Missbrauchserkennung in kooperativen intelligenten Verkehrssystemen[1]

Rens W. van der Heijden[2]

Abstract: Für die Verbesserung der Verkehrssicherheit und Verkehrseffizienz wird an kooperativen intelligenten Verkehrssystemen (Cooperative Intelligent Transport Systems, C-ITS) gearbeitet. Diese infastrukturlosen Kommunikationsnetzwerke erlauben den Informationsaustausch zwischen Fahrzeugen, welches allerdings auch ein großes Spektrum neuer Angriffe ermöglicht. Besonders wichtig ist hier die Überprüfung der Integrität und Korrektheit der Datenflüsse, da fehlerhafte Informationen zu Unfällen führen können. Das Maat Fusionsframework, welches im Rahmen dieser Arbeit entstanden ist, nutzt Subjective Logic, um eine modulare und flexible Überprüfung dieser Daten zu ermöglichen. Zur Umsetzung des Maat genannten Frameworks wurden Beiträge zur Fusion mittels Subjective Logic und neue Missbraucherkennungsalgorithmen entwickelt. Außerdem wurden verschiedene Metriken erarbeitet, welche die Anforderungen der C-ITS besser abbilden als bisherige Ansätze, und es wurde der erste öffentlich verfügbare Datensatz zur Auswertung von Missbraucherkennungssystemen erstellt.

1 Einführung

Autounfälle sind eine der Haupttodesursachen in der westlichen Welt, wofür Automobilhersteller und Forschende ein breites Spektrum an Lösungen analysiert haben. Die Kommunikation zwischen Fahrzeuge gilt hierbei als besonders vielversprechend, da sie hochmoderne Fahrerassistenzsysteme ermöglicht, die bisher nur mithilfe von Sensoren mit begrenzter Reichweite arbeiten. Um dem Fahrzeug ein vollständigeres Bild seiner Umgebung zu vermitteln, wurden verschiedene Standards vorgeschlagen, die den Informationsaustausch zwischen den Fahrzeugen ermöglichen. Jüngste Entwicklungen in diesem Bereich, die mehr Komponenten in diese Kommunikationsarchitektur integrieren, führen zu kooperativen intelligenten Verkehrssystemen (C-ITS), welche Entscheidungen auf Grundlage von Sensorinformationen treffen, die aus teilweise nicht-vertrauenswürdigen Quellen empfangen werden.

Für einen erfolgreichen Einsatz von C-ITS ist die Absicherung gegen ungültiges Verhalten sowie gegen bösartige Angriffe essentiell. Ohne einen solchen Schutz kann die Gültigkeit der von anderen Fahrzeugen erhaltenen Informationen nicht garantiert werden, sodass die Zuverlässigkeit aller C-ITS-Anwendungen beeinträchtigt wird. Die Forschung hat erhebliche Ressourcen in die Entwicklung grundlegender Sicherheitsfunktionen wie Pseudonymisierung und Absenderauthentifizierung investiert, was auch zu Standardisierung

[1] Englischer Titel der Dissertation: “Misbehavior Detection in Cooperative Intelligent Transport Systems” [He18a]

[2] Institut für verteilte Systeme, Universität Ulm, rens.vanderheijden@uni-ulm.de

geführt hat. Ein Bereich, der hierbei bisher wenig beachte wurde, ist das Fehlverhalten authentisierter Entitäten im Netzwerk. Ein bösartiges Fahrzeug kann gezielt Fehlverhalten aufzeigen, welches aufgrund gültigen Schlüsselmaterials von anderen Entitäten im Netzwerk als authentisch akzeptiert wird. Zum Beispiel könnte so versucht werden, gefälschte Nachrichten zu übermitteln, die gezielt eine Notfallreaktion auslösen, was im schlimmsten Fall einen Unfall zwischen anderen Fahrzeugen verursachen könnte. Solche Angriffe können mit Standard-Sicherheitsfunktionen wie kryptographischen Signaturen nicht verhindert werden, weswegen Erkennungsmechanismen für solche Angriffe unersetzlich sind.

Die Beiträge dieser Arbeit umfassen (a) einen Überblick über bestehende Mechanismen für Misbehavior Detection, (b) Maat, einen Vorschlag für ein generisches Fusionsframework zur Misbehavior Detection in C-ITS, (c) Multi-Source-Fusionsoperationen für Subjective Logic, die das mathematische Fundament unseres Frameworks bilden, (d) mehrere neue Erkennungsmechanismen, (e) eine detaillierte Überprüfung der Bewertungsmethoden und Vorschläge für neue Metriken, (f) einen neuen, öffentlichen Datensatz, der als Grundlage für den Vergleich von Erkennungsmechanismen dienen kann, (g) eine detaillierte Bewertung der vorgeschlagenen Mechanismen und Fusionsverfahren und (h) einen Ausblick, wie diese Ergebnisse auf andere cyberphysikalische Systeme angewendet werden können.

