Ochrona integralności dynamicznych sieci Ad-Hoc w kontekście sieci samochodowych typu VANET

The security of the dynamic Ad-Hoc networks' integrity in the context of VANET automobile network

mgr inż. Krzysztof Stępień

Instytut Informatyki, Politechnika Łódzka

Łódź, 3 Czerwca 2022

Agenda

1. Problematyka
2. Typy sieci Ad-Hoc, VANET
    1. Rodzaje ataków na sieć VANET
    2. Atak typu Sybil
    3. Atak typu Bogus
3. Przegląd literatury
4. Autorskie rozwiązanie
    1. Przeprowadzone symulacje
    2. Wyniki
5. Wnioski
6. Opublikowane publikacje

Problematyka

- Obecnie produkowane pojazdy stają się stopniowo coraz bardziej powiązane z Internetem
- Szereg rozwiązań oferowanych przez nowe systemy wspiera zarówno kierowców, jak i producentów samochodów
- Nowe rozwiązania przynoszą też nowe kwestie bezpieczeństwa i problemy z podłączeniem wszystkich samochodów w jedną sieć
- Z pomocą przychodzą tutaj sieci typu Ad-Hoc, które niestety są podatne na ataki
- Ataki te mogą bezpośrednio doprowadzić do uszkodzenia sieci, straty czasu, pieniędzy, a nawet życia użytkowników podłączonych do sieci

Typy sieci Ad-Hoc

- MANET (Mobile Ad Hoc Network)
- **VANET** (Vehicular Ad Hoc Network)
- SPAN (Smartphone Ad Hoc Network)
- Wireless Mesh Network
- FANET (Flying Ad hoc Network)
- Army Tactical MANET
- Navy Ad Hoc

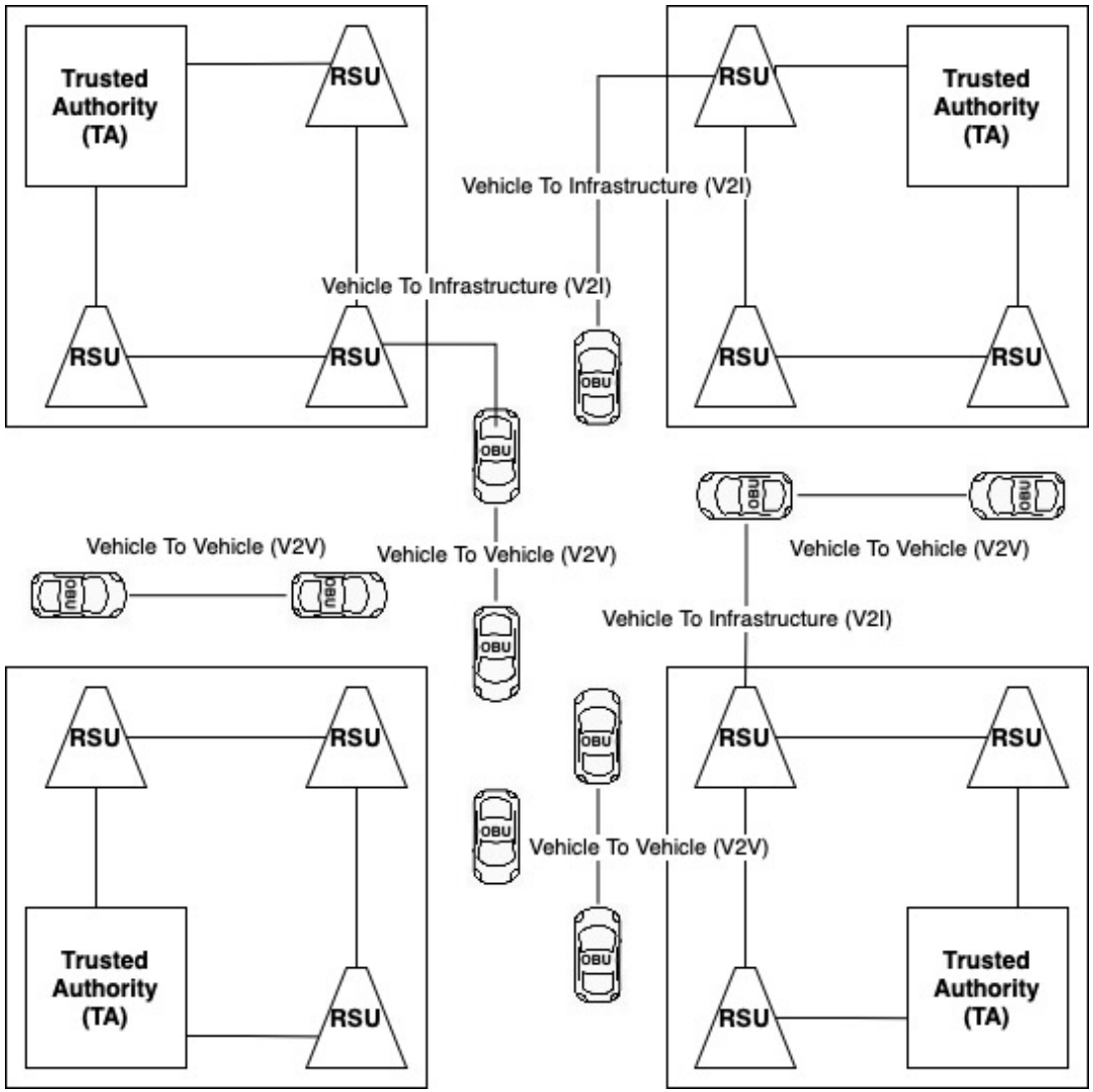
VANET

Vehicular Ad-Hoc networks (*VANET*s) – sieć tworzona zgodnie z zasadami mobilnych sieci (*MANET*s) – spontaniczna kreacja sieci bezprzewodowej dla komunikacji Samochód-Samochód.

