Team: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks

Mr.Nivin K S[1], Mr. Ambarish A[2], Mr. Unnikrishnan S Kumar[3]
[1,2,3] *Department of computer science and engineering, Malabar College of Engineering and Technology (MCET)*

***Abstract*- Vehicular ad-hoc network (VANET) provides a unique platform for vehicles to intelligently exchange critical information, such as collision avoidance messages. It is, therefore, paramount that this information remains reliable and authentic, i.e., originated from a legitimate and trusted vehicle. Trust establishment among vehicles can ensure security of a VANET by identifying dishonest vehicles and revoking messages with malicious content. For this purpose, several trust models (TMs) have been proposed but, currently, there is no effective way to compare how they would behave in practice under adversary conditions. To this end, we propose a novel trust evaluation and management (TEAM). The framework created has been tested with the implementation of three types of TMs (data oriented, entity oriented, and hybrid) under four different contexts of VANET based on the mobility of both honest and malicious vehicles. Results indicate that the TEAM is effective to simulate a wide range of TMs, where the efficiency is evaluated against different quality of service and security-related criteria. Such framework may be instrumental for planning smart cities and for car manufacturers.**

Index terms- Vehicular networks, trust management, smart cities, security, intelligent transportation systems, VEINS, SUMO, simulation

INTRODUCTION

Recently, a preeminent interest has been observed in the technologies to improve transportation around the world. Vehicular Ad-hoc Networks (VANET) is the state-of-the-art technology in the domain of transportation where vehicles communicate with each other and static Roadside Units (RSUs) via vehicle-to-vehicle (V2V) and vehicle-to- infrastructure (V2I) communication to offer various applications. It includes both safety (e.g., Traffic safety and efficiency) and non-safety (e.g., infotainment) applications [1]–[5]. VANET performs a key role in the emerging smart cities and Internet-of-Things (IoT) with the aim to improve overall transportation [6], [7]. Figure1illustrates the integration of VANET in smart cities where traffic safety is achieved by connecting vehicles to each other by virtue of V2V or V2I communication.

Since, applications offered to connected vehicles involve very critical information (such as steep-curve, or accident Warning), a secure, attack-free and trusted network is imperactive for the propagation of reliable, accurate and authentic information. In case of VANET, ensuring such network is extremely difficult due to its large-scale and open nature, making it susceptible to diverse range of attacks including man-in-the-middle (MITM), replay, jamming and eavesdrop- ping attacks [8]–[11]. Recently, various solutions have been proposed to achieve security in VANET.

Most of these solutions rely on traditional cryptography where vehicles utilize certificates and Public Key Infrastructure (PKI) to ensure security in the network. However, cryptography-based solutions reduce net- work efficiency due to following reasons. (1) Firstly, VANET includes both low and highly mobile vehicles which are dispersed randomly throughout the network, (2) Secondly, presence of an infrastructure cannot be ensured permanently, e.g., in rural areas, and (3) lastly, cryptographic solutions can be compromised by insider attacks in VANET, which

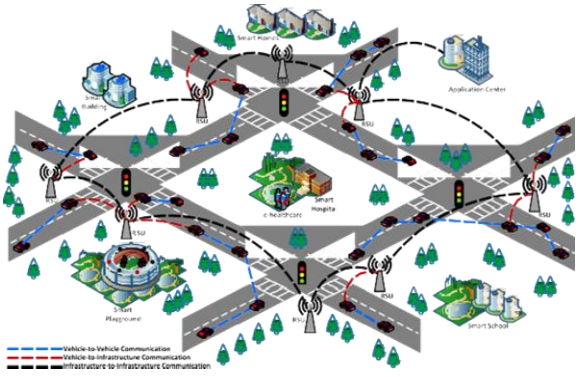


Illustration of VANET in smart cities

In order to address these shortcomings, trust has been proposed as a relevant technique to achieve network security. Trust is defined as the confidence of one node on the other for performing a specific action or set of actions. In VANET, it is established between two vehicles based on the messages exchanged regarding an event. Once, message is received, the evaluator node calculates trust based on numerous factors, including vehicles past interactions, vehicles reputation in the network and neighbors' recommendations about particular vehicle. However, trust between neighboring vehicles is created for a very limited duration of time due to highly mobile and randomly distributed vehicles. Therefore, establishing, calculating, and evaluating trust on received messages based on diverse factors in such short period of time is extremely challenging.