2 Stand der Forschung

In [He18b] beschreiben und klassifizieren wir verschiedene Erkennungsansätze die bereits in der Literatur behandelt sind. Die übergeordnete Klassifikation ist eine zweidimensionale Taxonomie, in der feinkörnigere Erkennungstechniken eingeordnet werden. Außerdem wird klassifiziert, wo die Erkennung stattfindet, sowie eine Abschätzung, inwiefern dieser Mechanismus mit Datenschutzanforderungen vereinbar ist. Ein besonders auffälliges Ergebnis war, dass viele Erkennungsansätze unterschiedliche, teilweise disjunkte Mengen von Angriffen erkennen können. Außerdem gibt es viele Mechanismen, die nur in bestimmten C-ITS-Szenarien anwendbar sind, z.B. nur im städtischen Verkehr oder nur auf Autobahnen. Diese zwei Erkenntnisse zeigen, dass die Kombination von Erkennungsmechanismen für die Entscheidungsfindung ein wesentlicher Bestandteil sein sollte, um die Sicherheit von C-ITS entsprechend zu verbessern. Diese Arbeit nähert sich dem Thema durch die Entwicklung von Maat, welches die Gültigkeit der empfangenen Daten sicherstellt.

Die bisherige Forschung hat sich mit dem Thema der Misbehavior Detection Frameworks bereits auseinandergesetzt. Wir beschreiben hier kurz vier wesentliche Arbeiten, die prototypisch für die bisherigen Ansätze sind, und unterschiedliche Stärken und Schwächen mit sich bringen: VEBAS von Schmidt et al. [Sc08], den Ansatz basierend auf Kalman Filter von Stübing [St13], das Framework von Raya [Ra09] und die Ideen von Bißmeyer [Bi14].

VEBAS [Sc08] kombiniert eine große Anzahl von Plausibilitäts- und Konsistenzmechanismen, die jeweils verschiedene Arten von Angreifern erkennen können. Die verschiedenen Mechanismen werden nach einer gewissen Laufzeit statisch zusammengeführt, wonach

mittels einem Exponential Weighted Average (EWA) ein Vetrauenswert abgeleitet wird. Die große Stärke dieser Arbeit ist die Einfachheit und die daraus folgende Interpretierbarkeit des Outputs. Schwächen sind u.a. die Inflexibiliät der Fusion, insbesondere wenn es darum geht, Mechanismen für neu erkannte Angriffsmuster hinzuzufügen, und die Verzögerung bei der Erkennung. Raya [Ra09] verfolgt ähnliche Ansätze, setzt aber einen noch stärkeren Fokus auf die Vertrauensmechanismen. Die späteren Arbeiten von Stübing [St13] und Bißmeyer [Bi14] beschreiben konkrete Ansätze für die Erkennung einer bestimmten Art von Angriffen, nämlich die Fälschung der Positionsdaten, die periodisch von den Fahrzeugen verbreitet werden. Im Ansatz von Stübing wird ein dediziertes Framework gebaut, um trotz des Einsatzes von Pseudonymisierungsalgorithmen aus den Nachrichten benachbarter Fahrzeugen mittels eines Kalman-Filters abschätzen zu können, wo sich welches Fahrzeug befindet. Dieses Framework hat die große Stärke, dass die Ergebnisse direkt verfügbar sind und ggf. angewendet werden können; das Framework ist jedoch nicht für andere Arten von Daten geeignet. Der Erkennungsansatz von Bißmeyer hat ähnliche Ziele und basiert darauf, dass der Angreifer bei Fälschung der Position eine Überschneidung mit der Position eines benachbartes Fahrzeug riskiert. Was in diesen Arbeiten fehlt, ist die Flexibilität, wie dies bei Arbeiten wie VEBAS möglich ist, neue Erkennungsmechanismen hinzuzufügen.