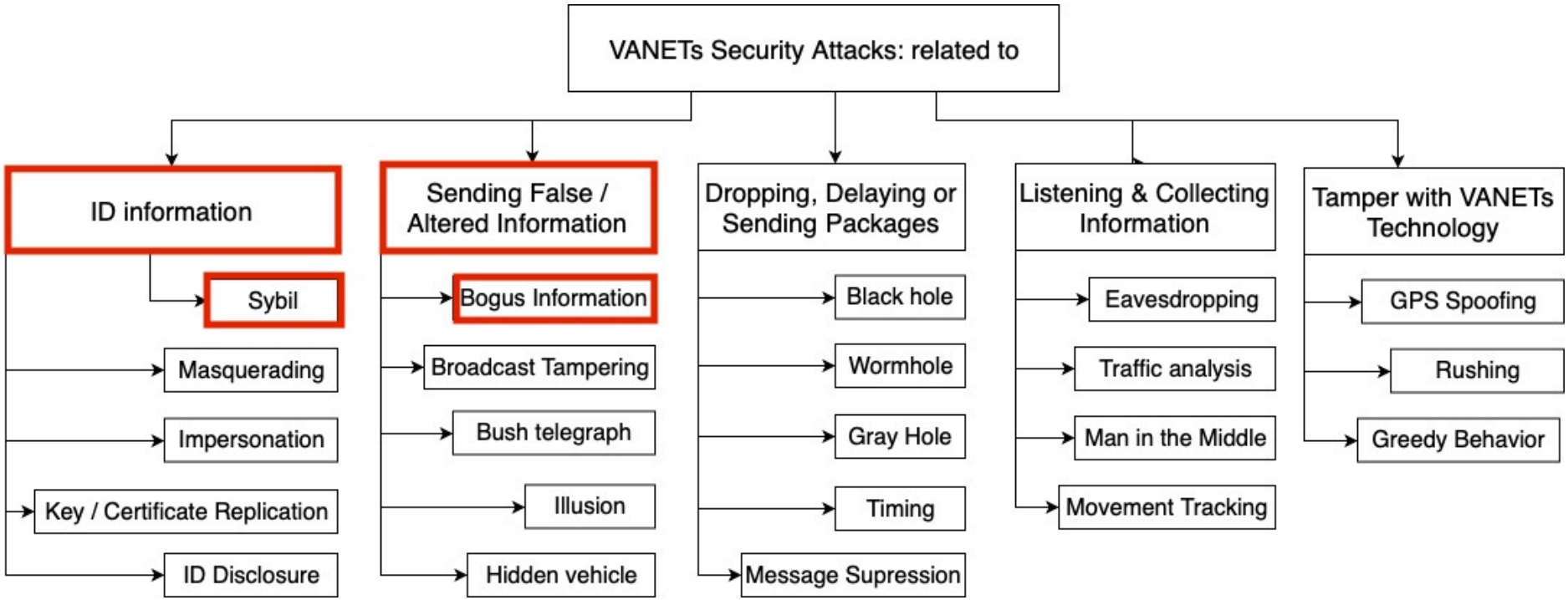
Możemy wyróżnić dwa typy węzłów:

- *RoadSide Unit* (*RSU*)
- *OnBoard Unit* (*OBU*)

