Vehicle-to-Vehicle Message Content Plausibility Check through Low-Power Beaconing

***Taeho Kim*, Hyogon Kim**

Department of Computer Science and Engineering

Korea University

VTC2017-Fall

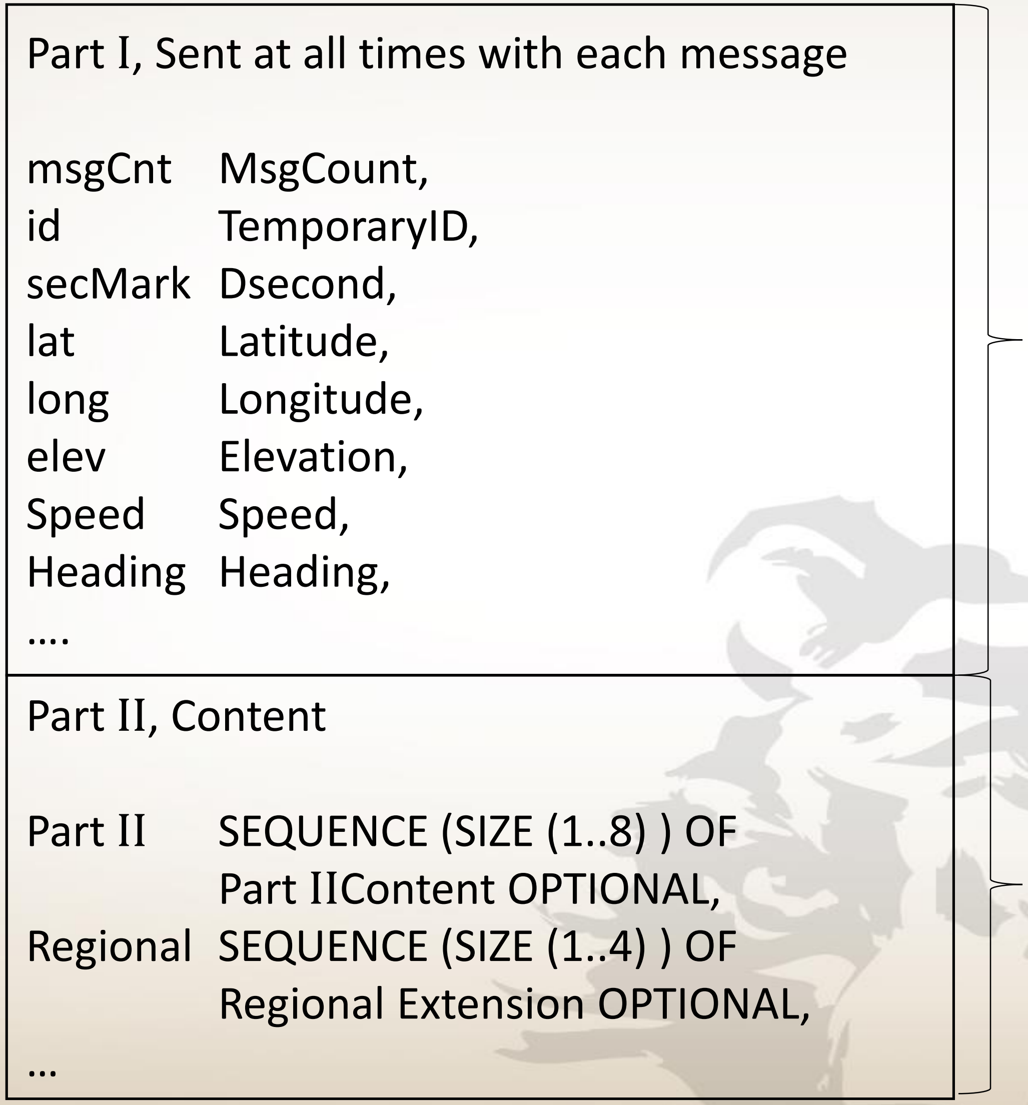
September 24-27 2017, Toronto, Canada

Outline

- Our question!
- Why is it a problem?
- Solution approach: Neighbor check through low-power beaconing
- Simulation and result
- Expanded solution
- Significance and discussion

Background – Basic Safety Message (BSM)

ex. Frequency: 10 Hz
Transmission power: 23 dBm



```
Part I, Sent at all times with each message

msgCnt    MsgCount,
id        TemporaryID,
secMark   Dsecond,
lat       Latitude,
long      Longitude,
elev      Elevation,
Speed     Speed,
Heading   Heading,
….
```

Compulsory

```
Part II, Content

Part II   SEQUENCE (SIZE (1..8) ) OF
          Part IIContent OPTIONAL,
Regional  SEQUENCE (SIZE (1..4) ) OF
          Regional Extension OPTIONAL,
…
```

Optional

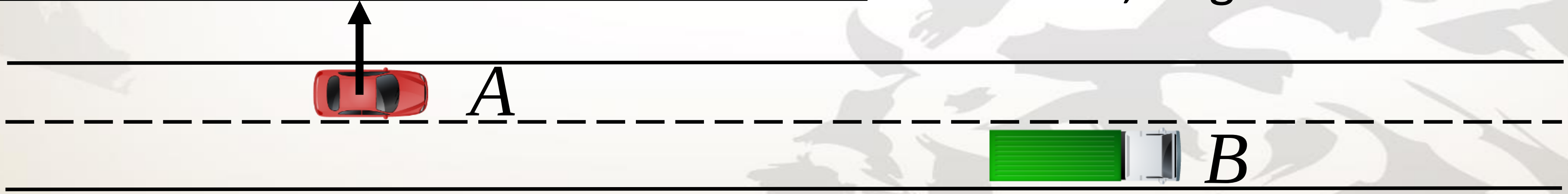
Our Question!

- How can we believe vehicle-to-vehicle message contents?
  - IEEE 1609.2 addresses the security aspect in WAVE except for plausibilility
  - Authorized vehicle (O), Message credibility (O), **Message contents plausibility (X)**

<A's checking list for B>

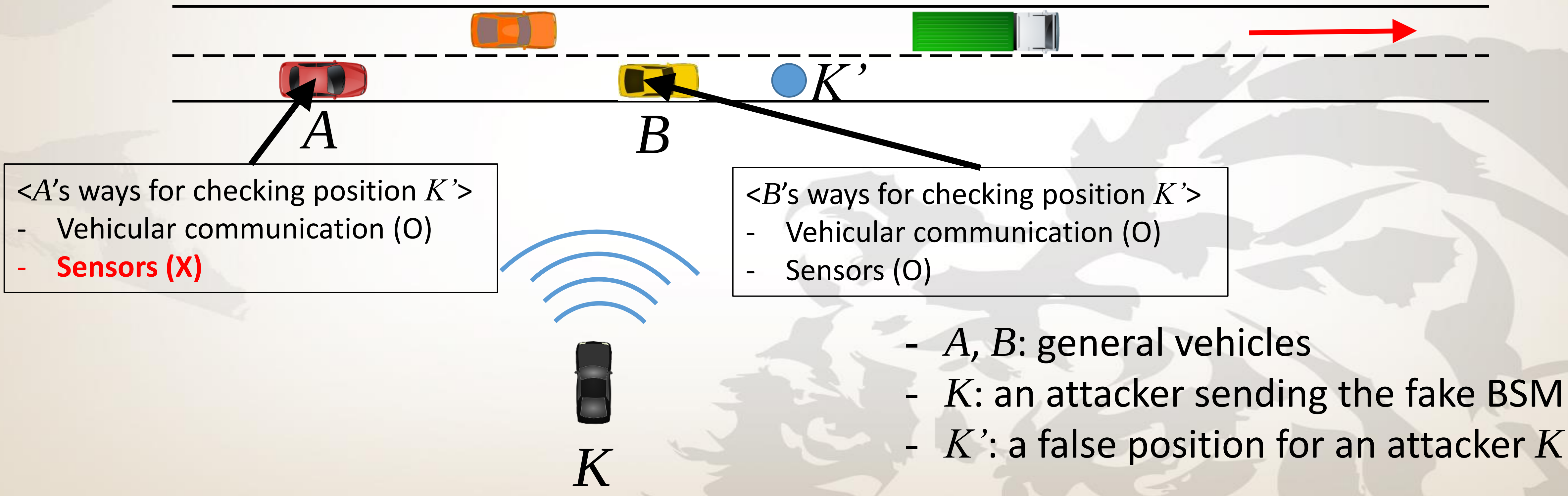
- The existence of B (O)
- Not change B's BSM after sending (O)
- **Check whether the data of B are plausible or not (X)**

- A, B: general vehicles



Why is it a problem?