3 Maat

Als Teil der Doktorarbeit wurde ein neues Framework entwickelt, Maat, dessen grundsätzlicher Ansatz es ist, die Ergebnisse verschiedener Erkennungsmechanismen mittels Subjective Logic zu fusionieren. Subjective Logic ist ein mathematisches Framework, welches den Ausdruck von Unsicherheit über Daten mittels sogenannten Opinions ermöglicht. Um dies zu ermöglichen, wurden Beiträge zur Logik selbst geliefert, sowie die Entwicklung neuer Erkennungsmechanismen, die Reproduktion und Verbesserung bestehender Erkennungsmechanismen, und der Aufbau eines Weltmodells, in dem die Erkennungsergebnisse verwaltet, ausgewertet und ggf. verbreitet werden können. Maat verwendet diese Logik, um ein flexibles Datenmanagement- und Fusionssystem aufzubauen, das die Vertrauenswürdigkeit der Daten bei jedem Zugriff durch Anwendungen bestimmt. Zur Unterstützung dieses Datenmanagements verwendet Maat einen gerichteten Graphen zur Speicherung der Daten und der zugehörigen Erkennungsergebnisse. Durch die getrennte Erfassung der Daten und der dazugehörigen Detektionsergebnisse kann eine Vielzahl von potenziellen neuen Detektoren untersucht werden. Darüber hinaus ermöglicht es den Austausch von Erkennungsergebnissen, zum Beispiel für die Revocation.

Erkennungsmechanismen Im Rahmen der Dissertation wurden verschiedene Erkennungsmechanismen entwickelt und erweitert [HLK18]. Außerdem haben wir versucht Ergebnisse bestehender Arbeiten zu reproduzieren, um diese an die neuen Anforderungen der C-ITS anzupassen. Im Folgenden wird beispielhaft der Acceptance Range Threshold (ART) [Sc08] eingeführt. Dieses Erkennungsverfahren prüft anhand des Abstands und

einer Abschätzung der Kommunikationsreichweite, ob die Positionsinformationen gefälscht wurden; ein Beispiel ist in Abbildung 1 zu sehen.

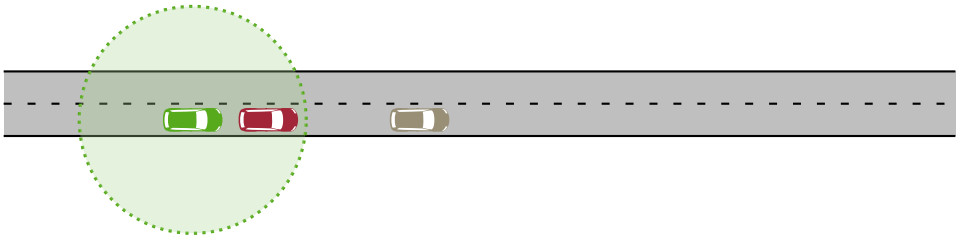


Abb. 1: Das grüne Fahrzeug nimmt für den ART die zirkelförmige Kommunikationsreichweite an, und erkennt hierdurch den roten Angreifer, welcher vorgibt, an der grauen Position zu sein.

Eine Schwäche dieses Mechanismus ist, dass die Empfangstreichweite als fest angenommen wird, was jedoch bei sich schnell fortbewegenden Fahrzeuge nicht der Fall ist. Aufgrund dessen wird vorgeschlagen, mittels Subjective Logic eine Unsicherheit auszudrücken, die in der Fusion mit anderen Mechanismen eine bessere Erkennungsrate ermöglicht [HLK18].

Subjective Logic Subjective Logic bietet eine Vielzahl von Fusionsoperatoren, um Opinions zu fusionieren [Jø16]. Eine Opinion ist definiert über ein Zufallsvariabele X und besteht aus zwei Funktionen und einem Wert; der Belief Function $\mathbf{b}$, der Base Rate $\mathbf{a}$, und dem Unsicherheitswert u. Die Belief Function modelliert explizites Wissen, während die Base Rate A-priori-Wissen modelliert; durch die additive Eigenschaft $1 = u + \sum_{x \in X} \mathbf{b}(x)$ wird die Second-order Uncertainty mittels u beschrieben. Um die Opinions verschiedener Entitäten fusionieren zu können, ist eine Verallgemeinerung der existierenden Fusionoperatoren nötig, da manche Fusionsoperatoren nicht kommutativ sind. Diese wurde im Rahmen der Dissertation [He18a] geliefert; als Beispiel zeigt Definition 1 die WBF, bei der die Evidenz weder unendlich noch null ist $(\forall A \in \mathbb{A} : u_X^A \neq 0) \wedge (\exists A \in \mathbb{A} : u_X^A \neq 1)$. Für die Base Rate wird aus Platzgründe auf [He18a] verwiesen.