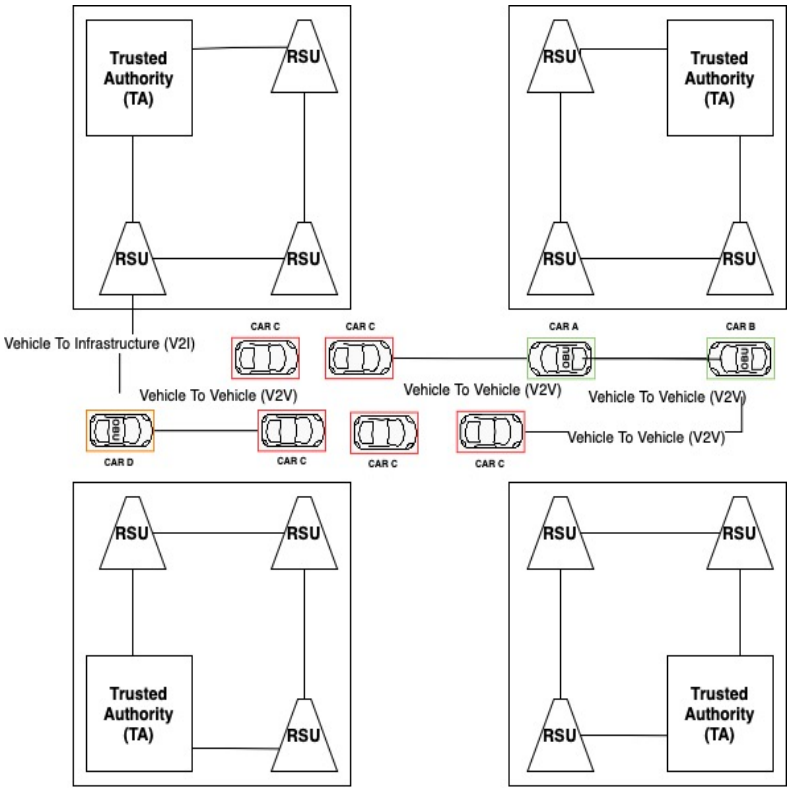
Struktura sieci VANET



Rodzaje ataków na sieć VANET

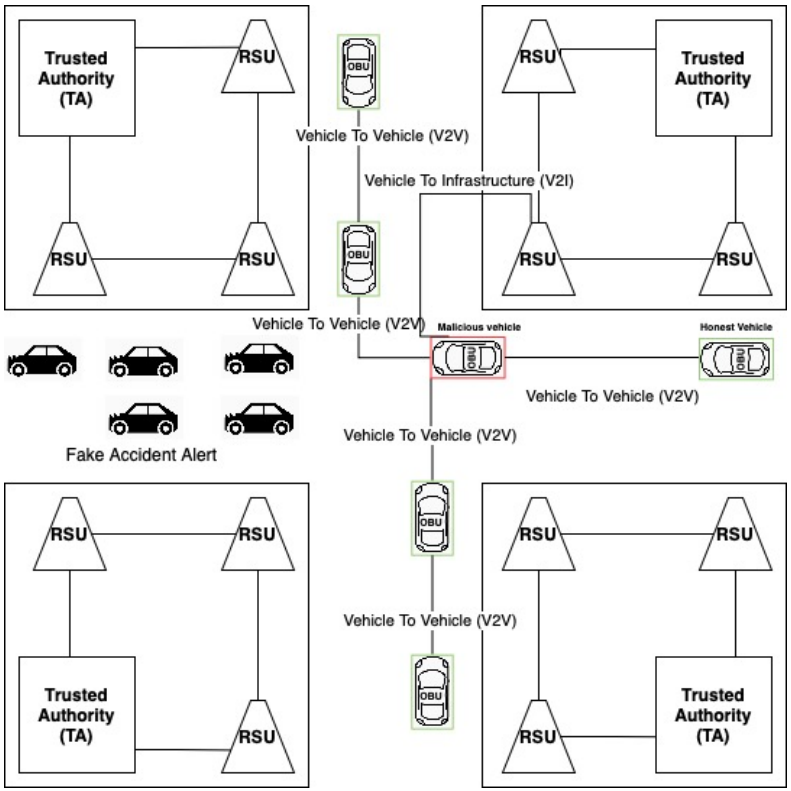


Atak typu Sybil



- Atak ten opiera się na tworzeniu fałszywej sąsiedniej obecności w sieci *VANET*
- W celu wykonania takiej formy ataku, pojazd tworzy fałszywą reprezentację kilku pojazdów w tym samym czasie i miejscu

Atak typu Bogus



- Jest to typ ataku na sieci *VANET* opierający się na wysyłaniu fałszywych informacji do sieci
- Atak opiera się na przesyłaniu nieprawidłowych lub fałszywych informacji w sieci w celu uzyskania korzyści osobistej

Ochrona integralności dynamicznych sieci Ad-Hoc w kontekście sieci samochodowych typu VANET

Problematyka pracy doktorskiej skupia się na stworzeniu **autorskich rozwiązań / algorytmów** mających na celu przeciwdziałanie atakom typu **Sybil oraz Bogus** na sieć typu VANET, a co za tym idzie **zapobieganiu celowej modyfikacji danych** dokonanej z użyciem zaawansowanych technik, mających na celu **zachwiania ich spójności**.

Cel badań

- **Analiza** głównych **problemów sieci VANET**
- Porównanie aktualnie stosowanych ataków i **wyłonienie dwóch typów ataków**, w których przewiduje się możliwość zastosowania nowych rozwiązań
- **Przegląd literatury** i stworzenie zestawienia aktualnie stosowanych metod
- Stworzenie autorskiej metody – **B&SEBP&F (Enhanced Behaviour Processing & Footprint)** przeciwdziałania atakom typu Sybil oraz Bogus
- **Przeprowadzenie symulacji** mającej na celu zebranie wyników działania i efektywności stworzonego algorytmu
- **Porównanie wyników** autorskiej metody wraz z aktualnie stosowanymi rozwiązaniami

Przegląd stanu wiedzy w tematyce badań

Przeprowadzony został przegląd dotychczasowych publikacji. Wyłoniono łącznie 369 publikacji dotyczących ataków typu Sybil (spośród nich zaakceptowano do głębszej analizy 116) oraz 231 publikacji dotyczących ataków typu Bogus (spośród nich zaakceptowano do głębszej analizy 70). Powodem odrzucenia pozostałych artykułów była:

- Analiza domeny ataku na innej warstwie sieciowej
- Rozwiązania dotyczące problematyki użycia Blockchaina
- Przeglądowe artykuły, które nie wnosiły autorskich metod przeciwdziałania atakom.

Przegląd literatury

W ramach przeglądu literatury wybrano artykuły z ostatnich 8 lat, tj. **2014-2022**. Dodatkowo zostały **ustalone kryteria przyjęcia i odrzucenia**. Zostały postawione **pytania badawcze**, takie jak:

- **Jakie ograniczenia** narzucają autorzy, które należy przeanalizować i poprawić?
- Czy podczas symulacji brane są pod uwagę **masowe ataki**?
- **Jakie są osiągnięte lub oczekiwane** główne **korzyści** proponowanego rozwiązania?

