CaTch: A Confidence Range Tolerant Misbehavior Detection Approach

2019 IEEE Wireless Communications and Networking Conference (WCNC)

Presented by Marshall Thompson

Misbehavior Detection and CaTch Purpose

- Misbehavior detection is a two step process
  - A suite of misbehavior checks are run on message data
  - The misbehavior checks pass their determination to a global misbehavior detector, which will make the final classification
- Prior versions of misbehavior checks only use the received numbers for speed, position and do not include the error levels sent in both CAM and BSM message formats
- CaTch aims to use the error values sent in CAM and BSM messages to generate more useful real number determinations for machine learning global detectors to take advantage of

Types of Misbehavior Checks

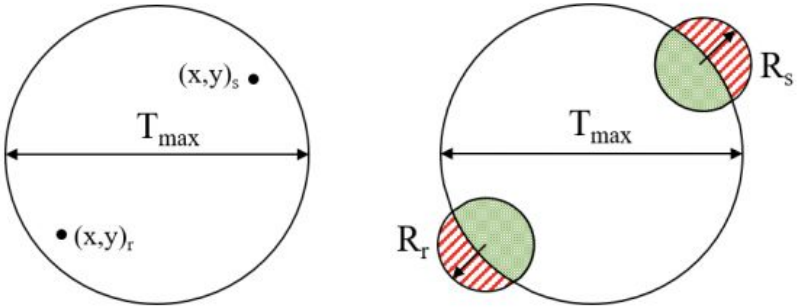
1. Consistency Checks
    a. Requires two successive messages from the same source
2. Plausibility Checks
    a. Requires only one received message

CaTch Plausibility Checks

CaTch Range Plausibility

TABLE I: Common Notations

R_x	$\triangleq$	Position confidence range in beacon x
V_x	$\triangleq$	Claimed speed in beacon x
C_x	$\triangleq$	Speed confidence range in beacon x
D_x	$\triangleq$	Claimed heading in beacon x
Δt_{ij}	$\triangleq$	Time separating beacons i and j
d_{ij}	$\triangleq$	Distance separating beacons i and j
A_x	$=$	πR_x^2



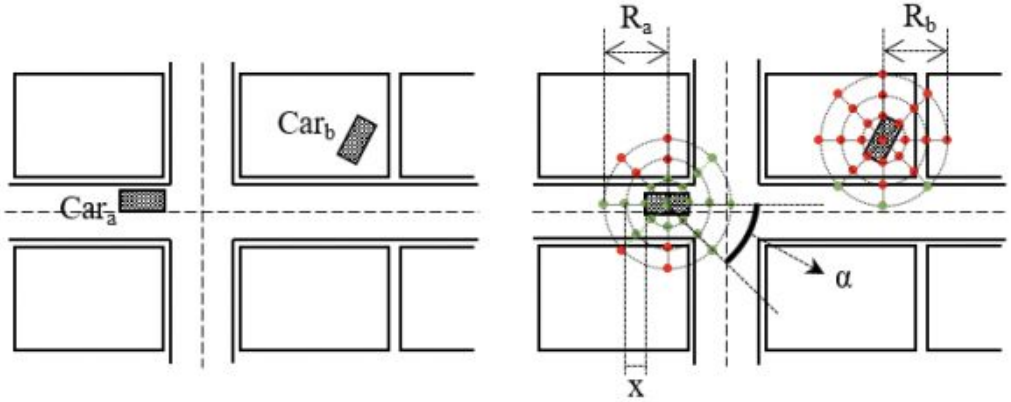
(a) Legacy Version (b) CaTCh Version

Fig. 1: Range Plausibility Check

T_{max}	$\triangleq$	Communication Diameter
$A_{T_{max}}$	$=$	$\frac{\pi T_{max}^2}{4}$
a_r	$=$	$A_{T_{max}} \cap A_r$
a_s	$=$	$A_{T_{max}} \cap A_s$