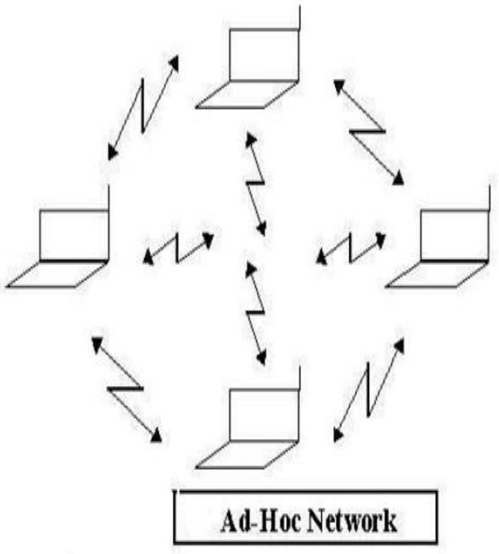
Trust, as a technique to achieve security in VANET, is in its early stage of development. Trust models (TMs) are embedded within vehicles to evaluate trustworthiness, accuracy and authenticity of received messages. TMs ensure the propagation of trusted information in the network by revoking both dishonest nodes (vehicle) and messages having malicious content. In VANET, TMs are classified into three distinct classes, i.e., entity-oriented, data-oriented and hybrid TMs [16]–[19]. Entity-oriented trust models (EOTM) aims to eliminate dishonest vehicles by evaluating trustworthiness on the node. Data-oriented trust models (DOTM) evaluates trust on the received messages (data) while hybrid trust models (HTM) relies on both vehicle and data for trust establishment.

In VANET, various TMs either are developed to ensure security by eliminating dishonest vehicles or tempered messages However, it is currently complicated to compare and evaluate the efficiency of these TMs due to absence of a unified trust evaluation framework. Moreover, high mobility and random distribution of vehicles across the network result in various contexts in VANET. Therefore, it becomes significantly important to take those contexts into account for trust management. For instance, in an urban location, extensive amount of messages (trusted & untrusted) are present due to low mobility of vehicles and abundant number of RSUs. On the other hand, rural areas cannot ensure the permanent presence of RSU. Moreover, high mobility and low number of vehicles in such locations produce minimum amount of messages. TMs, which depends on high number of RSUs and vehicles for trust management, will show poor results for a scenario with minimum number of vehicles. As a result, both scenarios demand separate techniques to evaluate trustworthiness on transmitting node and their messages. VANET can succeed only if secure and trusted messages are ensured in every context.

In this paper, we addressed this problem by proposing a novel trust evaluation and management framework called TEAM, which have the ability to evaluate TMs in numerous contexts of VANET. In TEAM framework, we model and evaluate the efficiency of different TMs based on main objects of VANET. i.e., data and node. Moreover, major attacks are also identified based on asset-based threat model and ISO-based risk assessment as a preliminary study. Once, the list of attacks related to TM is available, the TMs are evaluated under these attack models in different contexts of VANET. This can determine the impact of malicious attacks on TMs and their performance in various con- texts. In order to do so, we conducted an extensive set of experiments to evaluate the performance of TMs from each category (EOTM, DOTM & HTM) using TEAM. Simulation results depict that our framework can accurately evaluate the efficiencies of TMs in various context of VANET.

1.1 VEHICULAR AD HOC NETWORK

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motors, Toyota, Nissan, DaimlerChrysler, BMW and Ford promote this term.



1.2 STANDARDS

Intelligent vehicular ad-hoc network (InVANET) is another term for promoting vehicular networking. InVANET integrates multiple networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA and ZigBee. Vehicular ad hoc networks are expected to implement wireless technologies such as dedicated short-range communications (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are cellular, satellite, and WiMAX. Vehicular ad hoc networks can be viewed as component of the intelligent transportation systems (ITS). As promoted in ITS, vehicles communicate with each other via inter-vehicle communication (IVC) as well as with roadside base stations via roadside-to-vehicle communication (RVC).