- An attacker can send its forged message directly near the road
- There may exist a myriad of attacks



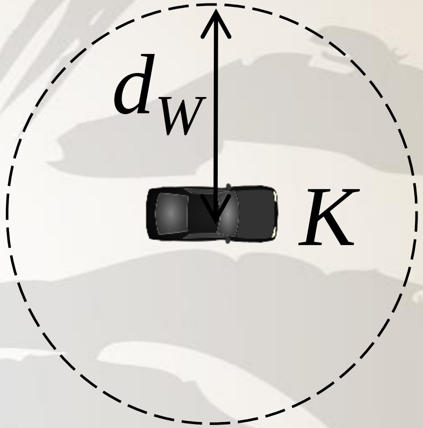
<A's ways for checking position K'>
- Vehicular communication (O)
- **Sensors (X)**

<B's ways for checking position K'>
- Vehicular communication (O)
- Sensors (O)

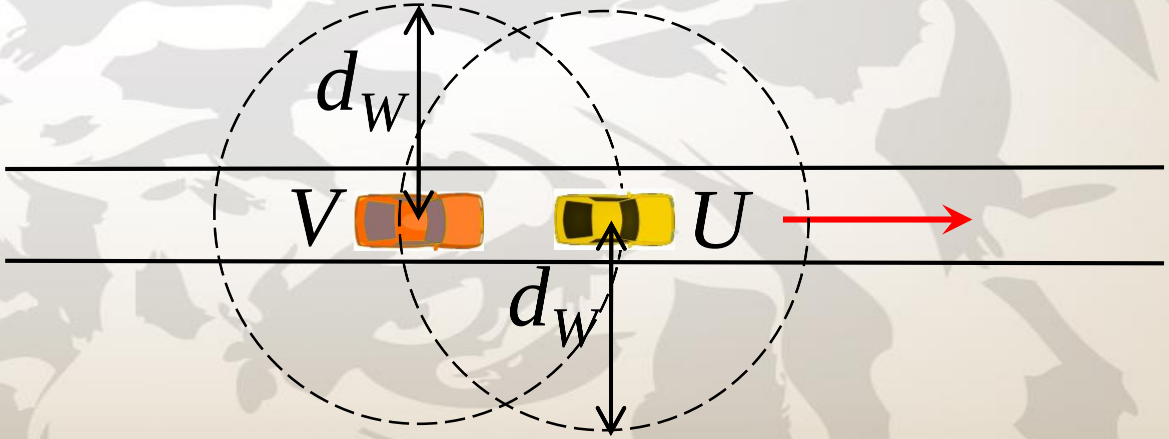
- A, B: general vehicles
- K: an attacker sending the fake BSM
- K': a false position for an attacker K

Solution approach

- Solution: Add low-power beaconing message (Whisper) for BSM contents verification
  - good : not need hardware components or sensors



- The maximum low-power beaconing distance $(ex.170m)$ is lower than the maximum BSM beaconing distance $(ex.760m)$



- V, U: general vehicles
- K: an attacker sending the fake BSM
- d_W: the maximum low-power beaconing distance

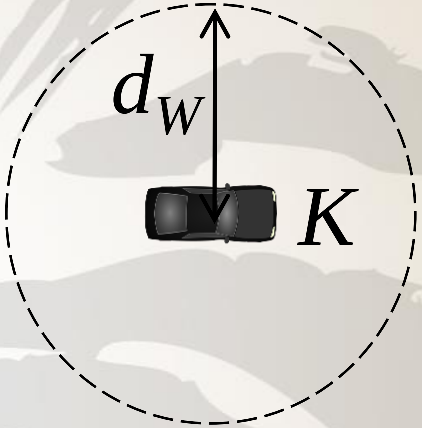
Neighbor check through low-power beaconing (Whisper check)

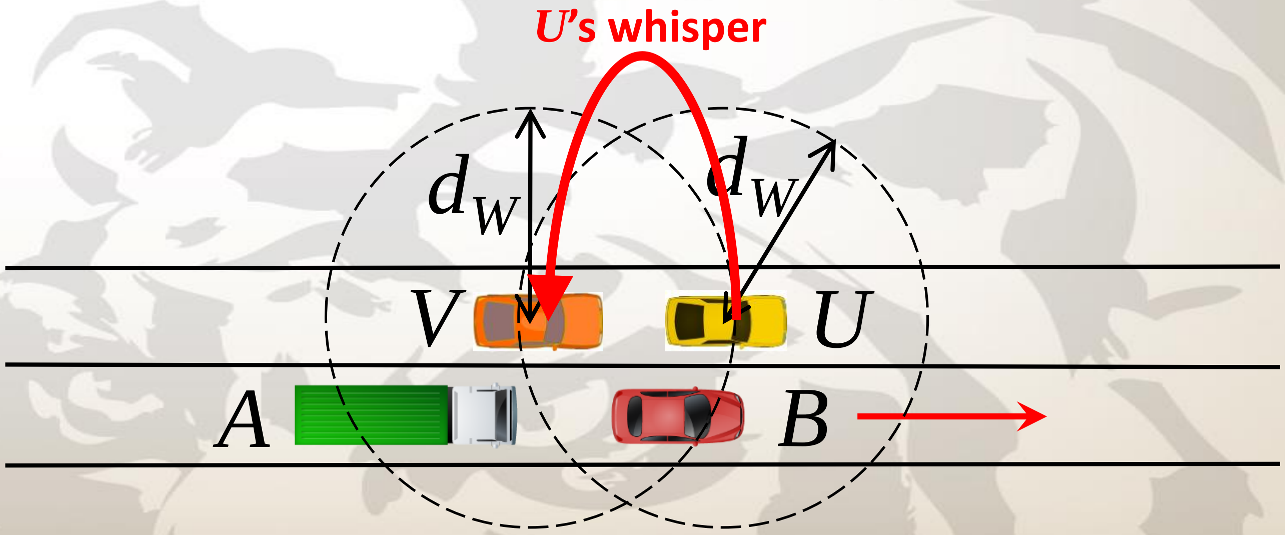
- Vehicle V's Whisper
  - $\boldsymbol{dig(C_V)}$**: digest of** ***V*****'s certificate**
  - I_V: Whisper identifier (WID) of V
  - L_V: list of WIDs heard by V
- Vehicle V's BSM + Certificate
  - $\boldsymbol{dig(C_V)}$**: digest of** ***V*****'s certificate**
  - Part 1 data (Compulsory)
  - Part 2 data (Optional)

- V, U, A, B: general vehicles
- K: an attacker sending the fake BSM
- d_W: the maximum low-power beaconing distance

V's whisper :

