2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) | 978-1-6654-3161-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/CCNC49033.2022.9700580

An Interaction Provenance-based Trust Management Scheme For Connected Vehicles

Mohammad Aminul Hoque
Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL 35294-1241
Email: mahoque@uab.edu

Ragib Hasan
Department of Computer Science
University of Alabama at Birmingham
Birmingham, AL 35294-1241
Email: ragib@uab.edu

***Abstract*—Connected vehicles (CVs) have facilitated the development of intelligent transportation system that supports critical safety information sharing with minimum latency. However, CVs are vulnerable to different external and internal attacks. Though cryptographic techniques can mitigate external attacks, preventing internal attacks imposes challenges due to authorized but malicious entities. Thwarting internal attacks require identifying the trustworthiness of the participating vehicles. This paper proposes a trust management framework for CVs using interaction provenance that ensures privacy, considers both in-vehicle and vehicular network security incidents, and supports flexible security policies. For this purpose, we present an interaction provenance recording and trust management protocol. Different events are extracted from interaction provenance, and trustworthiness is calculated using fuzzy policies based on the events.**

***Index Terms*—connected vehicles; interaction provenance; trustworthiness; security, misbehaviour detection;**

I. Introduction

Vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication in the connected vehicle (CV) environment enables the exchange of valuable safety and mobility information to improve traffic conditions significantly [1], [2]. Despite such advantages, the CVs impose significant challenges in secure data transmission among the vehicles since vehicles may send wrong information intentionally or unintentionally. Such misbehavior may impact the safety of CVs, which leads to the requirement of evaluating the vehicles' trustworthiness.

The formal security requirements in V2V communication, defined in IEEE 1609.2 standard [3], require all the messages to be digitally signed and verified. Though such a mechanism can efficiently identify outsider attackers, identifying inside attackers who possess valid credentials is challenging. A Trust management system enables vehicles to decide whether the received message from a vehicle is trustworthy. The Trust of a vehicle is calculated and managed based on past behavior, which can be performed based on a central trusted authority or by the vehicles or RSUs in a decentralized way [4].

There are several challenges and requirements for trust management in the CV environment. Privacy of the vehicles needs to be ensured while accumulating activities across multiple pseudonym certificate periods. Attacks on sensors or other autonomous driving components also need to be considered while calculating trustworthiness. A revoked vehicle due to legitimate misbehaviors can redo the bootstrapping process through Security Credential Management System (SCMS) [1]. The re-authenticated vehicle with new certificates can perform similar malicious activities again as the granted access does not depend on past actions. Hence, flexible security policies are required based on the length and quality of the trust management process. Moreover, the mechanism should be capable of mitigating collusion attacks and bad-mouthing incidents. Current research works do not support all these requirements together.

This paper proposes an interaction provenance-based trust management framework for the CVs. Interaction provenance is a chronological order of historical interactive events between two or more subjects [5]. Vehicles' trustworthiness is calculated based on the nature and length of previous interactions. Interaction provenance contains in-vehicle and vehicular network events, which are used to extract trustworthiness through fuzzy logic engines by creating simplistic policies.

II. Trust Management for Connected Vehicles

A. Interaction provenance terminologies

Actor: An actor is a CV entity that sends and receives messages. In our system, vehicles, RSUs, and SCMS authorities are considered as the actors.

Event: An event is a sequence of actions or messages transferred between the actors.

Interaction: An interaction is a message or an action exchanged between two actors during an event.

Interaction provenance: Interaction provenance of an actor is a tamper-proof and chronologically ordered sequence of events.

Interactions are collected based on a particular event or set of events related to vehicular applications. Multiple interactions are comprised in an event. An event has its own set of descriptors explained using key-value pairs. A generic structure to represent events and interactions are shown below:

EVENT: [Descriptors [key:value], <List: Interactions>]

INTERACTION: [<List: Actor>, Action, EventID, Descriptors[<key:value>]]

B. Interaction provenance frame

An interaction is bound in an interaction provenance frame, which consists of two parts: interaction header and payload. An interaction provenance frame header consists of the following fields: TS (timestamp), ET (event type), AT (application type), MT (message type), actor1, actor2, actor3, and I-SEQ (interaction sequence). The header contains metadata, and the payload consists of the data to be sent or received.

C. Interaction provenance recording

The interaction provenance recording system consists of Interaction Gateway (IG) service and Trust Management Service (TMS). Figure 1 shows the detailed framework architecture.

Interaction gateway service: Interaction Gateway (IG) is a distributed service that runs across all the vehicles, RSUs, SCMS entities vehicles, and RSUs communicate with, and cloud services related to the CVs. It is responsible for collecting the interactions and reporting to the TMS. IG collects interactions from in-vehicle intrusion detection system (IDS) and V2X communication across different events. Each event has a descriptor and a list of interactions. The messages are enhanced with interaction headers (IH) to create an interaction frame and processed by two interaction header handlers (IHH). Later, the interaction logger (IL) collects and stores interactions in the interaction database (IDB), and IR reports them to TMS.