Ataki typu Sybil - analiza publikacji

Wydawca	Związane z tematem badań	Wybrane do dalszej analizy	Powód odrzucenia
ScienceDirect	93	34	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej, rozwiązania tylko dla sieci MANET, brak zaproponowanych metod przeciwdziałania
SpringerLink	119	16	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej
IEEE	57	20	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej.
ACM	100	46	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej

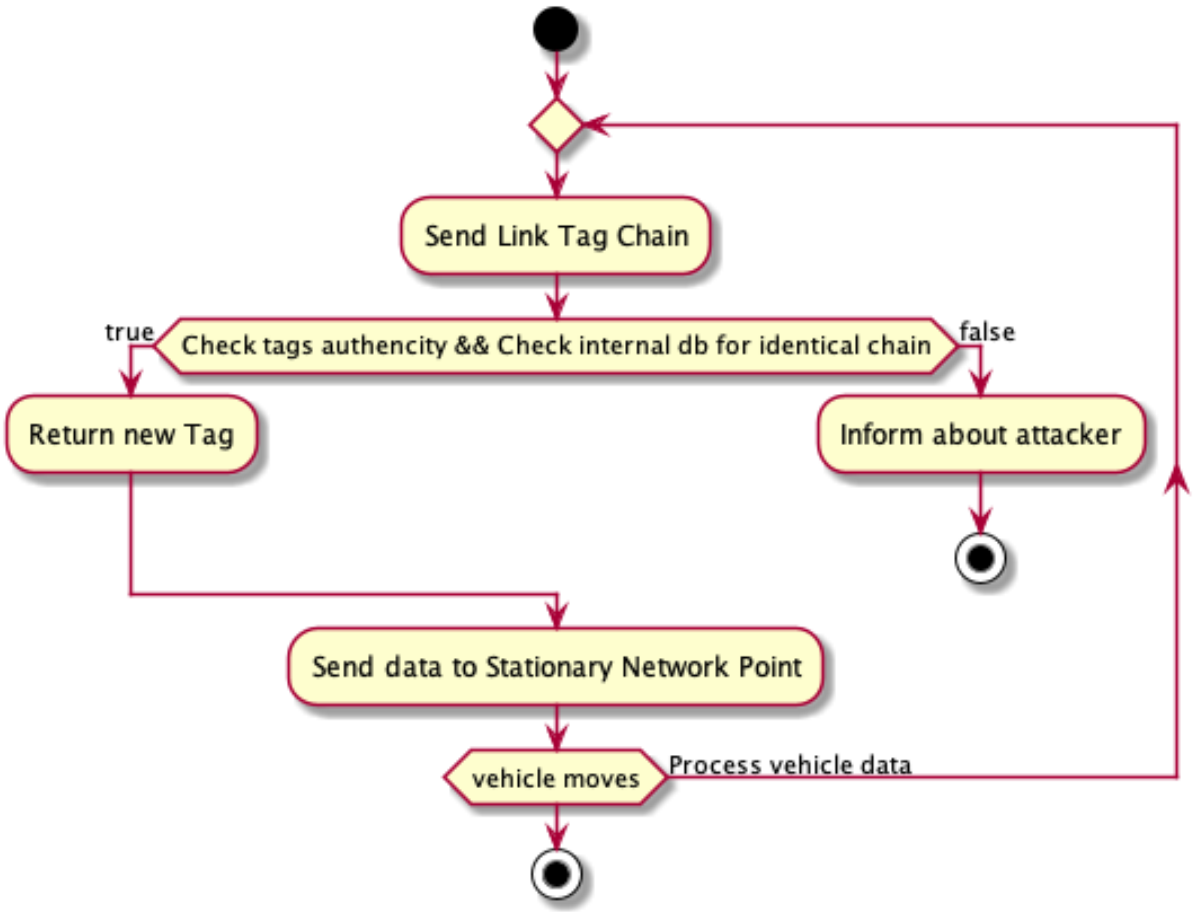
Ataki typu Bogus - analiza publikacji

Wydawca	Związane z tematem badań	Wybrane do dalszej analizy	Powód odrzucenia
ScienceDirect	56	17	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej.
SpringerLink	59	14	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej
IEEE	16	9	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej
ACM	100	30	Blockchain, tematyka głównie przeglądowa, rozwiązania bezpieczeństwa dla innej warstwy sieciowej

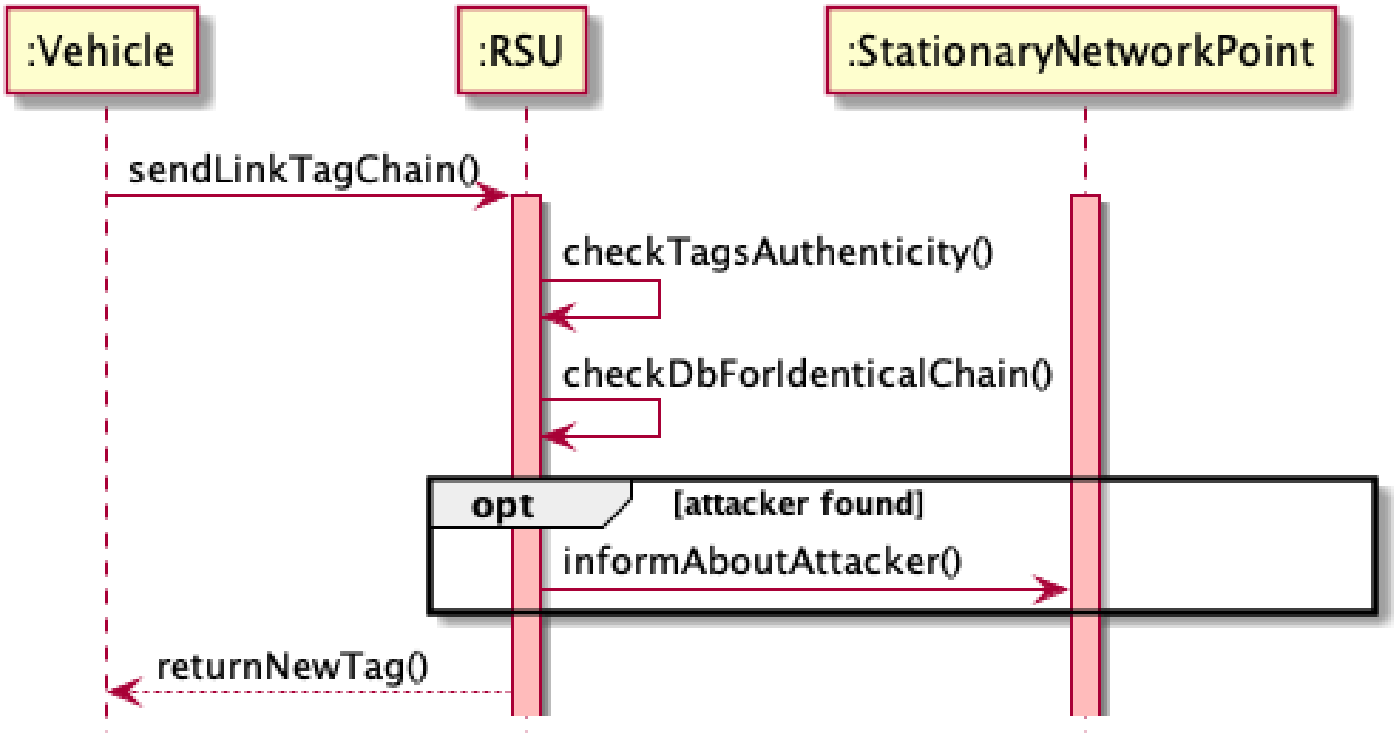
Autorskie rozwiązanie - algorytm B&SEBP&F