The next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Vehicular Ad-hoc Networks (VANETs) can be considered as a subset of Mobile Ad hoc Networks (MANETs) with unique characteristics. A typical VANET consists of vehicles and access points along the road. Vehicles move on the roads sharing information between themselves and with the Internet through the access points. Vehicles often move at high speed but their mobility is rather regular and Predictable. High speed movement creates scenarios characterized by a very dynamic network topology. Vehicles can always rely on recharging batteries. An accurate estimate of vehicles position can be made available through GPS systems or on-board sensors. VANETs are used for short range high-speed communication among nearby vehicles, and between vehicles and roadside infrastructure units.

Vehicle-to-Vehicle (V2V) communication supports services such as car collision avoidance and road safety by exchanging warning messages across vehicles. Here, an integrationof VANET and 3G networks using mobile gateways (i.e., vehicles) is introduced. The envisioned architecture shall enable mobile data access for vehicles, anytime and anywhere. In particular, the integration of IEEE 802.11-based multi-hop VANETs with 3G shall contribute to the evolution of Beyond 3G (B3G) wireless communication systems. As an integral part of the architecture, UMTS enables mobile data access to vehicles, offering a wide range of communication of around 8 to 10 km per BST. The UMTS takes a phased approach towards an all-IP network by extending 2G GSM/GPRS networks with international roaming capabilities and using Wide-band Code Division Multiple Access (WCDMA) technology. The set of enhancements to the UMTS, introduced in the 3GPP Release 8, defines the Long Term Evolution (LTE), which is the last step towards the 4G communication systems.

VANET is a special class of MANET to provide communication among nearby vehicles and between vehicles and nearby roadside equipment's. It is based upon short range wireless communication between vehicles. In these networks, each vehicle is equipped with communication equipment's, computing devices and GPS (Global Positioning Systems) receivers. GPS receiver provides all the information of a vehicle like speed, direction of movement of vehicle, time, location etc. Each vehicle stores the information about itself and other vehicles in a local database. The records of this database are periodically broadcasted to other vehicles and road side equipment's.

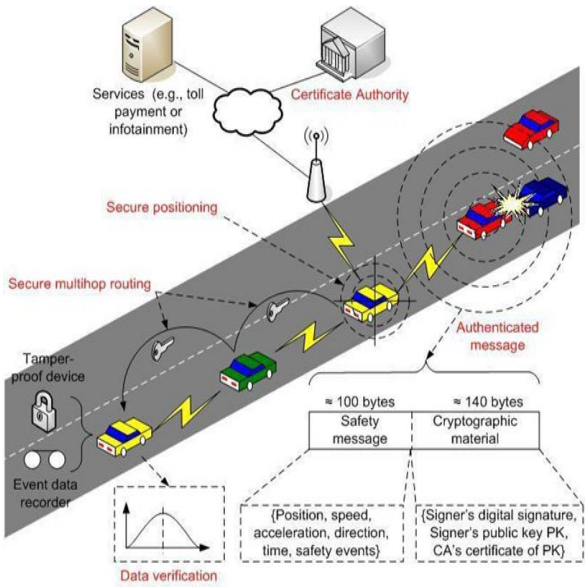


Figure 1.2 VANET Application Architecture

CHARACTERISTICS OF VANET

- High mobility nodes
- Predictable topology (using digital map)
- Critical latency requirements
- Slow migration rate
- No problem with power
- Security and privacy

1.4 WORKING OF VEHICULAR NETWORKS

Vehicular Networks System consists of large number of nodes (for vehicles).Here, each vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz), within 1 KM range area. The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely, there is no any wires required, the routers used is called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. Typically, in a VANET each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) that are installed along the roads. A trusted authority (TA) and application servers are installed in the back end. The onboard unit and road-side units communicate with each other by using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (Internet).

In Vehicular Networks System each vehicle has OBU (on board unit), that is connected to the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device). Tamper Proof Device (TPD) holds the vehicle secrets, that is all the information about the vehicle like keys, drivers identity, trip details of that vehicle, speed of the vehicle, rout etc.