$$f = (a_r + a_s)/(A_r + A_s) \quad (1)$$

CaTch Position Plausibility

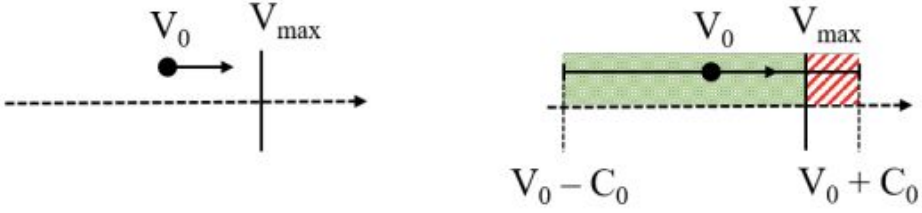


(a) Legacy Version (b) CaTch Version

Fig. 2: Position Plausibility Check

$$f = n/N \tag{2}$$

CaTch Speed Plausibility Check



(a) Legacy Version (b) CaTCh Version

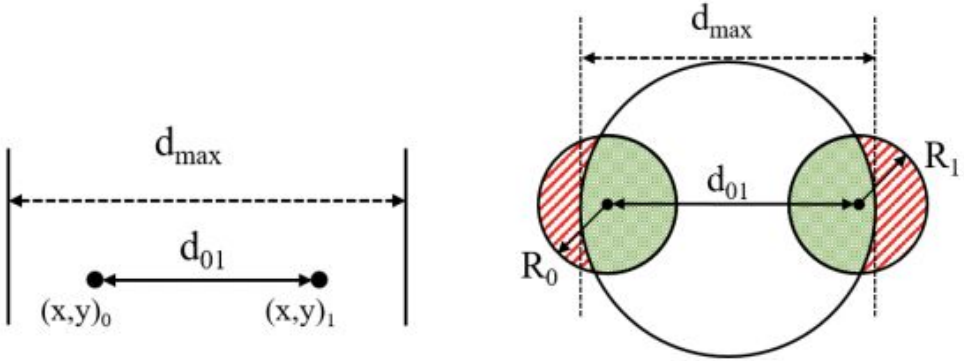
Fig. 3: Speed Plausibility Check

V_{max} $\triangleq$ Max Plausible Speed

$$f = \frac{(V_{max} - V_0 + C_0)}{2C_0} \tag{3}$$

CaTch Consistency Checks

CaTch Position Consistency Check

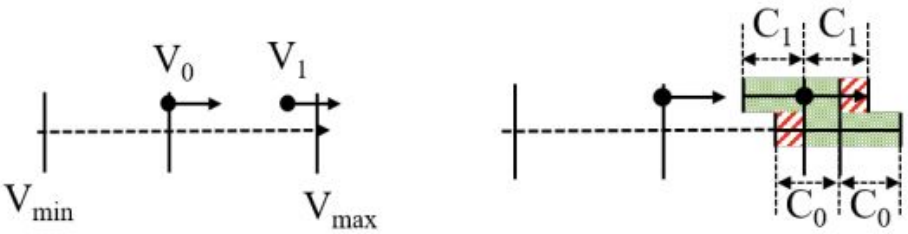


(a) Legacy Version (b) CaTch Version

Fig. 4: Position Consistency Check

$$f = (a_0 + a_1)/(A_0 + A_1) \tag{4}$$

CaTch Speed Consistency Check



(a) Legacy Version (b) CaTch Version

Fig. 5: Speed Consistency Check

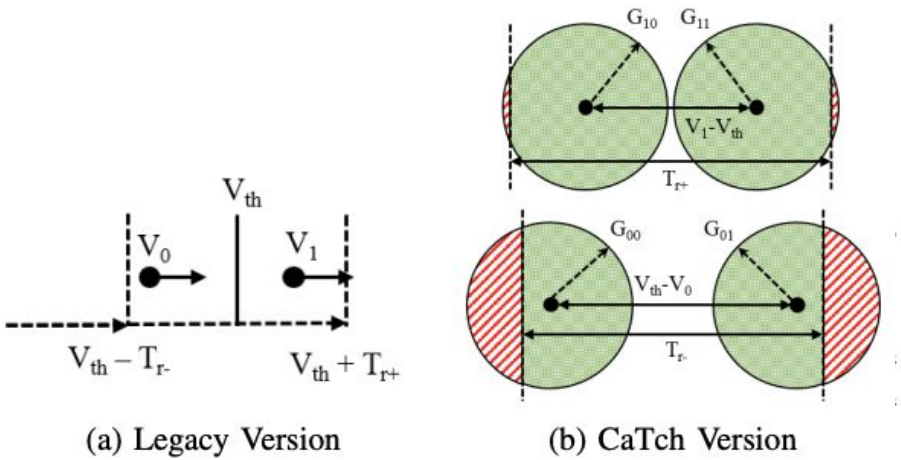
V_{min}	$\triangleq$	Minimum plausible speed when the vehicle decelerates
V_{max}	$\triangleq$	Maximum plausible speed when the vehicle accelerates

$$f_{max} = \frac{V_{max} - V_1 + C_0}{4C_0} + \frac{V_{max} - V_1 + C_1}{4C_1}$$

$$f_{min} = \frac{V_1 - V_{min} + C_0}{4C_0} + \frac{V_1 - V_{min} + C_1}{4C_1}$$

$$f = \left\{ \begin{array}{ll} f_{min}, & \text{when } V_1 \leq V_0 \\ f_{max}, & \text{when } V_1 > V_0 \end{array} \right\} \quad (5)$$

