

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

Jason Li
EE 582 Fall 2023
Professor Yao



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

Direct SideLink Communications controls vehicles. This is done through radio. Centralized mode has the base station manage resource allocation. The one we are focusing on is distributed mode where the vehicle manages resource allocations. If you zone out during this presentation, this basically is useful for self driving cars and how disruption attacks can be prevented.

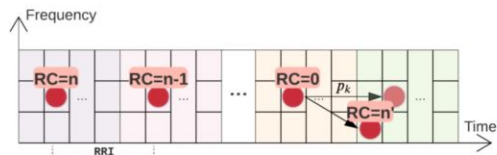
Semi Persistent Scheduling Algorithm (SPS)

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

A Semi Persistent Scheduling Algorithm is used in Distributed Mode. It allocates radio resources via patterns from neighboring vehicles. It transmits the resource through a # of consecutive packets on a saved frequency.

Resource scheduling procedure (RSP)

- Resource Reservation Interval (RRI)
 - Time interval between 2 consecutive packets
 - Constant value (20, 50 or 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



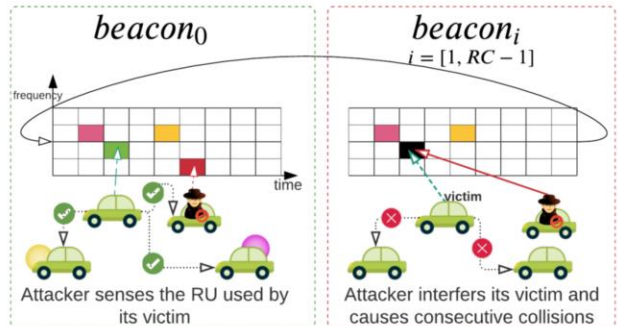
EITHER the reserved resource is kept, or a new RSP is triggered at a lower frequency

The resource scheduling procedure involves these 2 factors: Resource reservation interval is the time interval between 2 consecutive packets. It is a constant value of any multiple from 100 ms to 1 s.

The re-selection counter is a random number (between 5 to 15) of transmissions before a new resource is transmitted. This RC will decrease by 1 after each transmission until it hits 0.

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



Distributed allocation can minimize communication collision in vehicular systems. Compared to the centralized mode, communication doesn't have to travel a far distance and can lead to a quicker response. With the car network, the system can be better utilized. However, malicious vehicles can block the distribution signal. Adversarial resource selection is performed which disrupts the vehicle network especially for emergency services leading to accidents and fatalities. In the grid, the head car after the first beacon sends background info to nearby cars in the network including our disruptor. With this info, they are able to jam the next RSP to prevent the RC from counting down.

Improving the SPS Scheme

Protect SPS scheme by:

1. Developing feedback alert system regarding collisions
2. Fuzzy inference system as optimal defense policy
 - Dynamically changing the SPS based on whether an attack happens
 - ◎ Reduces attacks on packet drops
 - ◎ Improves packet delivery ratio

Related Works


- ◎ Channel Surfing
 - Continuously switching channel
- ◎ Spatial retreat
 - Move mobile nodes to safe place outside interference
 - Too cramp for moving vehicle networks
- ◎ Evasive maneuver – switch to random different sub-frame of same sub-channel for RU; collision in SL Control Info (SCI)
 - Increases # of collisions due to unreserved RU but reduces attacker prediction
 - Another attacker can act as feedback provider and abort detection

Related Works (continued)

- ◎ Reserve and allocate multiple resources alternatively to reduce continuous collisions
- ◎ Terminals transmit explicit feedback about current channel conditions and acknowledges radio resources that have been successfully decoded
 - Designed candidate resource selector to extend sensing range and reduce number of hidden terminal situations



Attacker strategy and intuitive solutions

- ⊙ Attacker wants to causes max mass collisions
 - ⊙ Tracks vehicle down and follows it
 - Attacker in internal node and has info from SCI and beacons
 - ⊙ 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
 - ⊙ Attackers are considered 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

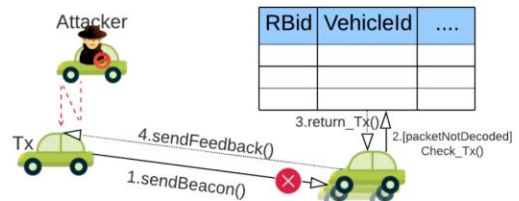
In order to remedy this, targeted vehicles can select a new resource after each sent beacon with $RC = 1$ every time. This makes the attack useless and futile but it increases the number of legitimate packet collisions due to the fact that there's no resource reservation process. It's just going to $RC = 1$ to $RC = 0$.

Another strategy involves making RC adaptive. If a vehicle is attacked, consecutive resource reselections are made after each resource reservation interval to outcompete the attacker. It may look like the vehicle spams RRI, but victim gradually increases its reservation period. The attacker will be in a time-lost situation to not wait. Then, this process repeats if a new attack is detected making the attack not futile to the jammer. It basically randomizes the reservation process so attackers will have less of a shot of being able to intercept unless they have the algorithm with them. We shouldn't be giving it to them and they're probably not smart to understand it.

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

Each car has its own transmitter (Tx) value. A car checks a table to see if it's good. If a hacker hacks, they'll have a different Rbid and VehicleId so the transmission will not be valid.