Definition 1 (Multi-source WBF) *Gegeben die Opinion $\omega_X^A = (\mathbf{b}_X^A, u_X^A, \mathbf{a}_X^A)$ von Aktor $A \in \mathbb{A}$ über die Zufallsvariable X ist die gemeinsame Opinion $\omega_X^{\widehat{\diamond}\mathbb{A}} = (\mathbf{b}_X^{\widehat{\diamond}\mathbb{A}}, u_X^{\widehat{\diamond}\mathbb{A}}, \mathbf{a}_X^{\widehat{\diamond}\mathbb{A}})$:*

$$\mathbf{b}_X^{\widehat{\diamond}\mathbb{A}}(x) = \frac{\sum\limits_{A \in \mathbb{A}} \mathbf{b}_X^A(x)\left(1 - u_X^A\right) \prod\limits_{A' \in \mathbb{A}, A' \neq A} u_X^{A'}}{\left(\sum\limits_{A \in \mathbb{A}} \prod\limits_{A' \neq A} u_X^A\right) - |\mathbb{A}| \cdot \prod\limits_{A \in \mathbb{A}} u_X^A} \qquad u_X^{\widehat{\diamond}\mathbb{A}} = \frac{\left(|\mathbb{A}| - \sum\limits_{A \in \mathbb{A}} u_X^A\right) \cdot \prod\limits_{A \in \mathbb{A}} u_X^A}{\left(\sum\limits_{A \in \mathbb{A}} \prod\limits_{A' \neq A} u_X^A\right) - |\mathbb{A}| \cdot \prod\limits_{A \in \mathbb{A}} u_X^A}$$

Um bereits existierende Fusionsansätze modellieren zu können, die nicht in Subjective Logic vorhanden sind, wurden außerdem die Operatoren Minimum (MIN) und Majority

(MAJ) definiert. Um Vertrauensbeziehungen zwischen Fahrzeugen mit einbeziehen zu können, bietet Subjective Logic bereits transitive Vertrauensbeziehungen. Letztlich wurde im Rahmen der Dissertation eine Variante des EWA vorgeschlagen, welche über Opinions definiert ist, da dieser Ansatz häufig in der Literatur zur Anwendung kommt.

Weltmodell Maat nutzt die Subjective Logic um Beziehungen zwischen Informationen, Entitäten und Erkennungsmechanismen in einem gerichteten Graph zu modellieren, bei dem die Kanten mit Opinions beschriftet werden. In Abbildung 2 befindet sich ein Beispiel für einen solchen Graph. Die Semantik der Kanten von Maat zum Erkennungsmechanismus ist eine konfigurierbare Gewichtung (welche wir mit *Fusionability* bezeichnen), während die Kanten vom Erkennungsmechanismus zu Daten oder Entitäten den Erkennungsergebnissen entsprechen. Die Kanten von Entitäten zu anderen Entitäten oder zu Daten sind Opinions, die in einer Nachricht mitübertragen werden können.

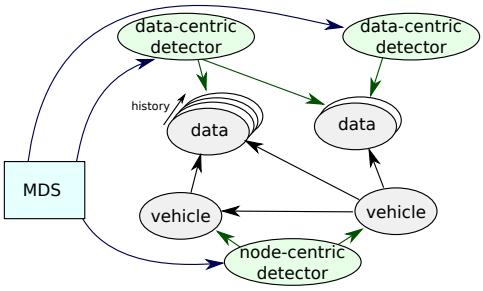


Abb. 2: Ein Weltmodell in Maat, in dem zwei Fahrzeuge Daten liefern, und innerhalb von Maat drei Erkennungsmechanismen genutzt werden. Alle Kanten werden mit Opinions beschriftet.

Wenn eine neue Nachricht im Fahrzeug eingeht, wird diese an Maat übermittelt und an alle angeschaltete Erkennungsmechanismen weitergegeben, die über diese (und ggf. ältere) Nachrichten jeweils Opinions erzeugen; diese werden anschließend zusammen mit den Informationen in der neuen Nachricht gleichtzeitig im Weltmodell gespeichert. Eine C-ITS Anwendung kann jederzeit Anfragen an das Weltmodell stellen; dieses wird zur Zeit der Anfrage den letzten konsistenten Zustand nutzen und eine Fusion durchführen. Die Laufzeit, bis ein neuer konsistenter Zustand vorliegt, hängt maßgeblich von der Laufzeit der einzelnen Erkennungsmechanismen ab, die modular wählbar sind.