CaTch Position Speed Consistency Check



(a) Legacy Version (b) CaTch Version

Fig. 6: Position Speed Consistency Check

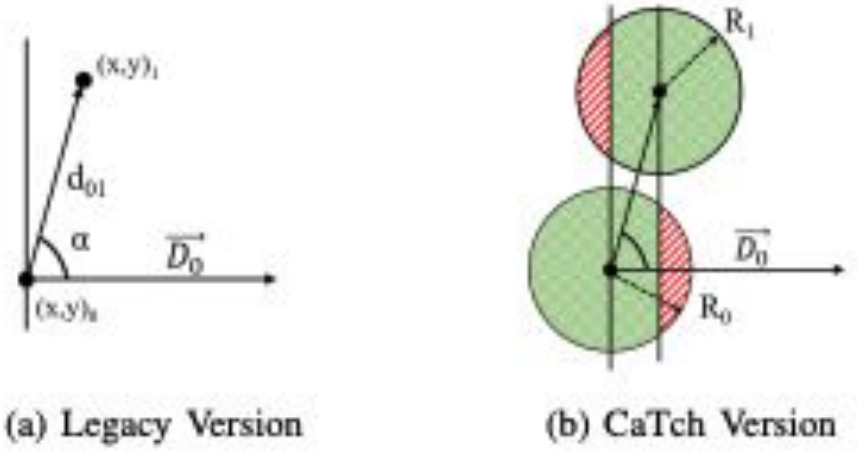
V_{th}	$\triangleq$	Theoretical speed based on separating distance
V_{min}	$\triangleq$	Minimum advertised speed between 1^{st} & 2^{nd} beacon
V_{max}	$\triangleq$	Maximum advertised speed between 1^{st} & 2^{nd} beacon
T_{r+}	$\triangleq$	Tolerance range on excess speed
T_{r-}	$\triangleq$	Tolerance range on dearth speed
Δt	$\triangleq$	Time separating first & second beacon
G_{min0}	$=$	$C_{min} + R_0/\Delta t$
G_{min1}	$=$	$C_{min} + R_1/\Delta t$
G_{max0}	$=$	$C_{max} + R_0/\Delta t$
G_{max1}	$=$	$C_{max} + R_1/\Delta t$
lb_{min}	$=$	$V_{th}/2 - V_{min}/2 - T_{t-}$
lb_{max}	$=$	$-V_{th}/2 + V_{max}/2 - T_{t+}$

$$f_{min} = \frac{2\int_{lb_{min}}^{G_{min0}} \sqrt{G_{min0}^2 - x^2}\,dx + 2\int_{-G_{min1}}^{-lb_{min}} \sqrt{G_{min1}^2 - x^2}\,dx}{A_0 + A_1}$$

$$f_{max} = \frac{2\int_{lb_{max}}^{G_{max1}} \sqrt{G_{max1}^2 - x^2}\,dx + 2\int_{-G_{max0}}^{-lb_{max}} \sqrt{G_{max0}^2 - x^2}\,dx}{A_0 + A_1}$$

$$f = \left\{ \begin{array}{ll} f_{min}, & \text{when } f_{min} > f_{max} \\ f_{max}, & \text{when } f_{min} \leq f_{max} \end{array} \right\} \tag{6}$$

CaTch Position Heading Consistency Check



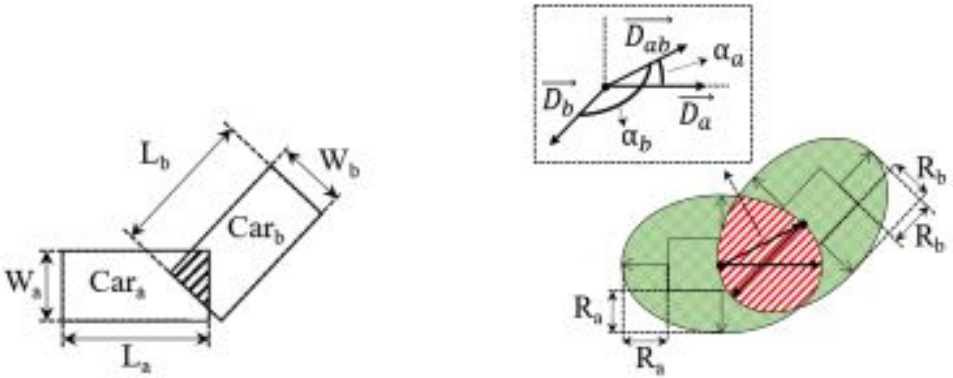
(a) Legacy Version (b) CaTch Version

Fig. 7: Position Heading Consistency Check

$\vec{D_{01}}$	$\triangleq$	Vector formed by the centers of the 1^{st} & 2^{nd} beacons
α	$\triangleq$	Angle between $\vec{D_0}$ & $\vec{D_{01}}$