- **Algorytm Footprint** – analiza link tagów oraz timestamp-ów wysyłanych przez węzły w sieci
- Stworzony **system reputacji węzłów**
- Identyfikacja atakujących poprzez analizę porzuconych pakietów przy użyciu algorytmu **SDGA**

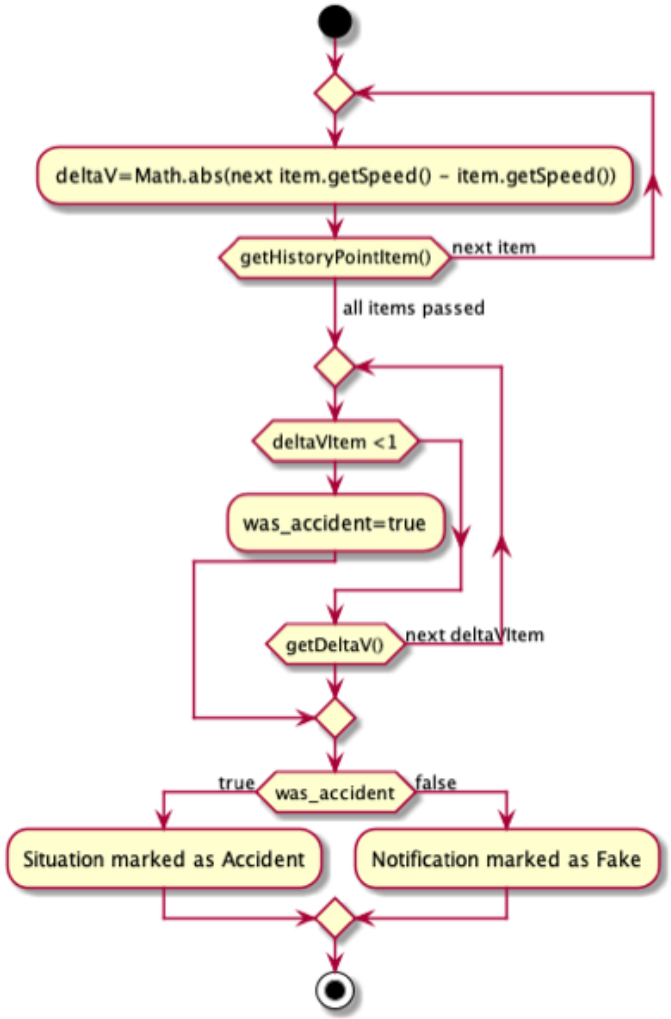
Autorskie rozwiązanie - przeciwdziałanie atakowi typu Sybil