Um eine Anfrage beantworten zu können, wird in Maat der Fusionsprozess in Abbildung 3 angestoßen und durchgeführt. Um das Vertrauen in bestimmte Daten zu bestimmen, wird zuerst eine Pfadsuche durchgeführt. Danach wird in jedem Pfad der Transitive-Trust-Operator genutzt, um das Pfad-Vertrauen zu berechnen; insbesondere wird hierdurch das Vertrauen in den Erkennungsmechanismus mit eingerechnet. Dies ist nützlich um die Erkennung nachträglich optimieren zu können (z.B. wenn Maat bereits in vielen Fahrzeugen implementiert ist). Danach wird der konfigurierte Fusionsoperator genutzt, um das Gesamtvertrauen zu berechnen. Das Ergebnis ist eine Opinion, die wahlweise zu einer

Entscheidung projiziert werden kann (wie in der Abbildung dargestellt) oder von einer Anwendung direkt verarbeitet werden kann. Letzteres ist insbesondere nützlich, wenn die Anwendung die Unsicherheit der Opinion direkt verarbeiten kann.

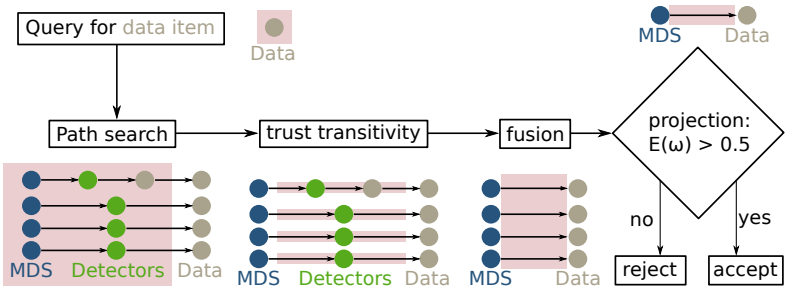


Abb. 3: Das Fusionsprozess von Maat

4 Auswertung

Da die meisten Arbeiten weder Quellcode des Detektors, noch Quellcode des Angreifers, noch das Auswertungsszenario veröffentlichen, ist die Reproduktion bestehender Ergebnisse erschwert; für einige Arbeiten konnten daher die Ergebnisse nur teilweise reproduziert werden. Um dieses Problem für die Zukunft zu vermeiden, wurde ein synthetischer Datensatz entwickelt, welcher auf Basis verbreiteter Open-Source Tools eine Grundlage für Angriffserkennung bildet. Dieser Datensatz, VeReMi, besteht neben dem Auswertungsszenario auch aus Angriffen; die Erkennungsmechanismen wurden als Teil von Maat veröffentlicht. Es ist allerdings wichtig zu betonen, dass dieser Datensatz immer als *Grundlage* dienen sollte; VeReMi bietet einen Rahmen, in dem neue Angriffe ergänzt werden können.

Metriken Im Rahmen dieser Arbeit wurden zwei Kategorien von Metriken analysiert: Anwendungsmetriken und Erkennungsqualitätsmetriken. Für die Anwendungsmetrik wurde die Anwendung Cooperative Adaptive Cruise Control (CACC) als Grundlage gewählt; da in der Literatur noch keine geeignete Metriken oder Angriffe vorhanden waren, wurde die Analyse solcher Angriffe im Detail durchgeführt. Im Rahmen von [HLK17] haben wir herausgestellt, wie die Anfälligkeit von CACC für Angriffe aussieht, sowohl in der Form von Jamming als auch in der Form von Datenfälschung. Für die Erkennungsqualität wurde Precision & Recall gewählt, auf Basis der korrekte Klassifikation der Nachrichten.

Der Datensatz, der im Rahmen der Arbeit entwickelt wurde, bietet ein realistisches Verkehrsszenario, auf dem CACC allerdings nicht direkt einsetzbar war. Dementspechend wurden hierfür die Erkennungsmetriken eingesetzt, die auch bei bestehenden Arbeiten zum Einsatz kommen. Es lässt sich allerdings noch ergänzen, dass viele bisherige Arbeiten die Metriken auf die Erkennung von Angreifern anwenden, statt auf die Erkennung von Angreifernachrichten. Der Unterschied zeigt sich darin, dass im ersten Fall nur am Ende

des Simulationsdurchlaufs analysiert wird, wie vielen Angreifern fälschlicherweise vertraut wurde. Viel interessanter ist jedoch, insbesondere für C-ITS Anwendungen, wie sich das Vertrauen pro Nachricht zusammenstellt; ob der Angriff am Ende erkannt wurde, reicht nicht aus, wenn der Angriff vorher schon einen Unfall ausgelöst hat. Aufgrund dessen wird in unseren Arbeiten über die Nachrichten aggregiert statt über die Fahrzeuge.