$$f = \frac{2\int_{d_{01}\cos\alpha}^{R_0}\sqrt{R_0^2 - x^2}dx + 2\int_{-R_1}^{-d_{01}\cos\alpha}\sqrt{R_1^2 - x^2}dx}{A_0 + A_1} \tag{7}$$

CaTch Intersection Check



(a) Legacy Version (b) CaTch Version

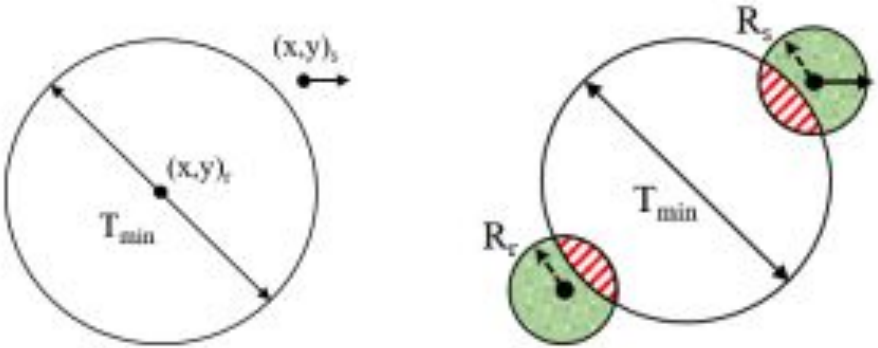
Fig. 8: Intersection Check

$$f_a = Ae_{ab}/(Ae_a + Ae_b - Ae_{ab})$$

$$f_i = ol_{ab}/(I_a + I_b - ol_{ab})$$

$$f = f_a f_i \tag{8}$$

CaTch Sudden Appearance Check



(a) Legacy Version (b) CaTch Version

Fig. 9: Sudden Appearance Check

T_{min}	$\triangleq$	Minimum acceptable range for sudden appearance
$A_{T_{min}}$	$=$	$\frac{\pi T_{min}^2}{4}$
a_r	$=$	$A_{T_{min}} \cap R_r$
a_s	$=$	$A_{T_{min}} \cap R_s$

$$f = (R_r + R_s - a_r - a_s)/(R_r + R_s) \quad (9)$$

Misbehavior Apps

Detection Applications

1. Simple App
    a. Anything above 0.5 uncertainty for any detector is reported
    b. This means that CaTch and legacy detectors should perform similarly
2. Advanced App
    a. Used machine learning
    b. Using data from simulations, a neural network was trained
    c. A model was trained for CaTch and Legacy detectors