$dig(\boldsymbol{C_V})$	I_V	$L_V = \{I_A, I_B, \boldsymbol{I_U}\}$

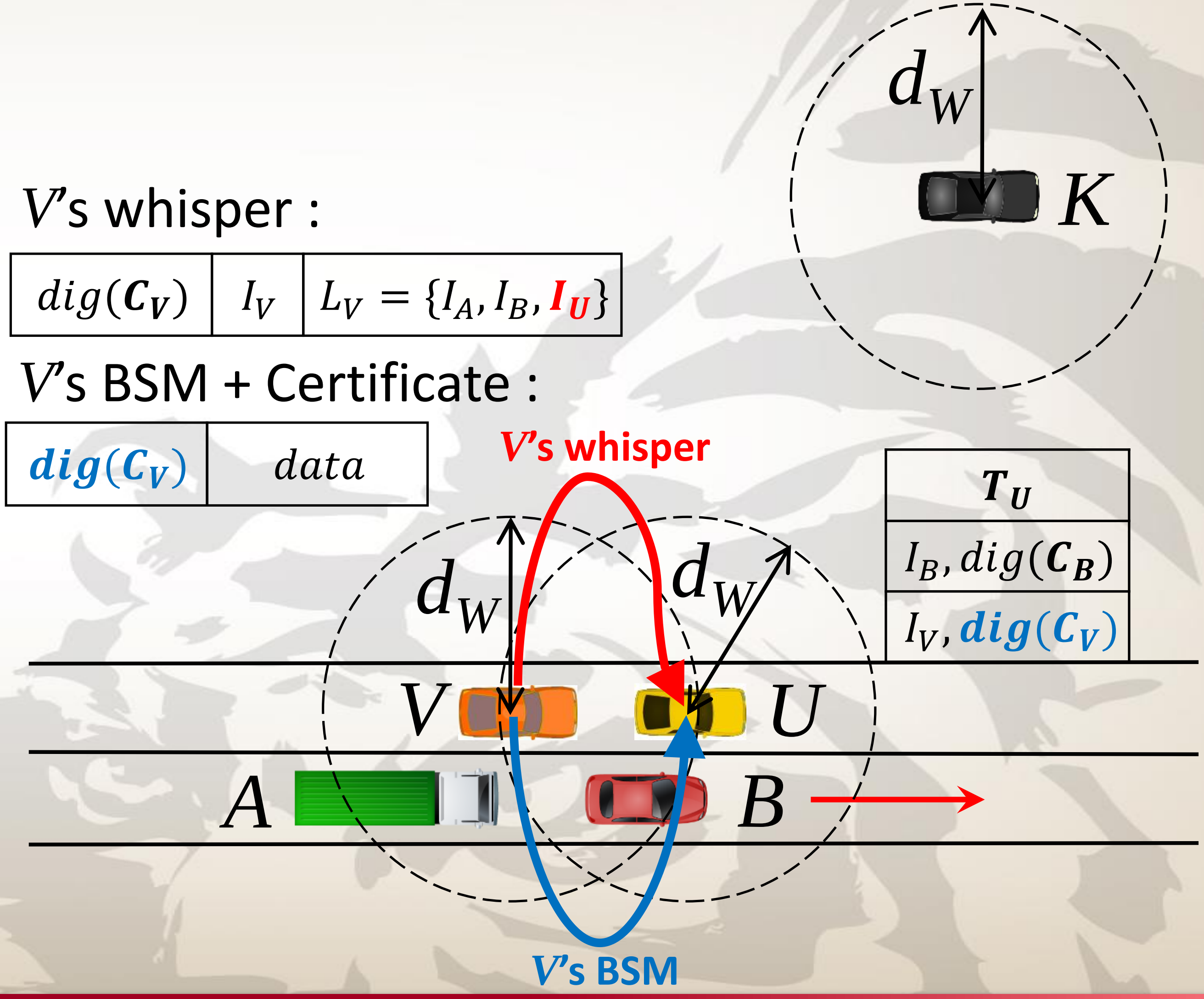




Neighbor check through low-power beaconing (Whisper check)

- Vehicle V's Whisper
  - $dig(C_V)$: digest of V's certificate
  - I_V: Whisper identifier (WID) of V
  - L_V: list of WIDs heard by V
- Vehicle V's BSM + Certificate
  - $dig(C_V)$: digest of V's certificate
  - Part 1 data (Compulsory)
  - Part 2 data (Optional)

- V, U, A, B: general vehicles
- K: an attacker sending the fake BSM
- d_W: the maximum low-power beaconing distance
- T_U: list of trust vehicles' WID and digest in vehicle U



V's whisper :

$dig(\boldsymbol{C_V})$	I_V	$L_V = \{I_A, I_B, \boldsymbol{I_U}\}$

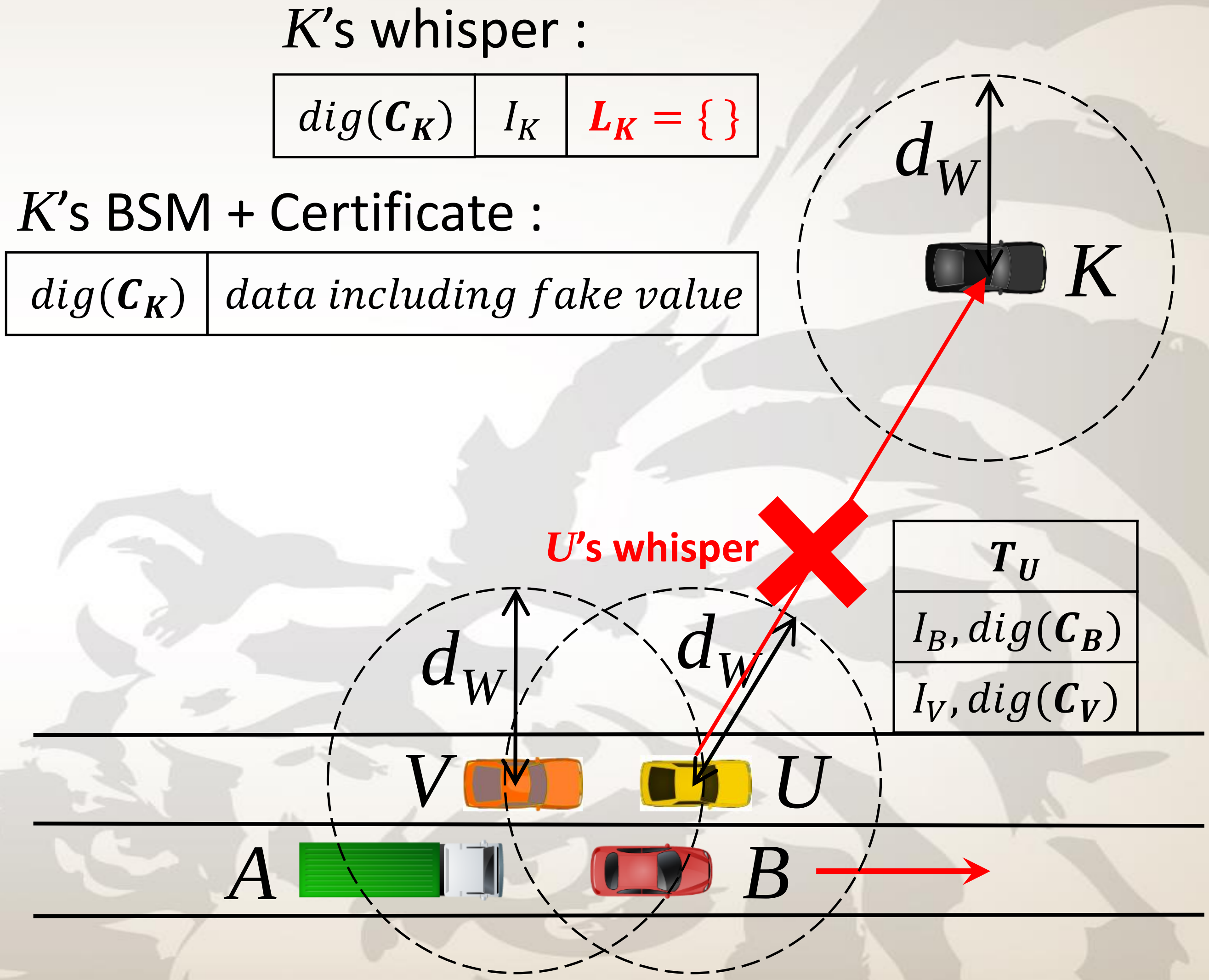
V's BSM + Certificate :

$\boldsymbol{dig(C_V)}$	$data$

$\boldsymbol{T_U}$
$I_B, dig(\boldsymbol{C_B})$
$I_V, \boldsymbol{dig(C_V)}$

Neighbor check through low-power beaconing (Whisper check)

- Vehicle V's Whisper
  - $dig(C_V)$: digest of V's certificate
  - I_V: Whisper identifier (WID) of V
  - L_V: list of WIDs heard by V
- Vehicle V's BSM + Certificate
  - $dig(C_V)$: digest of V's certificate
  - Part 1 data (Compulsory)
  - Part 2 data (Optional)



K's whisper :

$dig(\boldsymbol{C_K})$	I_K	$\boldsymbol{L_K} = \{\ \}$

K's BSM + Certificate :