Autorskie rozwiązanie - przeciwdziałanie atakowi typu Sybil

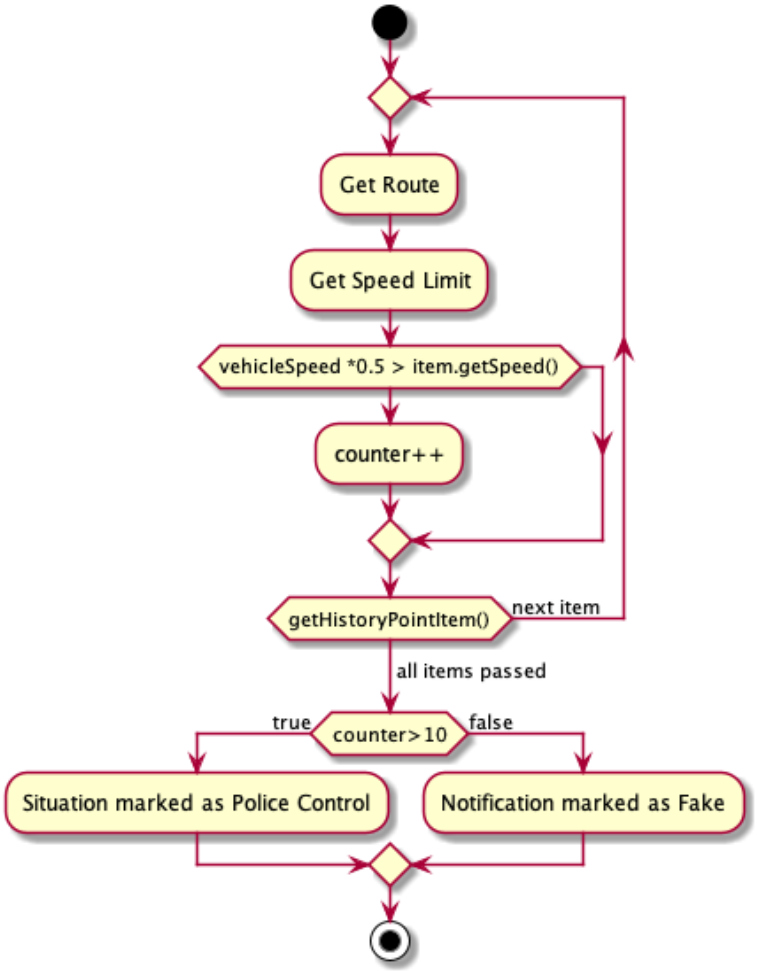


Autorskie rozwiązanie - przeciwdziałanie atakowi typu Bogus



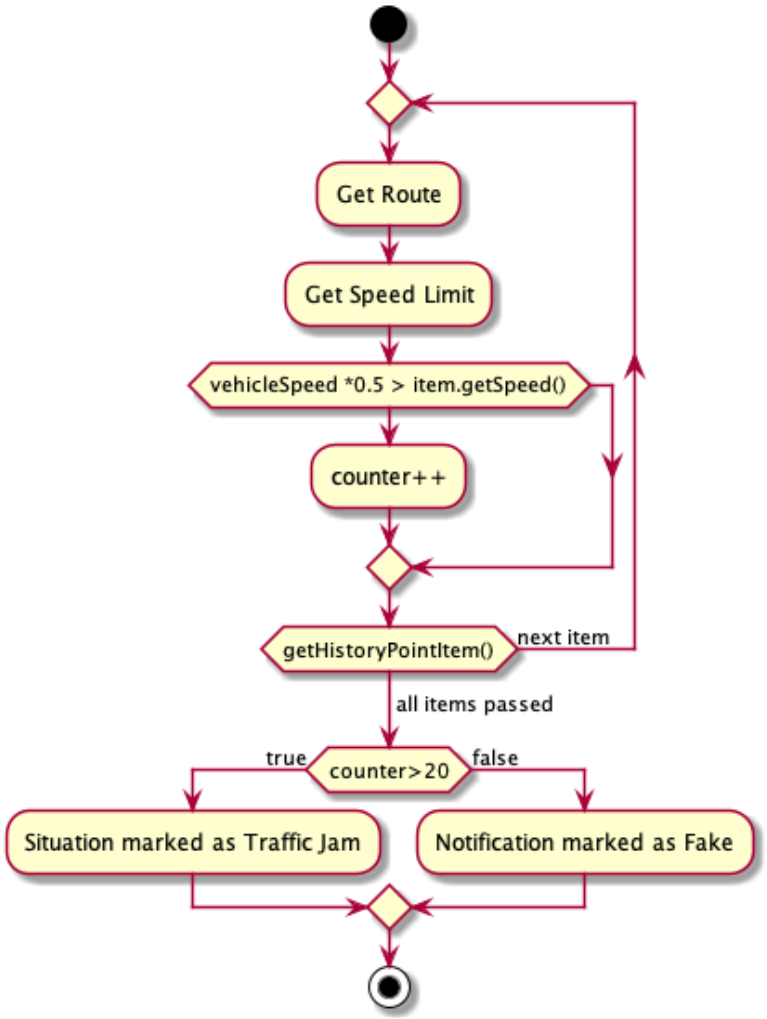
$$[isAccident = |nextItem.getSpeed() - item.getSpeed()| < 1$$

Autorskie rozwiązanie - przeciwdziałanie atakowi typu Bogus



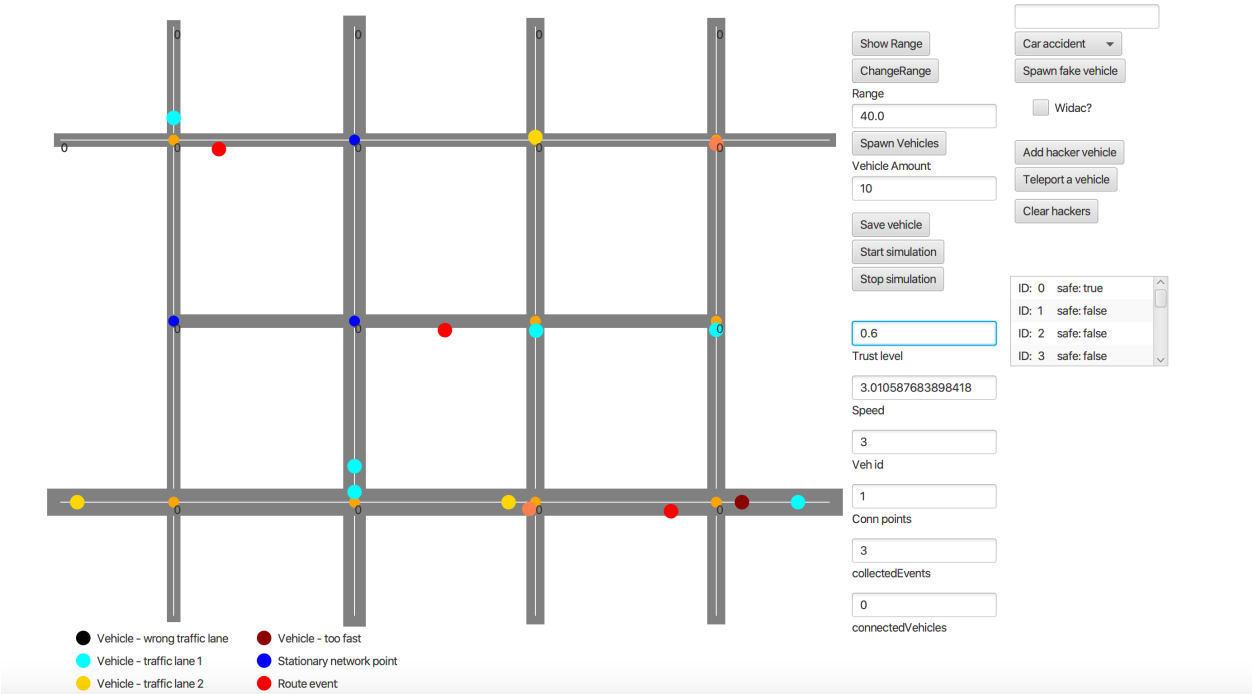
$$\left\| \sum_{i=1}^{10} roadEventCounter = vehicleSpeedRestriction * 0.5 > item.getSpeed() \right\|$$