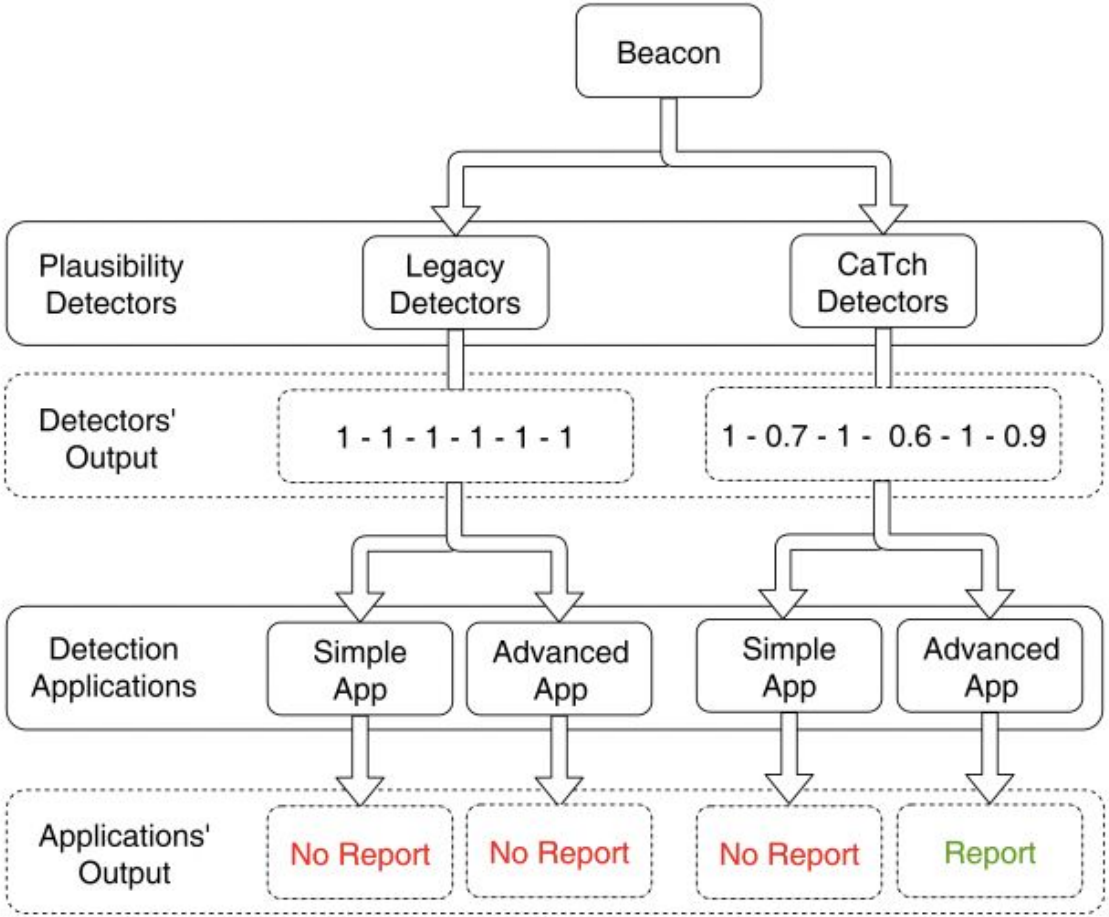


Fig. 10: Example illustrating an advantage of using CaTch

Evaluation

Experimental Setup

- Legacy and CaTch checks were implemented as a VEINS extension.
- Considered Attacks
  - Constant offset attacks
  - Sybil Attacks
- Measurement uncertainty not included in VEINS out of the box
- Evaluation metrics:
  - Recall
  - Precision
  - Accuracy
  - F1 Score
  - Bookmaker Informedness
  - Matthews Correlation Coefficient

Results

TABLE III: Simulation Results

App	Scenario / Detectors	Evaluation Metrics		
Threshold		**Recall**	**Precision**	**Accuracy**
	Legacy	0.7621	0.9233	0.9691
	CaTch	0.7625	0.9207	0.9689
		Δ0.1%	Δ-0.3%	Δ0.0%
		F_1Score	**BM**	**MCC**
	Legacy	0.8350	0.7548	0.8227
	CaTch	0.8342	0.7550	0.8216
		Δ-0.1%	Δ0.0%	Δ-0.1%
Machine Learning		**Recall**	**Precision**	**Accuracy**
	Legacy	0.7642	0.9375	0.9706
	CaTch	0.7498	0.9721	0.9721
		Δ-1.9%	Δ3.7%	Δ0.2%
		F_1Score	**BM**	**MCC**
	Legacy	0.8420	0.7584	0.8312
	CaTch	0.8466	0.7473	0.8400
		Δ0.5%	Δ-1.5%	Δ1.1%

(a) Constant Offset Scenario

App	Scenario / Detectors	Evaluation Metrics		
Threshold		**Recall**	**Precision**	**Accuracy**
	Legacy	0.3976	0.9504	0.7468
	CaTch	0.4203	0.9457	0.7546
		Δ5.7%	Δ-0.5%	Δ1.1%
		F_1Score	**BM**	**MCC**
	Legacy	0.5607	0.3834	0.5013
	CaTch	0.5819	0.4038	0.5155
		Δ3.8%	Δ5.3%	Δ2.8%
Machine Learning		**Recall**	**Precision**	**Accuracy**
	Legacy	0.3928	0.9498	0.7446
	CaTch	0.7961	0.9102	0.8852
		Δ102.7%	Δ-4.2%	Δ19.8%
		F_1Score	**BM**	**MCC**
	Legacy	0.5556	0.3783	0.4967
	CaTch	0.8494	0.7424	0.7618
		Δ52.9%	Δ96.2%	Δ53.4%

(b) Sybil Attack Scenario

Questions?

Discussion Questions

1. The authors only used two types of attacks to evaluate the CaTch detector. Can you think of an attack that may fool the CaTch + either type of evaluation app?
2. Any other interesting or unique ideas for a misbehavior detector? I saw a few really good results on MP III!