Security Prediction and Forecasting for a Trust Management System in VANET

Mohammed A. Abdelmaguid Hossam S. Hassanein Mohammad Zulkernine
School of Computing, Queen's University, Kingston, Ontario, Canada
Emails:{18ma5, hossam, mz}@queensu.ca

***Abstract*—This paper explores utilizing proactive security measures as opposed to traditional reactive approaches in vehicular ad-hoc networks (VANETs). The paper focuses on integrating predictive approaches into every component of trust management systems (TMSs). This includes utilizing situation awareness (SA) to assess the trustworthiness of subjects and predicting the potential impact of attacks on trust services. Additionally, the study leverages attack rate data from honeypots to forecast ongoing attacks, aiming to improve the proactive capabilities of security measures in VANETs.**

***Index Terms*—vehicular ad hoc networks (VANETs), machine learning (ML), security, trust measurement, road safety**

I. Introduction

Vehicular ad-hoc networks (VANETs) are self-organizing networks where vehicles communicate in a decentralized manner, enhancing the driving experience through improved safety and efficient traffic management. The expansion of VANETs introduces significant security challenges. While standard protocols, such as those outlined in IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE), address message authentication, ensuring message correctness remains challenging. The presence of malicious entities within the network or the transmission of false information by drivers, referred to as misbehavior, can compromise the integrity of the entire communication process.

Traditional security measures are often reactive; thus, there is a pressing need for proactive strategies, such as attack forecasting and prediction, which utilize historical data and situational awareness to anticipate and mitigate potential threats. This paper proposes a novel proactive trust management system. This system, tailored for VANETs, aims to enhance security through early detection and mitigation of insider misbehavior.

II. Problem Statement

In VANETs, while public key infrastructure (PKI) ensures robust infrastructure security through authentication and certificate management, the ad-hoc segments face significant vulnerabilities from insider attacks. These attacks, perpetrated by authenticated users or entities that evade PKI, highlight the inadequacy of traditional reactive security" measures, which primarily focus on responding to breaches after they occur. This reactive approach proves insufficient against the complex and unpredictable nature of insider threats in VANETs. Consequently, there is a pressing need for proactive security measures that can preemptively address potential breaches and maintain network integrity.

III. Proposed Scheme

In the development of the proactive trust management system (TMS), our primary objective is to integrate proactive security measures into each of its core components. As illustrated in Figure 1, our system is structured around three pivotal modules, each corresponding to a component of TMS, which is integrated with a proactive security approach. The modules within our proposed approach include (1) the implementation of situation awareness (SA) for evaluating trust subjects, (2) the application of attack endgame prediction methodologies for trust services, and (3) the incorporation of unprepared-for attack prediction strategies concerning trust origin. These modules encompass our research objectives to construct a proactive TMS compatible with VANET environments, enhancing their security posture.

A. Trust Subject: Situation Awareness for Misbehaving Detection

Figure 2 shows the key components of the SA model to predict and assess the trustworthiness of subjects by identifying misbehavior. The SA model processes inputs from the environment and machine learning (ML) model outputs, not as binary outcomes but as probabilities to assess the likelihood of messages being benign or malicious. Feedback mechanisms are also incorporated to refine future outcomes based on past data and trust scores. The SA model comprises three levels: Perception, which gathers data such as location and speed from surrounding vehicles; Comprehension, where this data is analyzed to compute trust elements and reputation; and Projection, which predicts the trust level of other vehicles and decides on message acceptance. Environmental and individual factors, such as network stability, further influence these processes, enabling the model to adapt to changing conditions and improve misbehavior detection.

B. Trust Service: Attack Endgame Prediction

Figure 3 shows a workflow developed for predicting the attack endgame (e.g., causing hazards or accidents) [1] in VANETs, beginning with the collection of basic safety messages (BSMs) and cooperative awareness messages (CAMs). These messages are prepared in a time series format with selected features arranged chronologically to maintain the