Autorskie rozwiązanie - przeciwdziałanie atakowi typu Bogus



$$\left\| \sum_{i=1}^{20} trafficJamCounter = vehicleSpeedRestriction * 0.5 > item.getSpeed() \right\|$$

Środowisko do testów symulacji i analizy autorskiej metody B&SEBP&F



Procesor: **Intel Core i5 2.3GHz**, Pamięć RAM: **16 GB DDR3**, Dysk: **SSD 256GB**, wersja środowiska Java: **JDK 11**

Parametry symulacji

Stworzony został **prototyp aplikacji**, który **symuluje zachowanie uczestników drogi oraz atakujących**. Przygotowano **20 scenariuszy testowych** na podstawie zebranego stanu wiedzy oraz przeprowadzono eksperyment z następującymi parametrami:

- Poziom zintensyfikowania pojazdów – **10 - 200**
- Liczba skrzyżowań – **1, 2, 3, 4**
- Analiza rozpoznania – **pierwszy atakujący, kolejni atakujący, aż do ostatniego**
- Stosunek liczby atakujących do normalnych uczestników ruchu drogowego – **30% - 100%**

Przeprowadzona symulacja z wykorzystaniem algorytmu B&SEBP&F - wyniki

No Exper.	False Positives after Identifying All Attackers	Time to First Detection	Time to All Detection	No of Ordinary Vehicle	No of Attackers	Attacker to Ordinary Ratio
1	1	18.73	32.90	10	1	0.0901
2	2	3.062	35.65	10	5	0.33
3	1	3.24	34.65	10	10	0.5
4	1	2.74	2.743	50	1	0.019
5	1	2.835	34.79	50	5	0.09
6	2	2.757	37.744	50	25	0.33
7	5	2.836	44.968	50	50	0.5
8	9	2.842	33.834	100	20	0.16
9	11	2.873	44.23234	100	60	0.375
10	7	2.823	39.07	100	75	0.42
11	5	2.91	46.47	100	100	0.5
12	0	28.3	41.851	0	10	1.0
13	0	28.668	40.558	0	20	1.0
14	0	26.884	97.919	0	56	1.0
15	0	24.612	54.653	0	100	1.0
16	3	2.951	30.53	15	3	0.16
17	3	2.96	44.10	15	5	0.25
18	3	2.96	35.80	15	10	0.4
19	4	5.263	45.326	15	15	0.5

Dotychczas przeprowadzone symulacje w literaturze - wyniki

No Experiment	False Pos. after Ident. All Attack.	Time to All Detection	No. of Ordinary Vehicle	No. of Attackers	Attacker to Ordinary Ratio	Method
1	1	165	95	5	0.05	RABTM
2	2	158	90	10	0.11	RABTM
3	1	140	85	15	0.17	RABTM
4	1	122	80	20	0.25	RABTM
5	1	110	75	25	0.33	RABTM
6	1	45	45	5	0.11	DMV
7	1	40	40	10	0.25	DMV
8	2	35	35	15	0.42	DMV
9	1	32	30	20	0.66	DMV
10	1	30	25	25	1.0	DMV
11	1	20	85	15	0.17	Motion Trajectories Similarity
12	2	40	80	20	0.25	Motion Trajectories Similarity
13	1	60	70	30	0.42	Motion Trajectories Similarity
14	1	80	65	35	0.53	Motion Trajectories Similarity
15	4	100	60	40	0.66	Motion Trajectories Similarity
16	1	120	55	45	0.81	Motion Trajectories Similarity
17	1	140	50	50	1.0	Motion Trajectories Similarity
18	1	55	90	10	0.11	RSUs cooperation
19	1	60	85	15	0.17	RSUs cooperation
20	3	70	80	20	0.25	RSUs cooperation
21	1	80	75	25	0.33	RSUs cooperation
22	1	90	70	30	0.42	RSUs cooperation

Wyniki

- Stosunek normalnych kierowców do atakujących – **5% - 100%**
- Średni stosunek – **30%**
- Najbardziej korzystne scenariusze – **liczba zwykłych pojazdów większa niż liczba atakujących**
- Maksymalna liczba użytkowników – **200 pojazdów**
- Średni czas wykrycia pierwszego atakującego – **29 ms**

Wyniki

- Odchylenie standardowe – **±15%**
- Usprawnienie w stosunku do aktualnie stosowanych metod – **w zależności od scenariusza testowoego - do 30%**
- Średnia liczba false positive-ów – **1 (dla 90% przeprowadzonych eksperymentów)**

Wnioski

- Sieć VANET okazuje się być dobrą alternatywą dla uniwersalnego oraz scentralizowanego Internetu
- Pomimo badań prowadzonych od początku 2000 r., nowe rozwiązania bezpieczeństwa wciąż stanowią wyzwanie
- Brak rozwiązań bezpieczeństwa w sieciach VANET może doprowadzić do dezinformacji wewnątrz ww. sieci
- Przyszłością ITS (Intelligent Transportation System) jest sieć Ad Hoc dla pojazdów