$dig(\boldsymbol{C_K})$	$data\ including\ fake\ value$

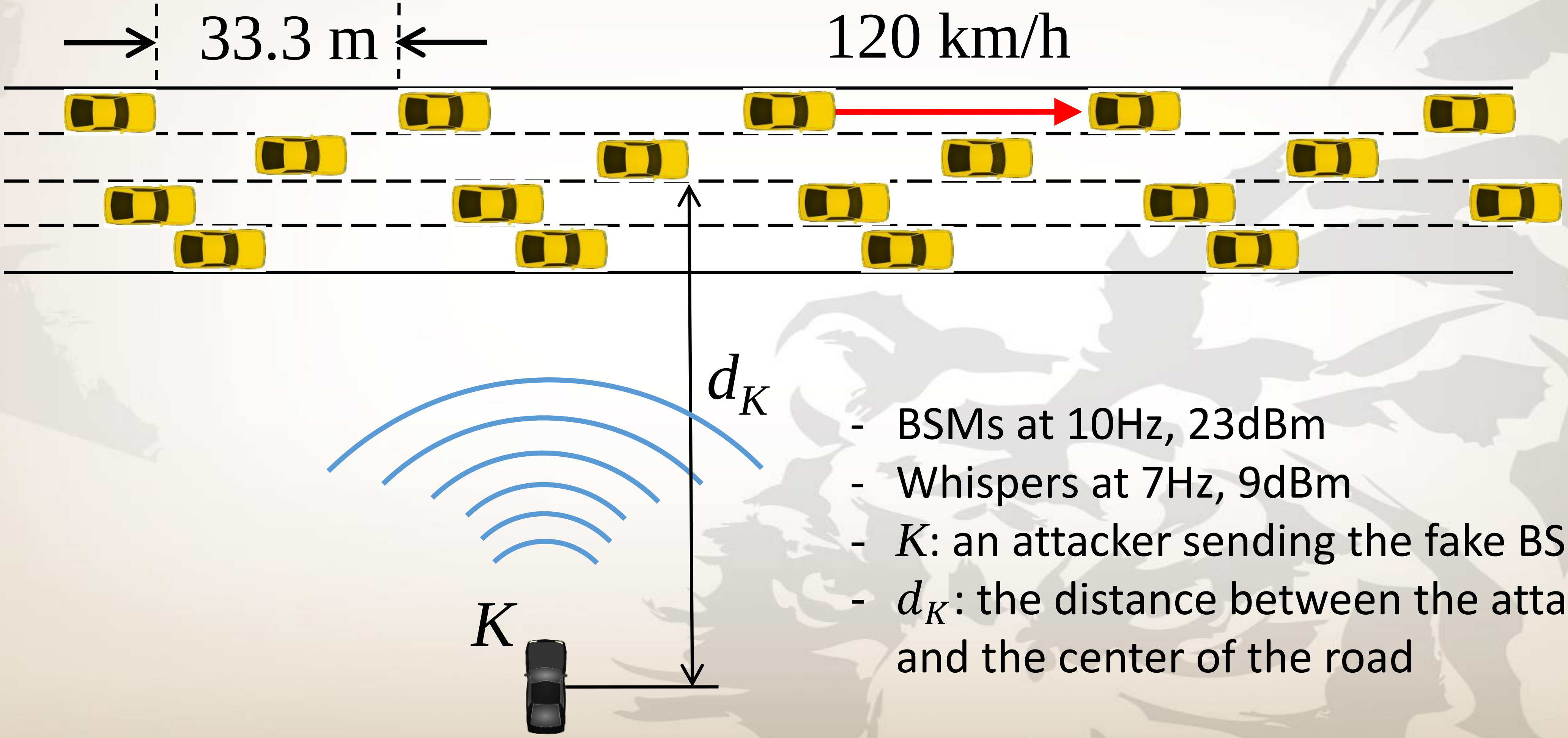
U's whisper

$\boldsymbol{T_U}$
$I_B, dig(\boldsymbol{C_B})$
$I_V, dig(\boldsymbol{C_V})$

- V, U, A, B: general vehicles
- K: an attacker sending the fake BSM
- d_W: the maximum low-power beaconing distance
- T_U: list of trust vehicles' WID and digest in vehicle U

Simulation scenario

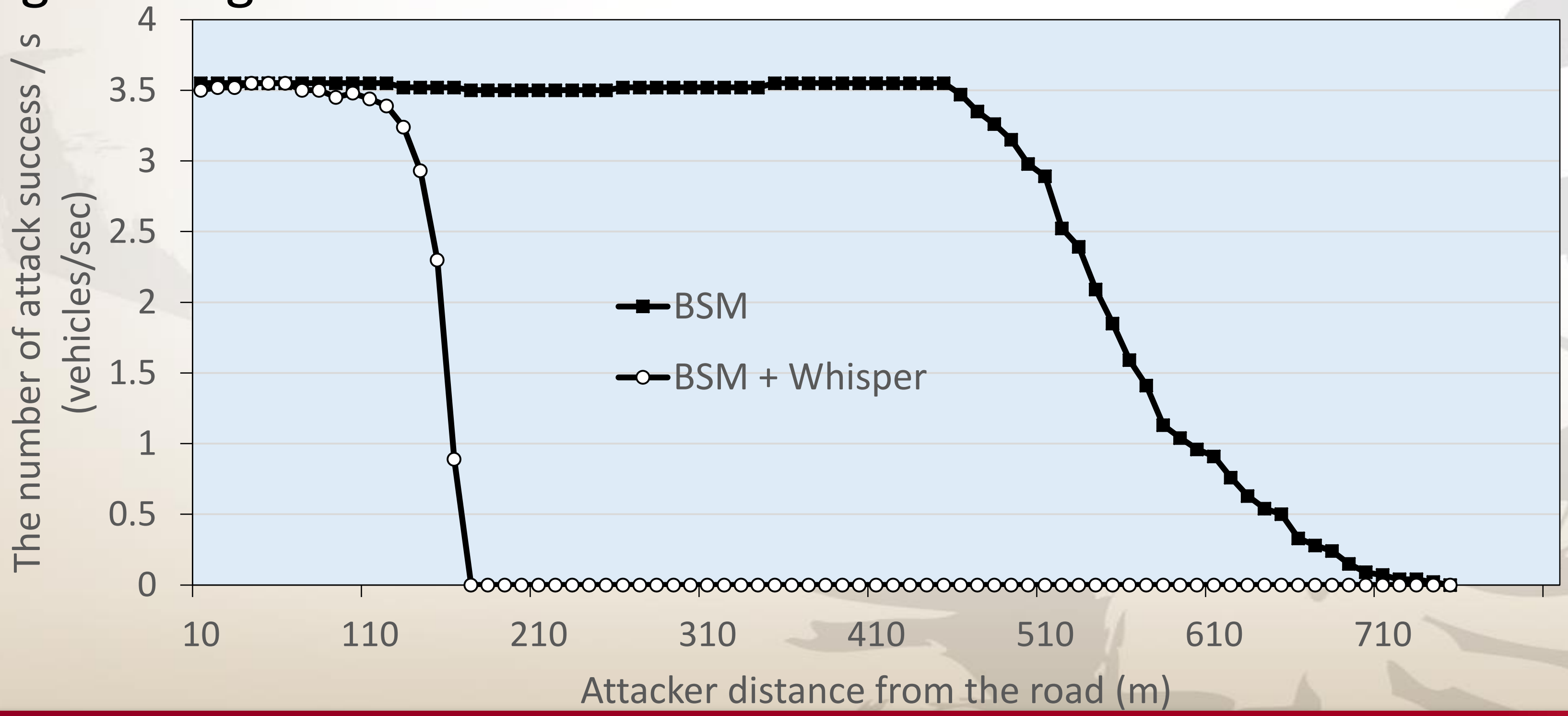
- An attacker K controls d_K and broadcasts its forged messages.



- BSMs at 10Hz, 23dBm
- Whispers at 7Hz, 9dBm
- K: an attacker sending the fake BSM
- d_K: the distance between the attacker K and the center of the road

Whisper check simulation result: “Attack success”