Neben der Standardmetrik (Precision & Recall) analysieren wir auch den Gini Index des False Positive (FPR) bzw False Negative rates (FNR) über die Fahrzeuge. Ziel hiervon ist festzustellen, wie gleichmäßig solche Fehler sind; je gleichmäßiger die Fehler, desto unwahrscheinlicher ist es, dass ein Austausch von Erkennungsergebnissen die Erkennung verbessern könnte. Außerdem dient dieser Ansatz zur Überprüfung der These, dass das Verhältnis zwischen Fahrzeug und Angreifer die Möglichkeit der korrekten Erkennung maßgeblich beeinflusst. Wenn ein Angreifer zum Beispiel die Position lediglich um wenige Millimeter fälscht, ist die Erkennung nicht möglich, weil dies wesentlich unterhalb der Messfehler von GPS liegt; um den maximalen Recall zu erreichen sollten jedoch auch diese Angriffe erkannt werden. Der Gini Index G_{FPR} wird für eine Simulation mit μ gutartigen Fahrzeugen, die jeweils eine FPR von x_i haben, wie folgt definiert: $G_{FPR} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|x_i - x_j|}{2n^2\mu}$

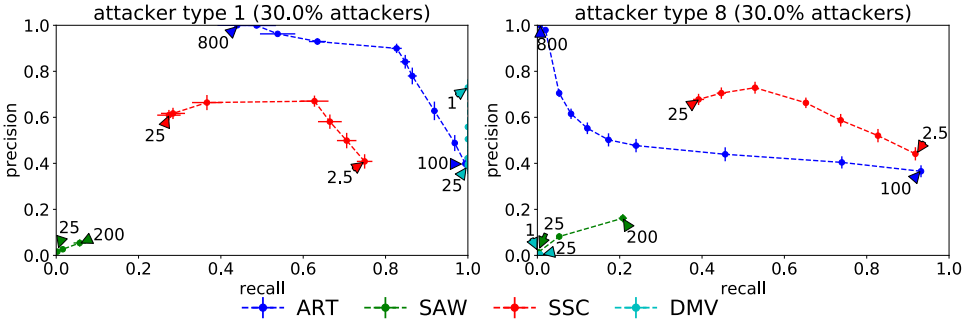


Abb. 4: Erkennungsergebnisse einzelner Erkennungsalgorithmen (aus [HLK18])

Ergebnisse & Diskussion Basierend auf der beschriebenen Auswertungsmethodik und dem VeReMi-Datensatz wird im Folgenden die Auswertung von Maat dagestellt. Hierzu wurde Maat mit verschiedenen Erkennungsmechanismen ausgestattet, welche bereits in unserer VeReMi-Arbeit vorgestellt wurden [HLK18]. Im folgenden werden beispielhaft Erkennungsergebnisse im Bezug auf Angreifer Typen 1 (immer die gleiche Position) und 8 (für jede Nachricht ein Random Offset der echten Position) in ein Szenario mit hoher Verkehrsdichte und Angreiferdichte (30%) abgebildet. In Abbildung 4 sind die Mechanismen mit unterschiedlichen Schwellwerten abgebildet. Hieraus lässt sich ablesen, dass sich die Erkennungsmechanismen stark in ihrer Performanz unterscheiden, in Abhängigkeit von der Art der Angreifer. Zum Beispiel erkennt der DMV-Detektor Angreifer 1 immer (Recall = 1), jedoch Angreifer 8 nie (Recall = 0). Hieraus lässt sich ableiten, dass die Fusion verschiedener Mechanismen nötig ist, denn ansonsten könnte der Angreifer den richtigen Angriff wählen,

um die Erkennung zu umgehen. In Abbildung 5 ist im gleichen Szenario die Fusion mit zwei unterschiedlichen Werten für den EWA und jeweils fünf unterschiedlichen Fusionsansätzen dargestellt. Die Zahlen in dem Plot stellen hier das Basisvertrauen der Mechanismen dar. Bei der Fusion wurde zusätzlich EWA eingesetzt, um die Qualität der fusionierten Ergebnisse vor der Fusion zu erhöhen. Da in unserem Szenario die Angreifer jede Nachricht manipulieren, sollte der EWA hier eine höhere Erkennungsrate ermöglichen. Allerdings zeigen die Ergebnisse, dass der EWA nur marginal beeinflusst, welche Angreifernachrichten erkannt werden (leichte Steigerung im Recall), aber eine bedeutende Reduktion der Precision zur Folge hat. Außerdem ist direkt erkennbar, dass MIN allen Nachrichten misstraut, während MAJ hauptsächlich vom Angreifer abhängt (gut gegen Angreifer 1, schlecht gegen Angreifer 8). Zwischen den einzelnen Subjective Logic Operatoren gibt es keinen Operator, der in jedem Fall gut funktioniert; in zukünftigen Studien soll herausgearbeitet werden, inwiefern Verbesserungen an den Erkennungsmechanismen hier Fortschritte ermöglichen. Eine Alternative hierzu wäre die programmatische Beschreibung des Fusionsprozesses, womit festgelegt werden kann, welcher Prozess wozu geeigneter ist; in diesen Fall würde für jede Anwendung ein jeweils passender Prozess definiert werden müssen.