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 = $\frac{\# \text{ of received feedback}}{\# \text{ of neighboring vehicles}}$
 - 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

```
1: if Check_RU(fb.RUid) then
2:   number_feedback[fb.RUid,fb.t] ++
3:    $\alpha \leftarrow \frac{\text{number\_feedback}[\text{fb.RU}_{id}, \text{fb.t}]}{\text{number\_close\_neighbors}}$ 
4:   if  $\alpha > \phi$  then
5:     RC  $\leftarrow$  0
6:   end if
7: end if
```

So with this algorithm, an array is created with feedback and a constant of close neighbors. If the transmission fails, the feedback counter will be upped by 1. Alpha will equal the number of feedback divided by number of close vehicles after the loop. If the value is above a specified threshold, the RC value will be set to 0, packets will be considered dropped and resource re-selection will begin.

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}

1: channelSensing()

2: $RU \leftarrow \text{ressourceSelection}()$

3: $cbr \leftarrow \text{calculateCBR}()$

{Updating RC}

4: $RC \leftarrow \text{fis}(\text{number_feedbacks}[:,t-\Delta:t], cbr)$

With this strategy, RC values have to be updated to reselect new radio resource if needed. Since RC values are redetermined, a random value fuzzy inference system (FIS) decides a new random reservation period of each next selected resource.

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

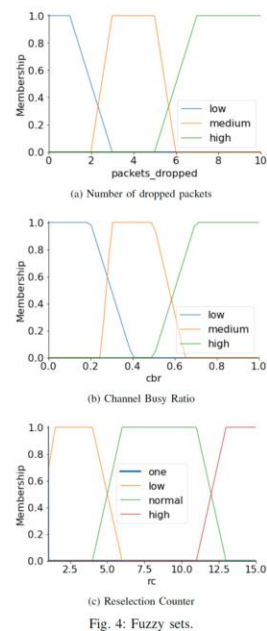


Fig. 4: Fuzzy sets.

Fuzzy sets are determined by three factors: number of dropped packets (analyzed of attack) classifies collisions as legitimate or malicious (low, medium, high) Channel Busy ratio (CBR) is time ratio channel is sensed as busy on total observation time based on SPS. Higher CBR means more vehicles will hog the network to find resources and causes congestion. This is based on vehicle density. RC value is the output of FIS. 4 linguistic values: one (fuzzy singleton), low, normal, and high. These linguistic groups will go to the higher densities (one -> low -> normal -> high) for as long an attack is sensed.

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.

The victim vehicle will basically be switching up the numbers randomly as an attacker is figuring out how to take em down. The fuzzy rule for decision making validation for inference systems ensures that it's approximately equal between consecutively changing resource to escape attacks and providing functionality for legitimate collisions.

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

A High CBR means that the computer network is packed with transmissions leading to a crash. The medium CBR will either escape attack or avoid legitimate collisions by reducing RC to cause the system to reselect and use fuzzy set to change the RRI interval to evade attackers. Low CBR is our “let’s outspeed this person and will automatically start going ham on the changing of RRI intervals.

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

If PRR is high compared to control, the method implemented can be successful for preventing attacks.

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)

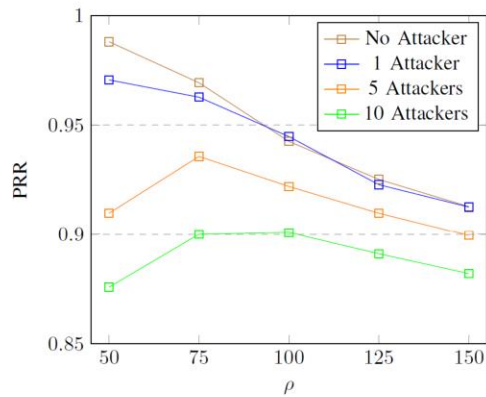


Fig. 5: Impact of adversarial resource selection attacks on PRR.

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

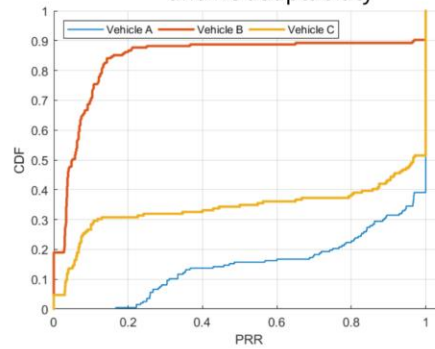


Fig. 6: Cumulative distribution function of PRR

Simulation and Results (cont.)

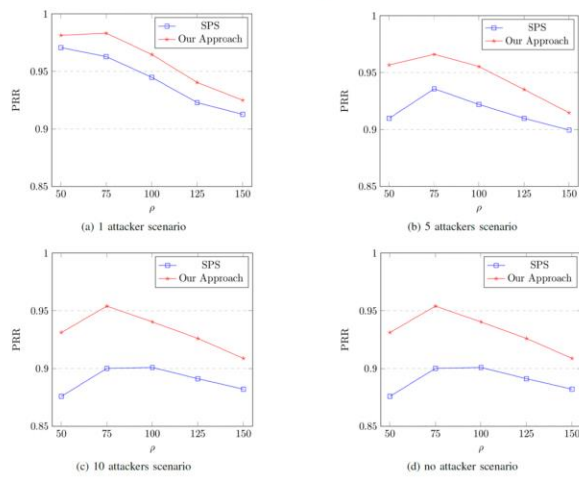


Fig. 7: SPS vs. defending approach

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!