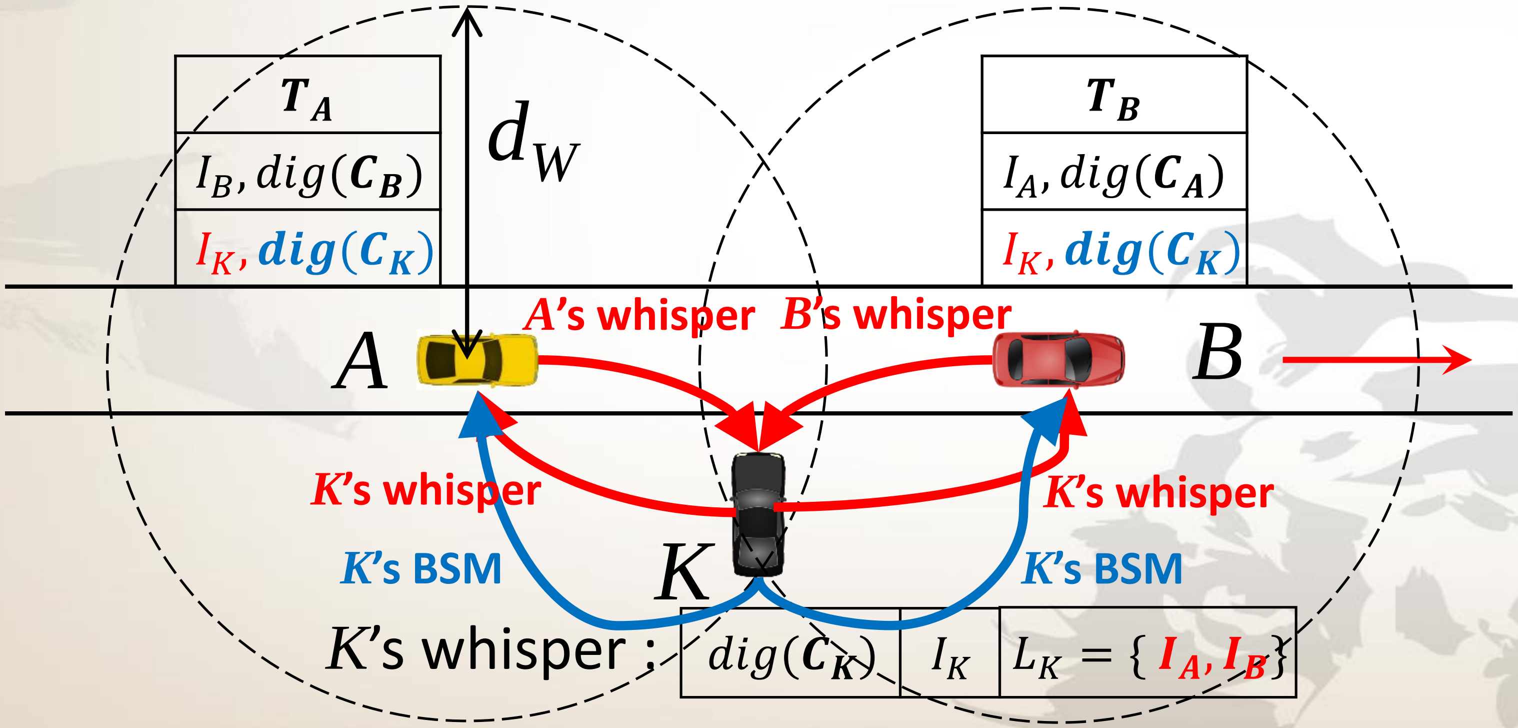
- “Attack success”: The case that the attacker delivers its fake message to a certain vehicle **at first** with passing “Whisper check”
- BSM + Whisper increases the Channel Busy Percentage (CBP) in some measure ($\approx 20\%$)
- The number of attack success per sec: The number of entering vehicles at first in the attack range during one second



- BSMs at 10Hz, 23dBm
- Whispers at 7Hz, 9dBm
- Vehicle speed: 120km/h
- Vehicle-to-Vehicle spacing: 33.3m

How can we cope with much closer attackers from the road?

- Attacker K receives Whisper messages from vehicles A and B
- K broadcasts its forged BSM with passing “Whisper check” of A and B



K’s whisper : $dig(C_K)$ | I_K | $L_K = \{ I_A, I_B \}$

K’s BSM + Certificate : $dig(C_K)$ | $data\ including\ fake\ value$

- $dig(C_V)$: digest of V’s certificate
- I_V: Whisper identifier (WID) of V
- L_V: list of WIDs heard by V
- T_V: list of trust vehicles’ WID and digest in V

- d_W: the maximum low-power beaconing distance
- A, B: general vehicles
- K: an attacker sending the fake BSM

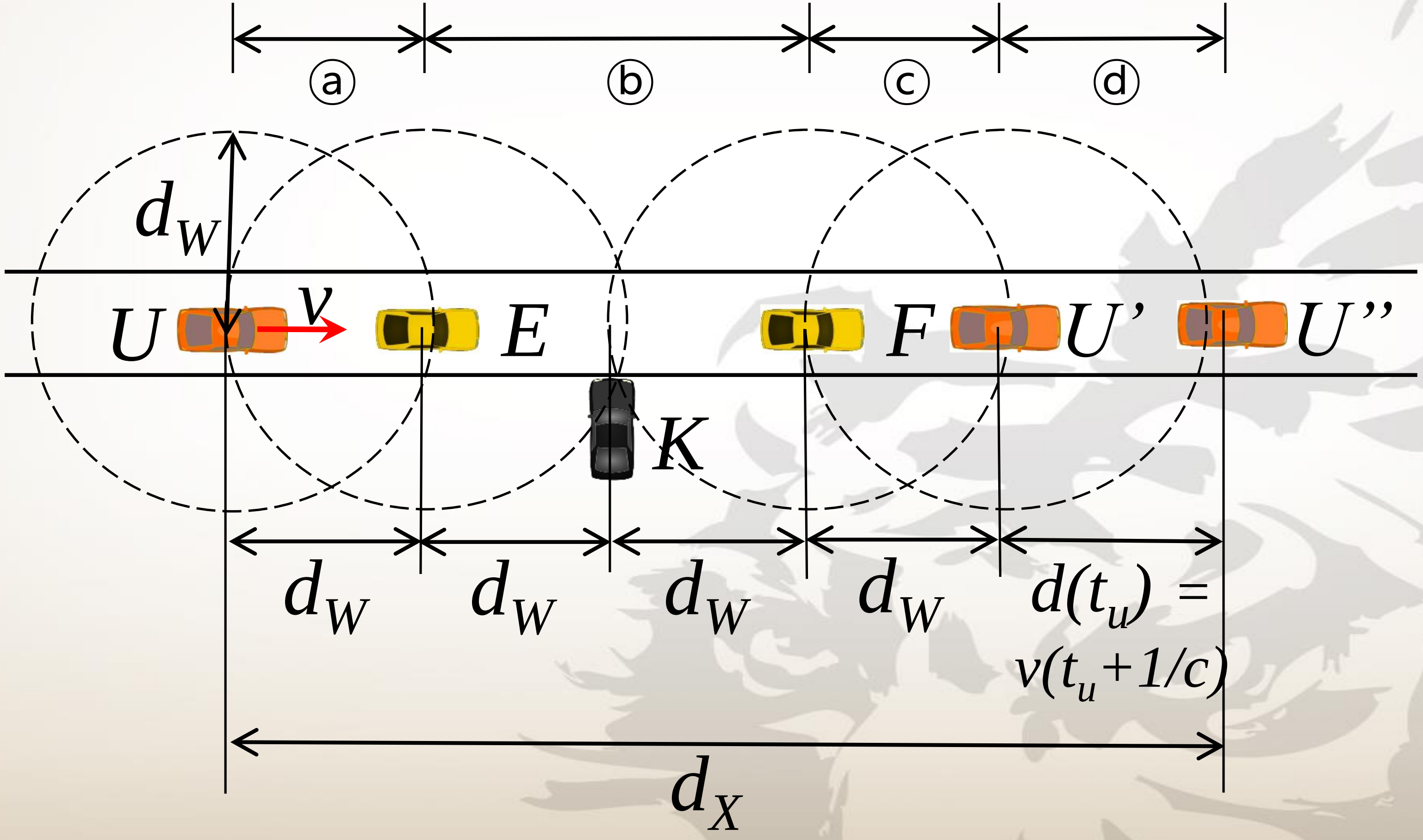
Expanded solution: Whispering with credit

- Expanded solution: **Using the maximum number of sending Whispers from a closer attacker to a certain vehicle** while the vehicle moves the distance that the closer attacker can attack

- First, calculating the attack range of a closer attacker
- Second, introduction the concept “Trust credit” and application it