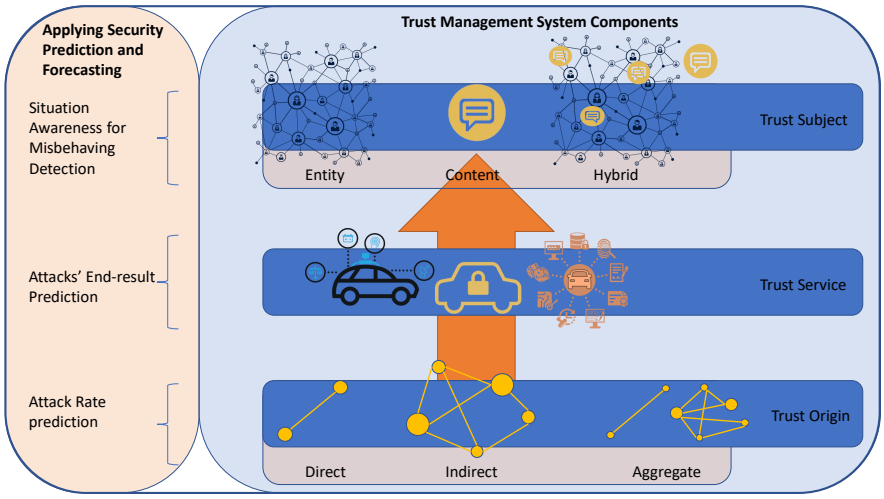

Figure 1: A trust management system for VANET with a proactive security approach for each component

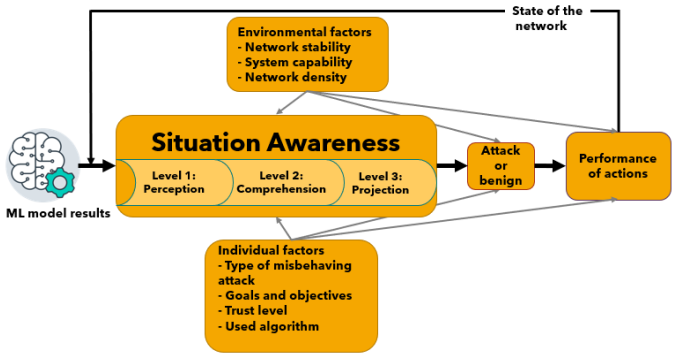

Figure 2: Situation awareness and machine learning model for detecting misbehavior attacks in VANETs

event sequences and fed to the ML model. In the training phase, a regressor fine-tunes the model to forecast network states. During testing, this attack endgame predictor utilizes new data to foresee ongoing attack outcomes. A decision-maker component analyzes predictions to determine message handling and mitigate attack impacts effectively.

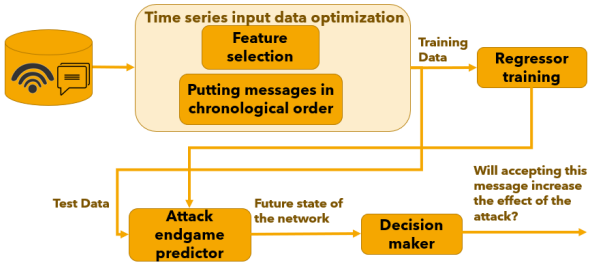

Figure 3: Predicting Attack Endgames in VANETs

C. Trust Origin: Attack Rate Prediction

Trust origin assesses the reliability of the connections through which trust is established. Utilizing honeypots and monitoring attack rates provides a robust method for predicting ongoing attacks in VANETs, which helps with evaluating trust origin. Honeypots, which serve as digital traps, simulate real network systems to attract and analyze attacker behaviors while safely gathering data without compromising actual vehicles. This data includes attack rates, which offer vital insights into the network's overall security state and helps adjust the trust levels assigned to vehicles in real-time. By functioning as an early warning system, elevated attack rates detected by honeypots can indicate potential risks, prompting immediate analysis and response. This approach enhances the capability to manage and predict security threats efficiently within VANETs, ensuring a proactive security stance in these critical systems.

IV. Experiments and Results

We independently tested each component of our proactive TMS. The first component, trust subject, detailed in [2], improved detection accuracy for misbehavior attacks, enhancing recall rates by up to 50% in some cases. The second component, trust service, reported in [1], successfully predicted attack effects up to 3.5 minutes in advance with over 80% accuracy.

V. Conclusion and Future Work

This study investigates implementing proactive security prediction techniques within each trust management system (TMS) component to enhance early attack detection and mitigation. Future research will explore further developments in Section III-C and assess the collective security performance when multiple TMS components, each equipped with proactive techniques, operate concurrently, aiming for a holistic improvement in system security.

References

[1] M. A. Abdelmaguid, H. S. Hassanein, and M. Zulkernine, "Attack endgame: Proactive security approach for predicting attack consequences in VANET," in *ICC IEEE International Conference on Communications*, 2023, pp. 3762–3767.

[2] M. A. Abdelmaguid, H. S. Hassanein, and M. Zulkernine, "Samm: Situation awareness with machine learning for misbehavior detection in VANET," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–10.