Senouci and Y. Ghamri-Doudane, "Adaptive Resource Reservation to Survive Against Adversarial Resource Selection Jamming Attacks in 5G NR-V2X Distributed Mode 2," ICC 2022 - IEEE International Conference on Communications, 2022, pp. 3406-3411, doi: 10.1109/ICC45855.2022.9839023.

THANK YOU!