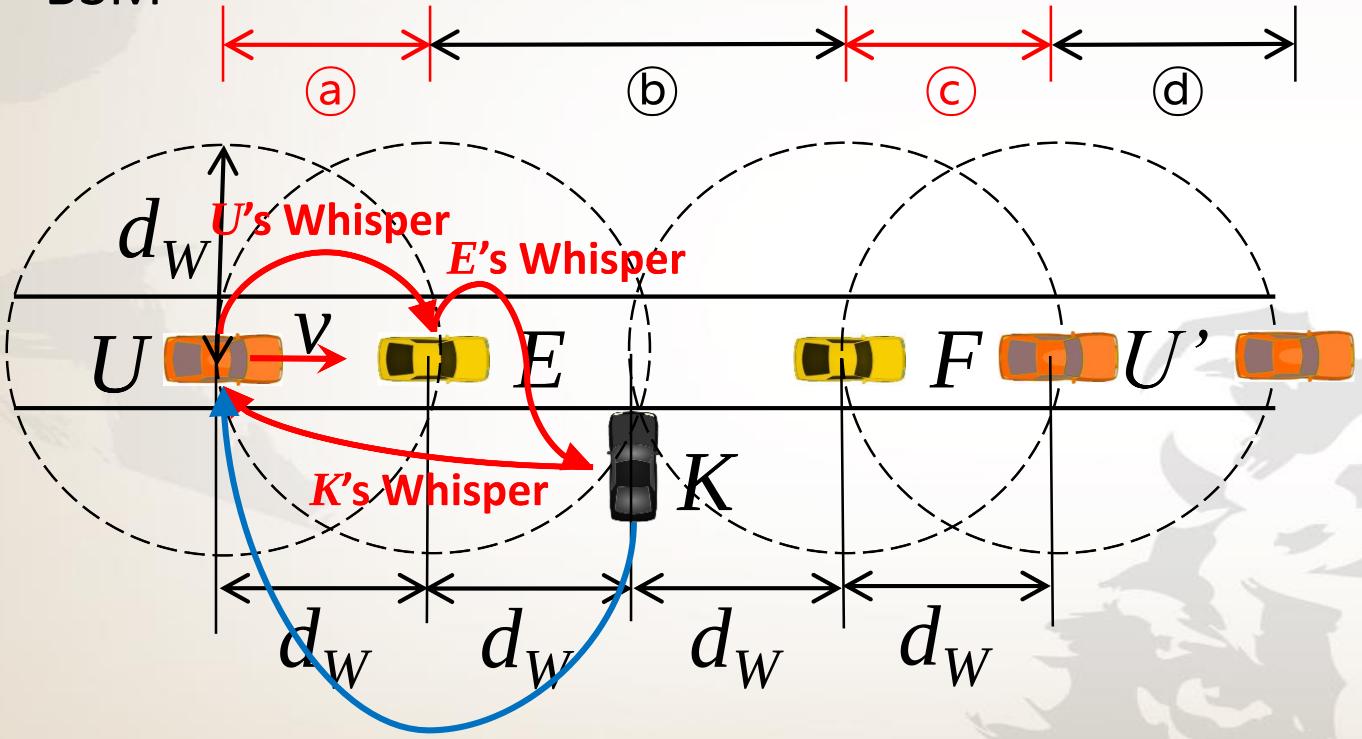
Expanded solution: 1. The attack range of a closer attacker

- Four sections for the attack range of a closer attacker



Expanded solution: 1. The attack range of a closer attacker

- Section ⓐ and ⓒ
  : *U*'s Whisper → *E*'s Whisper → *K*'s Whisper → *K*'s BSM



K's BSM + Certificate :

$\boldsymbol{dig(C_K)}$	$false\ data$

E's Whisper :

$dig(\boldsymbol{C_E})$	I_E	$L_E = \{\boldsymbol{I_U}\}$

K's Whisper :

$dig(\boldsymbol{C_K})$	I_K	$L_K = \{\boldsymbol{I_E}, \boldsymbol{I_U}\}$

$\boldsymbol{T_U}$
$I_E, dig(\boldsymbol{C_E})$
$I_K, \boldsymbol{dig(C_K)}$

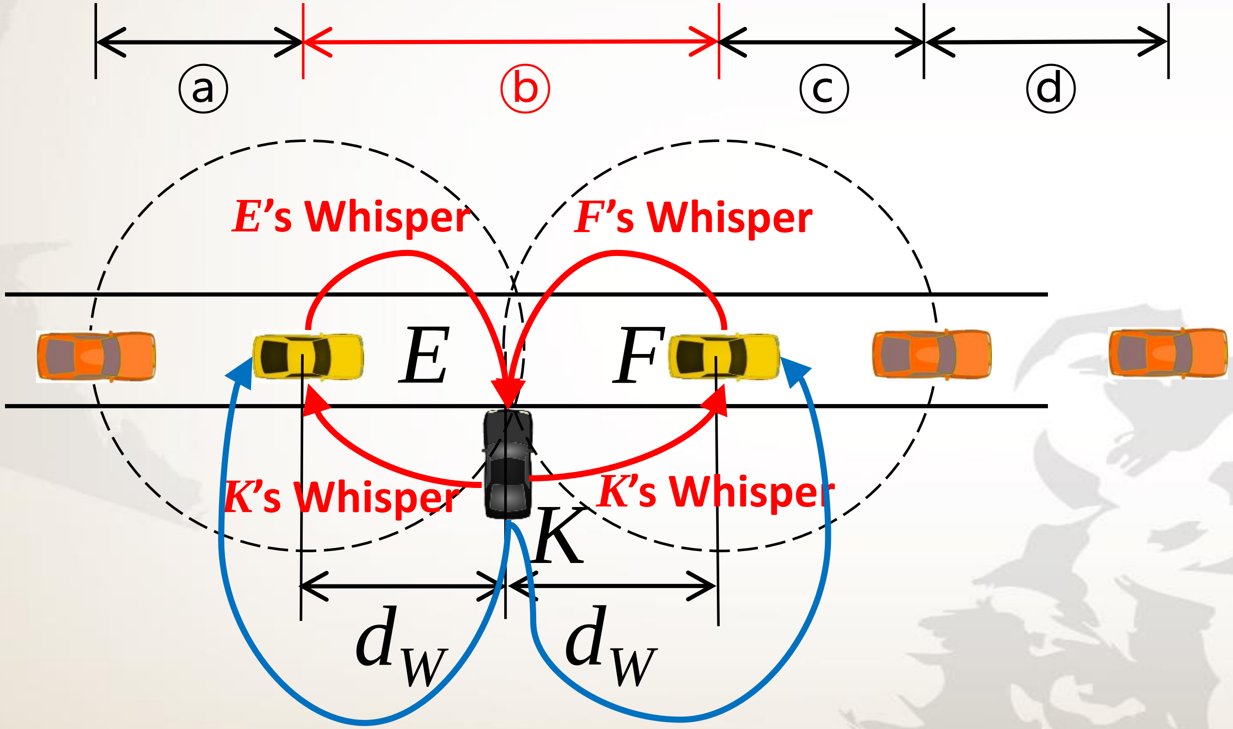
- $dig(C_V)$: digest of *V*'s certificate
- I_V: Whisper identifier (WID) of V
- L_V: list of WIDs heard by V
- T_V: list of trust vehicles' WID and digest in V

- d_W: the maximum low-power beaconing distance
- *U, E, F, U'*: general vehicles
- *K*: an attacker sending the fake BSM

Expanded solution: 1. The attack range of a closer attacker

- Section ⓑ

: Whispers of E and F → K's Whisper → K's BSM



K's BSM + Certificate :

$\boldsymbol{dig(C_K)}$	$false\ data$

K's Whisper :