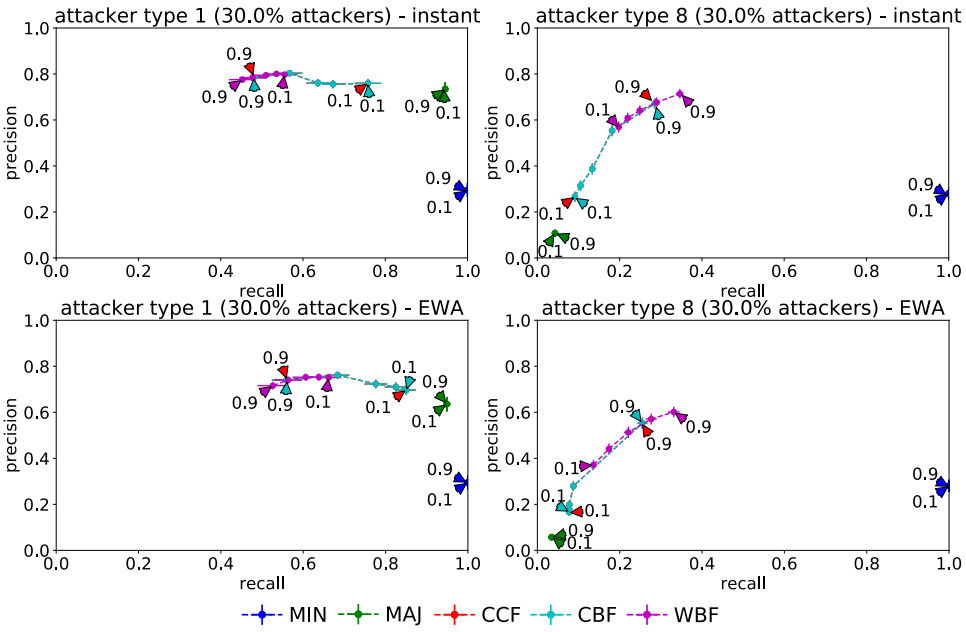


Abb. 5: Ergebnisse für verschiedene Fusionsoperatoren, mit einem EWA von 1 und 0.1.

5 Zusammenfassung

In dieser Arbeit wurde basierend auf einer ausführlichen Literaturanalyse für Misbehavior Detection ein neues Framework, Maat, beschrieben und implementiert. Dieses Framework

ermöglicht die Kombination verschiedener Erkennungsverfahren mittels Subjective Logic, sowie die Möglichkeit, das Framework mit neuen Erkennungsansätzen anzureichern. Um dies zu erreichen, wurden im Rahmen der Subjective Logic verschiedene Beiträge geleistet: insbesondere wurden die nicht-kommutativen Fusionsoperatoren verallgemeinert und verschiedene Operatoren entwickelt, die naive Fusionsansätze modellieren. Es wurden außerdem verschiedene neue Erkennungsmechanismen entwickelt und es wurden die Ergebnisse verschiedener bestehender Arbeiten reproduziert. Zur Auswertung wurden neue Mertiken entwickelt, die die neuen Anforderungen von C-ITS berücksichtigen, wobei insbesondere die Qualität der Erkennung ohne Vertrauensmechanismus betrachtet wird. Dies ist wichtig, da es bekannte Angriffstechniken gibt um Vertrauensmechanismen anzugreifen.