Bibliografia

1. Junwei Liang, Jianyong Chen, Yingying Zhu, Richard Yu, A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position, Applied Soft Computing Journal, Vol. 75(2019).
2. Basant Subba, Santosh Biswas, Sushanta Karmakar, A game theory based multi layered intrusion detection framework for VANET, Future Generation Computer Systems, Vol. 82 (2018).
3. Dimitrios Kosmanos, Apostolos Pappas, Leandros Maglaras, Sotiris Moschoyiannis, Francisco J. Aparicio-Navarro, Antonios Argyriou, Helge Janicke, A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles, Array, Vol. 5 (2020).
4. Marwane Ayaida, Nadhir Messai, Sameh Najeh, A Macroscopic Traffic Model-based Approach for Sybil Attack Detection in VANETs, Ad Hoc Networks, Vol. 90, 101845 (2019).
5. Ayoob Ayoob, Ghaith Khalil, Morshed Chowdhury, Robin Doss, Intrusion Detection System Classifier for VANET Based on Pre-processing Feature Extraction, Future Network Systems and Security (2018).
6. Hoon Shin, Kyuho Son, and Dongsoo Han, Sybil Tolerant Consensus Method Using Mutual Proof of Validation. In Proceedings of the 2020 2nd International Electronics Communication Conference (IECC 2020). Association for Computing Machinery, New York, NY, USA (2020).

Opublikowane publikacje

1. Stepień K., Poniszewska-Marańda A.: Security Measures with Enhanced Behavior Processing and Footprint Algorithm against Sybil and Bogus Attacks in Vehicular Ad Hoc Network. Sensors, 2021, MDPI, Vol. 21, No 5, 3538, 2021, pp. 1-26, open access, JCR, 100 pkt
2. Stępień K., Poniszewska-Marańda A.: Security methods against Black Hole attacks in Vehicular Ad-Hoc Network. IEEE International Symposium on Network Computing and Applications, NCA, 2020, November 24-27, 2020, Cambridge, MA, USA, (Eds. A. Gkoulalas-Divanis, M. Marchetti, D. Avresk), IEEE, 2020, 140 pkt
3. Stępień K., Poniszewska-Marańda A.: Analysis of security methods in Vehicular Ad-Hoc Network against Worm Hole and Gray Hole attacks, Proceedings of 18th IEEE International Symposium on Parallel and Distributed Processing with Applications, ISPA, 2020, December 17-19, 2020, Exeter, UK, IEEE, New York, NY, Exeter, UK, IEEE, New York, NY, USA, Publisher: IEEE (2020), pp. 371-378, 70 pkt
4. Stępień K., Poniszewska-Marańda A.: Security measures in the Vehicular Ad-Hoc Networks in the aspect of DoS attack. (Eds. L. Barolli et al.), Complex, Intelligent and Software Intensive Systems. CISIS 2020, in Advances in Intelligent Systems and Computing, AISC 1194, Vol. 1194, Chapter 21, Springer International Publishing 2021, Proceedings of 14th International Conference on Complex, Intelligent and Software Intensive Systems, CISIS-2020, 1-3 July 2020, Łódź, Poland, pp. 222-232, 70 pkt
5. Stępień K., Poniszewska-Marańda A.: Security measures in Vehicular Ad-Hoc Networks on the example of Bogus and Sybil attacks, Advanced Information Networking and Applications, AINA 2020, in Advances in Intelligent Systems and Computing, AISC 1151, Vol. 1151, Chapter 38, pp. 419-430, Publisher: Springer International Publishing (2020) (Proceedings of 34th International Conference on Advanced Information Networking and Applications, AINA-2020, 15-17 April 2020, Caserta, Italy), 70 pkt

Opublikowane publikacje

6. Stępień K., Poniszewska-Marańda A.: Security solution methods in the Vehicular Ad-Hoc Networks. (Eds. P. Delir Haghighi, I. Luiz Salvadori, M. Steinbauer, I. Khalil, G. Anderst-Kotsis), ACM Proceedings of 17th International Conference on Advances in Mobile Computing and Multimedia (MoMM '19), December 2-4, 2019, Munich, Germany, ACM, New York, NY, USA, Publisher: ACM (2019), pp. 127-135, 70 pkt
7. Stępień K., Poniszewska-Marańda A., Marańda W.: Securing Connection and Data Transfer Between Devices and IoT Cloud Service. Integrating Research and Practice in Software Engineering. Studies in Computational Intelligence 851, Springer, 2020, ISSN 1860-949X, ISSN 1860-9503 (electronic), pp. 83 – 96., 70 pkt
8. Stępień K., Poniszewska-Maranda A.: Security Measures in the Vehicular Ad-Hoc Networks – Man in the Middle Attack. (Eds. I. Awan et al.), Mobile Web and Intelligent Information Systems, MobiWIS 2019, Proceedings of 16th International Conference on Mobile Web and Intelligent Information Systems, 26-28 August 2019, Istanbul, Turkey, LNCS 11673, Springer 2019, pp. 136-147., 70 pkt
9. Stepień K., Poniszewska-Marańda A.: Towards the security measures of the Vehicular Ad-Hoc Networks.(Eds. Andrzej M. J. Skulimowski et al.), Internet of Vehicles. Technologies and Services Towards Smart City (IOV 2018), LNCS 11253, , Springer-Verlag Heidelberg (2018), Proceedings of 5th International Conference on Internet of Vehicles, 20-22 November 2018, Paris, France), pp. 233-248, WoS, 70 pkt

Dziękuję za uwagę