$dig(C_K)$	I_K	$L_K = \{\boldsymbol{I_E}, \boldsymbol{I_F}\}$

$\boldsymbol{T_E}$
$I_K, \boldsymbol{dig(C_K)}$

$\boldsymbol{T_F}$
$I_K, \boldsymbol{dig(C_K)}$

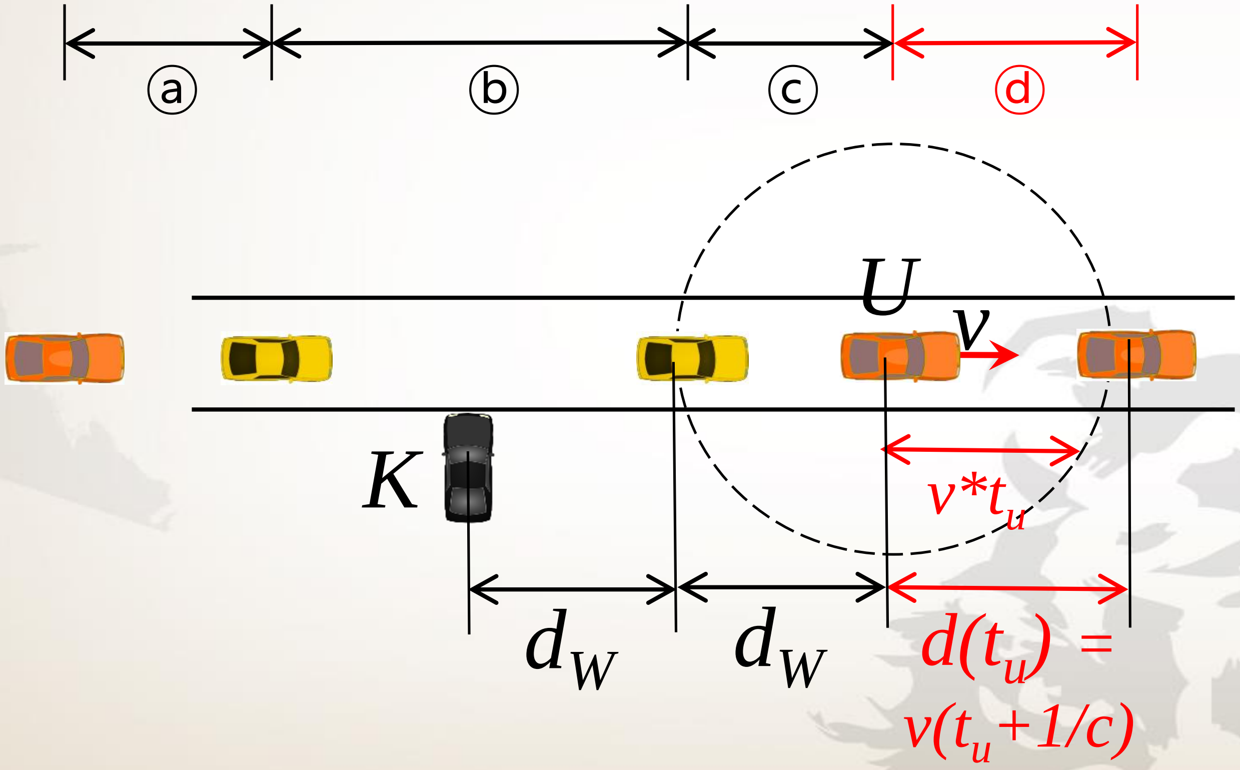
- $dig(C_V)$: digest of V's certificate
- I_V: Whisper identifier (WID) of V
- L_V: list of WIDs heard by V
- T_V: list of trust vehicles' WID and digest in V

- d_W: the maximum low-power beaconing distance
- E, F: general vehicles
- K: an attacker sending the fake BSM

Expanded solution: 1. The attack range of a closer attacker

- Section ⓓ

  : Whisper update period + the worst whispering rate



K's Whisper :

$dig(\boldsymbol{C_K})$	I_K	$L_K = \{\boldsymbol{I_U}\}$

U's Whisper : $\boldsymbol{I_U}$

$dig(\boldsymbol{C_U})$	$\boldsymbol{I'_U}$	$L_K = \{\boldsymbol{I_K}\}$

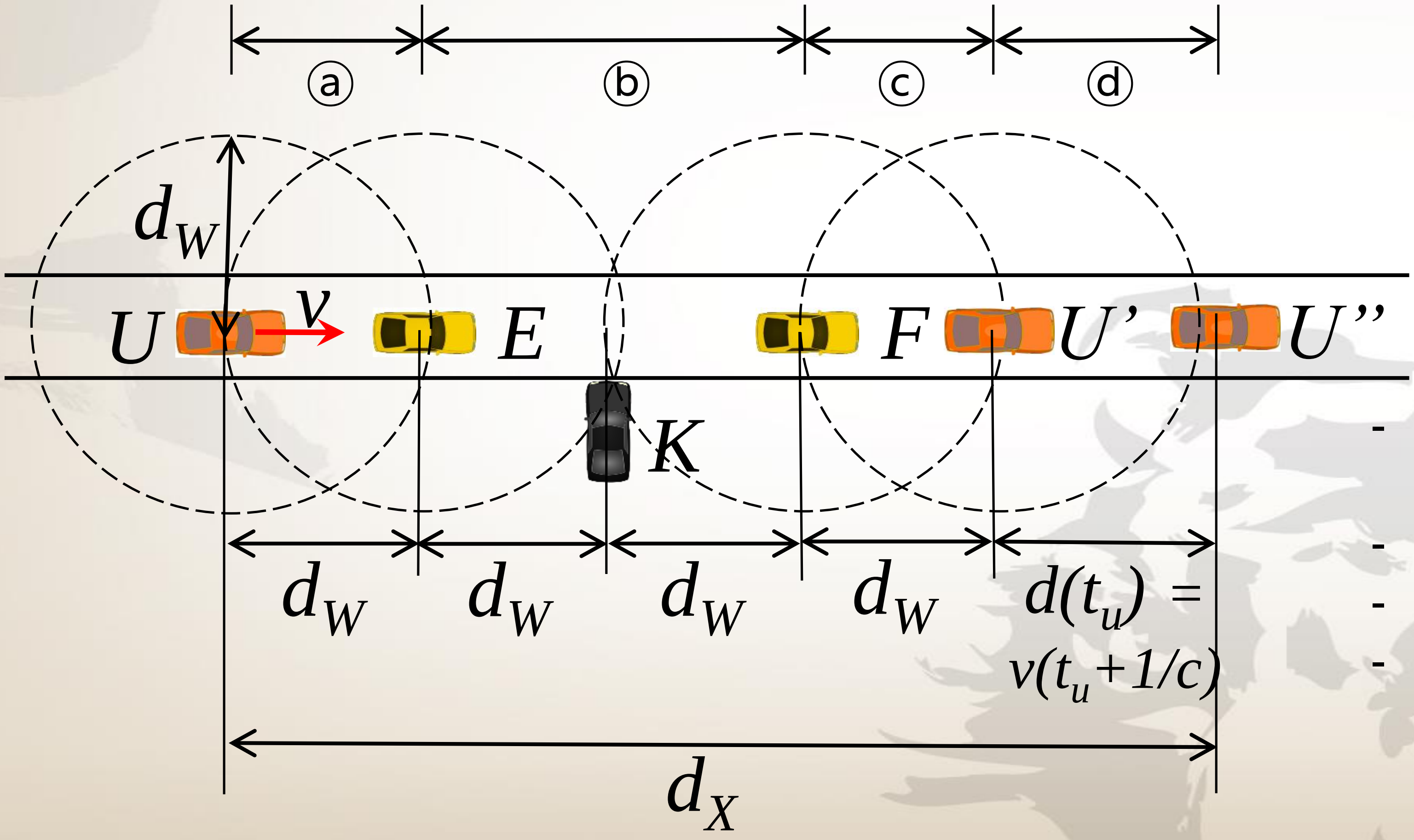
$\boldsymbol{T_U}$
$I_K, \boldsymbol{dig}(\boldsymbol{C_K})$

- $dig(C_V)$: digest of V's certificate
- I_V: Whisper identifier (WID) of V
- L_V: list of WIDs heard by V
- T_V: list of trust vehicles' WID and digest in V

- d_W: the maximum low-power beaconing distance
- t_u: the Whisper ID update period
- c : the Whispering rate in the worst case
- v: the velocity of vehicle U