Über die konkreten Ergebnisse für Misbehavior Detection hinaus wurde in der Arbeit beleuchtet, wie sich diese Ansätze auf andere Cyber-Physical Systems übertragen lassen. Im Rahmen dieses Ausblicks wurde analysiert, inwiefern sich die Fusion direkt auf das Monitoring von Industriesteuersysteme übertragen lässt. Hierbei stellt sich klar heraus, dass die Erfolgswahrscheinlichkeit einer zielführenden Erkennung wesentlich von der Informationsgrundlage der Erkennungsmechanismen abhängt. Im Bereich der Industriesteuersysteme ist diese Informationshierarchie sehr heterogen, was dazu führt, dass die Erkennung verteilt umgesetzt werden sollte. Außerdem basieren viele reale Angriffe auf fehlender Authentisierung in bestehenden verdrahteten Netzwerken; hier ist es für einen Angreifer einfach, alle Informationsflüsse zum Erkennungssystem zu kontrollieren.

Zukünftige Arbeiten können sich mit der Anwendung von Maat für fahrzeuginterne Angriffserkennungszwecke, sowie die Verbesserung der Erkennungsrate mittels dynamischer Konfiguration beschäftigen. Für fahrzeuginterne Netzwerke stellt sich besonders die Frage, ob die Erkennung mit echtzeitfähigen Mechanismen ausreichend ist. Die Ergebnisse der Arbeit legen nahe, dass die dynamische Konfiguration und Gewichtung eine erhebliche Verbesserung der Erkennungsrate ermöglichen könnte, da die Fehlerrate der einzelnen Mechanismen einen starken Zusammenhang mit dem Szenario aufweist. Obwohl bisherige Experimente mit Maat auf Cyber-Physical Systems beschränkt sind, ist der Fusionsprozess im Prinzip lösungsneutral. Dies bedeutet, dass Maat theoretisch auch für die Fusion anderer Angriffserkennungsmechanismen eingesetzt werden könnte. Das Framework könnte auch für andere High-Level-Informationsfusionsanwendungen zum Einsatz kommen, jedoch müssten hierfür neue Auswertungsansätze entwickelt werden. Die größte Hürde hierbei ist jedoch die Opinions geeignet zu wählen, so dass eine Fusion auch einen nennenswerten Vorteil hat.

Literatur

[Bi14] Bißmeyer, N.: Misbehavior Detection and Attacker Identification in Vehicular Ad-hoc Networks, Diss., Darmstadt Technical University, 2014.

[He18a] van der Heijden, R. W.: Misbehavior detection in cooperative intelligent transport systems, Diss., Universität Ulm, 2018.

[He18b] van der Heijden, R. W.; Dietzel, S.; Leinmüller, T.; Kargl, F.: Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. IEEE Communication Surveys & Tutorials/, 2018.

[HLK17] van der Heijden, R. W.; Lukaseder, T.; Kargl, F.: Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC). In: Vehicular Networking Conference. VNC, Best paper award, IEEE, S. 45–52, Nov. 2017.

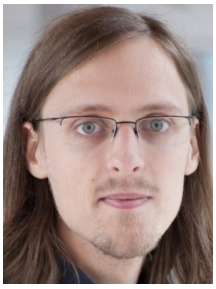
[HLK18] van der Heijden, R. W.; Lukaseder, T.; Kargl, F.: VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs. In: 14th EAI SecureComm. Springer, Aug. 2018.

[Jø16] Jøsang, A.: Subjective Logic: A Formalism for Reasoning Under Uncertainty. Springer International Publishing Switzerland, 2016.

[Ra09] Raya, M.: Data-centric trust in ephemeral networks, Diss., Lausanne: EPFL, 2009.

[Sc08] Schmidt, R. K.; Leinmüller, T.; Schoch, E.; Held, A.; Schäfer, G.: Vehicle Behavior Analysis to Enhance Security in VANETs. In: Proceedings of the 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008). IEEE, S. 1–8, 2008.

[St13] Stübing, H.: Multilayered Security and Privacy Protection in Car-to-X Networks, Diss., 2013.



Rens W. van der Heijden wurde am 19. September 1989 in den Niederlanden geboren. Er hat in August 2010 sein Bachelor in Informatik abgeschlossen und bekam im August 2012 einen *cum laude* Masterabschluss in *Computer Science* mit Spezialisierung in IT-Sicherheit. Am 9. November 2018 promovierte er *magna cum laude* an der Universität Ulm beim Institut für Verteilte Systeme bei Prof. Dr. Frank Kargl. Seit 2018 ist er wissenschaflticher Mitarbeiter am gleichen Institut und forscht dort schwerpunktmäßig an IT-Sicherheit in Fahrzeugen im Rahmen des BMBF SecForCARs Projekts. Seine weiteren Forschungsinteressen sind Subjective Logic, Intrusion Detection und Privacy. Er ist außerdem in der Lehre vertreten, wo er die Vorlesung Security & Privacy in Mobile Systems liest.