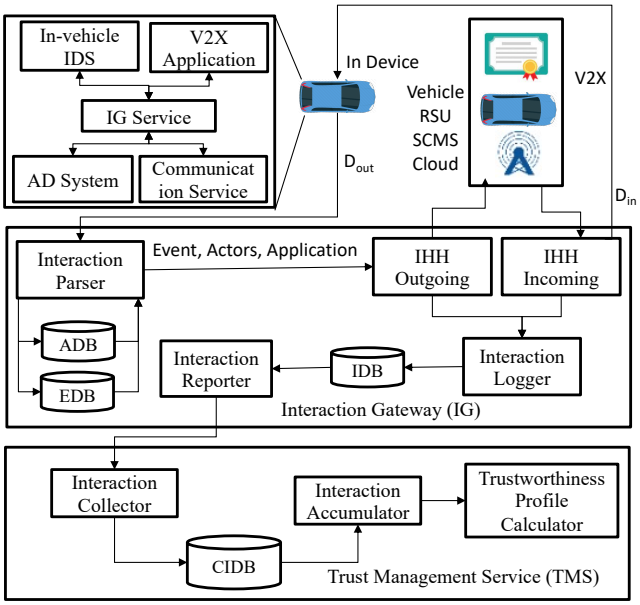

Fig. 1: Architecture of interaction provenance recording framework.

Trust management service (TMS): TMS is responsible for creating and maintaining the trustworthiness profile of a vehicle using interaction provenance. Interaction collector (IC) module collects all the interactions from the IR of IG. IC decrypts the interactions, verifies the signature, and stores them in a central interaction database (CIDB). The interaction accumulator (IA) module collects and specifies the interactions of a vehicle from CIDB. As the vehicles use pseudonym identity, the TMS contacts with linkage authority (LA) to link all the interactions of a vehicle together. Finally, the trustworthiness profile calculator (TPC) module periodically uses the accumulated interactions to update the vehicle's trustworthiness profile. The TMS can be integrated with misbehavior authority in SCMS.

D. Weighted interaction and vehicle trustworthiness profile

Each interaction is assigned a weight based on two properties.

Event (W_1): Weight is specified to the interaction based on the event type for a particular application. Depending on the event and application, the interaction can have four types of weights: very high, high, low, and very low.

Time (W_2): The weight of an interaction is also specified based on the event time, which reduces with the increasing difference with the current time. Hence, recent events have larger weights, and older events receive smaller weights.

Fuzzy ranges, aggregated weight, and trustworthiness profile mapping: We define weight mappings for each property of an interaction based on a pre-specified scale. Each interaction property is used with a combination function to calculate the total $weight$ of an interaction. The $interaction\ weight$ is calculated as: $InteractionWeight = \alpha_{E1}W_1 + \alpha_{E2}W_2$. Here α_x is a scalar coefficient for the linear combination function and $x \epsilon \{E1, E2\}$. For vector aggregation, polynomial features can also be used to create greater impact with increasing weight for a specific property. A defuzzifier function of predefined ranges similar to the fuzzifier function is applied to the aggregated weight. The defuzzifier provides a trustworthiness mapping for a particular vehicle, which is achieved by the fuzzy control logic and fuzzy ranges. Later, the trustworthiness is evaluated against threshold mapping and disseminated to the RSUs.

III. Design Discussion and Concluding Remarks

Interaction provenance-based trust management provides several advantages as it considers the events that a vehicle encounters in a chronological sequence. Since autonomy will be an integral part of the vehicles, considering both autonomy and connectivity events is required for identifying trustworthiness correctly. Moreover, accumulating trustworthiness across multiple pseudonym certificate periods in decentralized trust management schemes is not possible unless the Linkage Authority (LA) shares linkage information with RSUs or base stations. However, SCMS currently does not support this to ensure privacy. The proposed framework directly cooperates with LA and provides required privacy and linkability. The framework is also capable of preventing bad mouthing (wrong reputation dissemination regarding a benign vehicle) using the Bayesian inference technique [6]. Interaction provenance can prevent collusion attacks by adjusting fuzzy policies and emphasizing interactions among multiple different actors instead of colluding entities. The trustworthiness profile of the vehicle can be used to design flexible security policies. *Adaptive reputation initialization* and *threshold access control* for misbehavior detection and proper access control can be achieved based on the length and quality of the events the vehicle encountered previously.

Acknowledgement

This research was supported by the National Science Foundation through awards ECCS-1952090, ACI-1642078, and CNS-1351038.

References

[1] B. Brecht and T. Hehn, "A security credential management system for v2x communications," in *Connected Vehicles*. Springer, 2019, pp. 83–115.

[2] M. A. Hoque and R. Hasan, "Towards an analysis of the architecture, security, and privacy issues in vehicular fog computing," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–8.

[3] *Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*, vol. IEEE Standard 1609.2, 2016.

[4] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

[5] R. Khan and R. Hasan, "Fuzzy authentication using interaction provenance in service oriented computing," in *2015 IEEE International Conference on Services Computing*. IEEE, 2015, pp. 170–177.

[6] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Transactions on Intelligent Transportation Systems*, 2020.