Expanded solution: 1. The attack range of a closer attacker

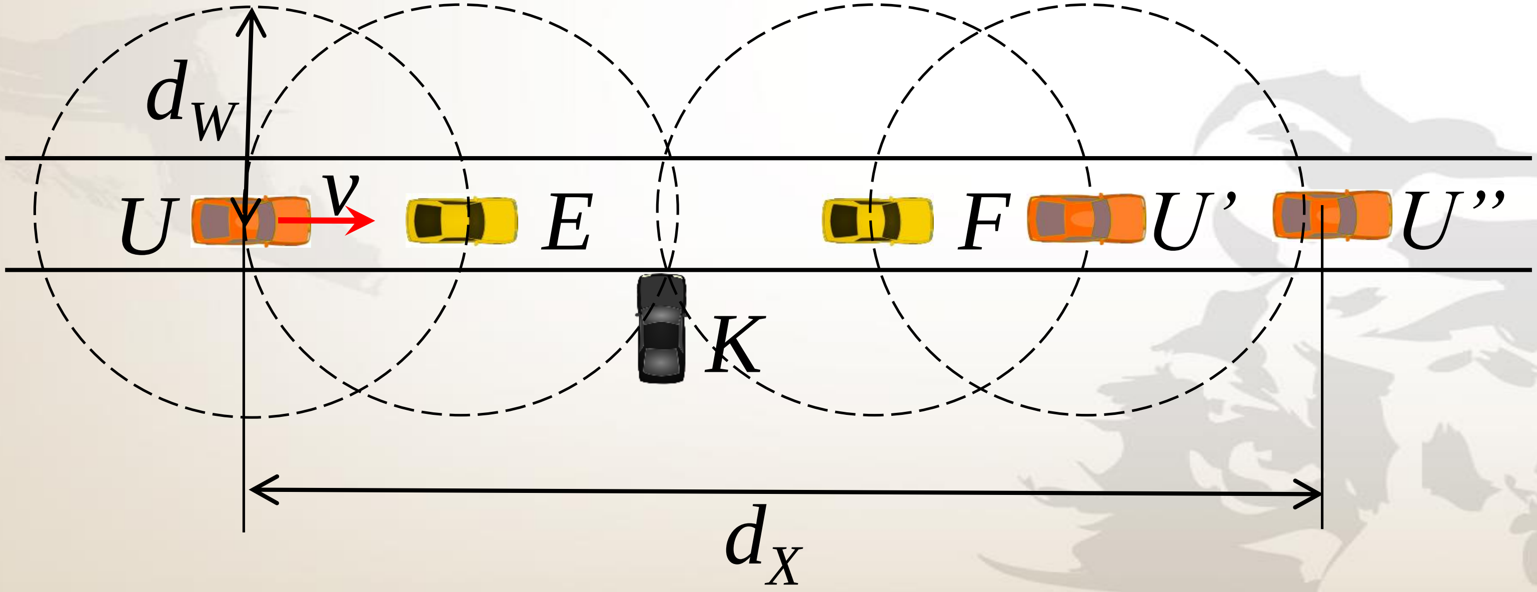
- Calculating the attack range of a closer attacker $d_X = 4 \cdot d_W + v \cdot \left(t_u + \frac{1}{c}\right)$



- d_W: the maximum Whisper beaconing distance
- t_u: the Whisper ID update period
- c : the Whispering rate in the worst case
- v: the velocity of vehicle U

Expanded solution: 2. “Trust credit” and applying it

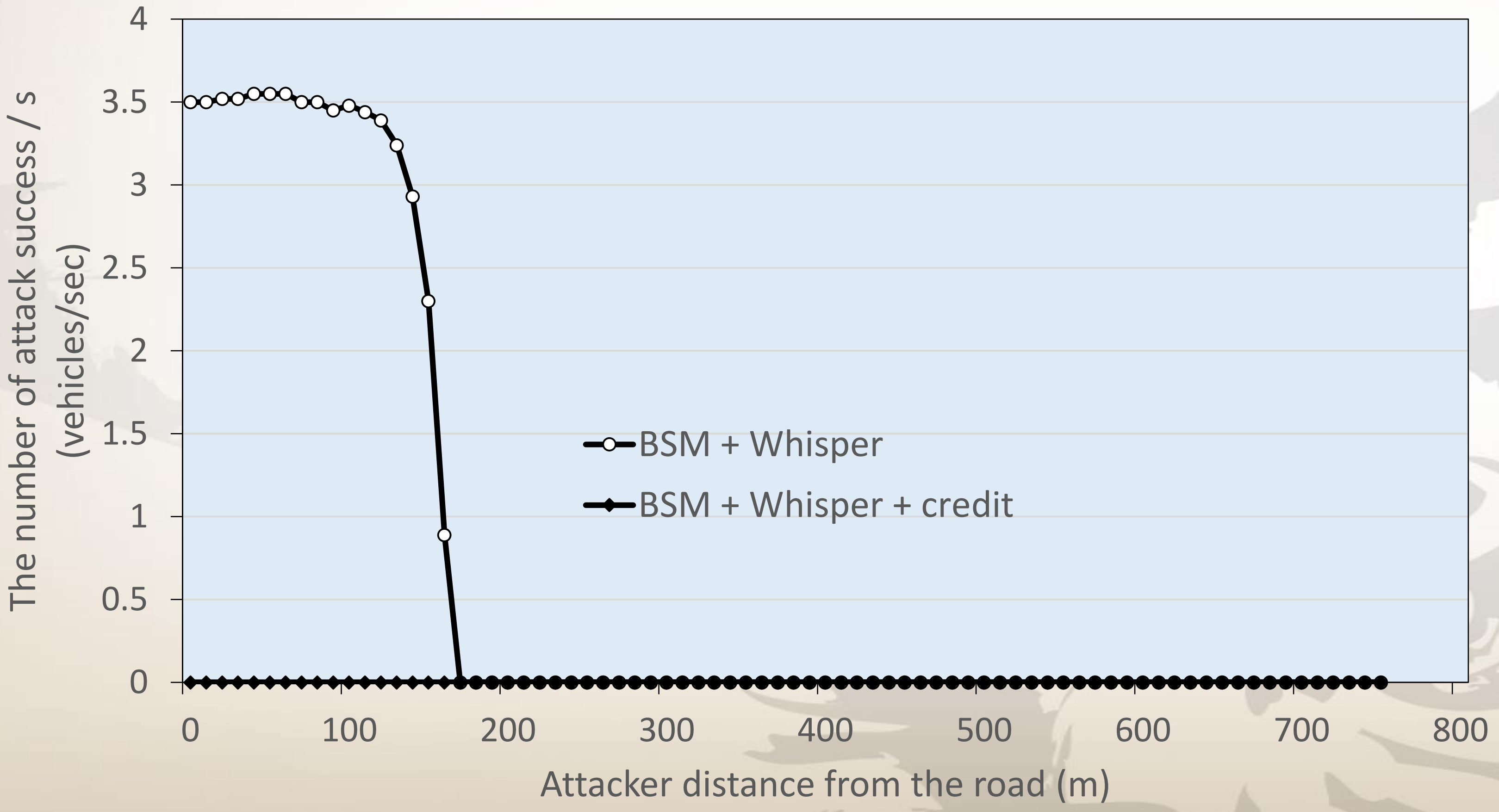
- Trust credit threshold θ_V is essentially the credit that a roadside attacker can maximally accumulate at U while vehicle U travels d_X
- $\theta_V = (f_W - 1) \cdot d_X / v$
- If a vehicle gets “Trust credits” more than the trust credit threshold



- f_W: the whispering frequency
- d_X: the attack range of a closer attacker

Whisper check with credit simulation result

- The credit-based check can solve the limit of BSM + Whisper
- To cope with a closer attacker from the road



- BSMs at 10Hz, 23dBm
- Whispers at 7Hz, 9dBm
- Vehicle speed: 120km/h
- Vehicle-to-Vehicle spacing: 33.3m

Significance and Discussion

[Significance of our work]

- Vehicles can mutually check if the BSM hence the position information therein indeed comes from a physically close neighbor
- Screening false messages of remote stationary attackers
- Expanded solution for an attack of a closer attacker from the road

[Discussion points]

- Legitimate vehicles that have not accumulated enough credit
- Mobile attackers
- Efficient whisper congestion control usage with BSM

Thank you!

Any questions?

Taeho Kim

Department of Computer Science and Engineering
Korea University

taehokim@korea.ac.kr

Digest of a certificate

- The BSM with a certificate is transmitted approximately every 500 ms, and other BSMs are transmitted with a certificate digest to reduce the overall message length.
  → BSM + a certificate digest: 80%, BSM + a certificate: 20%
- A certificate digest(hash of the current security certificate): 8 bytes
- A certificate: 125 bytes

Message latency ranges

Priority		Examples
7	Highest	**BSM** + Hard-Brake
6	↑	Electronic Toll Collection
5		**BSM**
4		Lane Coordination
3		WSA (WAVE Serice Announcement)
0		
2	↓	On-Board Navigation
1	Lowest	Commercial applications

Importance	Urgency		
	< 10 msec	From 10 th 20 msec	> 20 msec
Safety of Life	**7**	**5**	3
Public Safety	5	4	1
Non-Priority	2	1	1

IEEE 1609.2

- This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

SAE J2735

- This SAE Standard specifies a message set, and its data frames and data elements specifically for use by applications intended to utilize the 5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, referenced in this document simply as “DSRC”), communications systems.

SAE J2945/1

- This standard specifies the system requirements for an on-board vehicle-to-vehicle (V2V) safety communications system for light vehicles , including standards profiles, functional requirements, and performance requirements.
- The system is capable of transmitting and receiving the Society of Automotive Engineers (SAE) J2735-defined Basic Safety Message (BSM) over a Dedicated Short Range Communications (DSRC) wireless communications link as defined in the Institute of Electrical and Electronics Engineers (IEEE) 1609 suite and IEEE 802.11 standards.