1.5 ATTACKS

VANET facing many attacks, some of these attacks are as follows.

1.5.1 Denial of Service Attack (DoS)

Denial of Service attack happens when the hacker or attacker takes control of a all thevehicle's resources or maybe he jams the communication channel that are using by the VehicularNetwork, thus it prevents critical information from arriving.

1.5.2 Message Suppression

In this type of attack, an attacker selectively dropping packets from the network, these packets may hold critical information for the receiver. The attacker suppresses these packets and he can use that packet again in other time. For example, an attacker may suppress a congestion warning, and use it in another time, so vehicles will not receive the correct warning and it forced to wait in the traffic.

1.5.3 Alteration Attack

In this type of attack, an attacker simply alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted. For example, an attacker can alter a message telling other vehicles that the current road is highly congested even if the road is clear.

1.5.4 Sybil Attack

Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle with On Board Unit (OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity.

1.6 SECURITY REQUIREMENT FOR VANET

Security is an important issue for ad hoc networks, especially for security sensitive applications. To secure an ad hoc network, need to consider the

following attributes as criteria to measure security such as availability, confidentiality, integrity, authentication and non-repudiation

1.6.1 Availability

Availability is a very important factor for VANET. It guarantees that the network is functional, and useful information is available at any functioning time. Several attacks are in this category, one of the most famous attacks is Denial of Service attacks (DoS). The availability deals with network services for all nodes comprises of bandwidth and connectivity. Group signature scheme has been introduced in order to encounter the availability issues. The scheme is focusing on availability of exchanging the messages between vehicles and RSUs. When the attack causes network unavailability, the proposed technique still survives due to interconnection using public and private keys between RSUs and vehicles.

1.6.2 Confidentiality

Confidentiality is an important security requirement for VANETs communications; it ensures that data are only read by authorized parties. Confidentiality ensures that classified and important information in the network can never disclosed to unauthorized person. It also prevents unauthorized access to confidential information such as name of the driver, plate number and location of the vehicle. The most popular technique that are used to preserved privacy in vehicular networks is pseudonyms. Each vehicle node will have multiple key pairs with encryption. Messages are encrypted or signed using different pseudo and these pseudo has not linked to the vehicle node but relevant authority has access to it. Vehicle need to obtain new pseudo from RSUs before the earlier pseudo expires.

1.6.3 Authentication

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the attacker can be reduced easily with greater extent. In VANET, authentication is the verification of the identity between vehicles and RSU and the validation of integrity of the information exchange. Additionally, it ensures that all vehicles are the right vehicle to communicate within network. Public or private keys with CA are proposed to establish connection between vehicles, RSU and AS. On the other hand, password is used to access to the RSU and AS as authentication method. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be.

1.6.4 Integrity

Data integrity is the assurance that the data received by nodes, RSU and AS is the same as what has been originally generated during the exchanges of the message. In order to protect the integrity of the message, digital signature which is integrated with password access are

CONCLUSION

A secure and attack-free environment is a prerequisite in VANET for trusted message dissemination among vehicles and infrastructure. However, as various contexts are involved in VANET, ensuring trusted environment in every context is an extremely challenging task as the attackers penetrate the network and pollute it with bogus information. Therefore, the TMs should be validated in different context of VANET, and there should be a way to compare different proposed TMs. In this paper, we presented a novel framework which can validate and evaluate the efficiency of TMs in VANET. Various attacker models are identified using threat model and risk assessment which are integrated in our framework. These attacker models can be used to evaluate TMs in presence of the malicious nodes. In order to demonstrate our framework, we implemented three different TMs, i.e., entity-oriented, data-oriented and hybrid trust model.

We conducted an extensive set of simulations to study the behavior of TMs under different contexts and attacker models. TEAM revealed an interesting result which changes the general perception that hybrid trust models perform better in VANET due to their imperative nature of evaluating trust on both vehicle and data. However, according to our framework, entity-oriented TM outperforms both data-oriented and hybrid TMs. This is due to the presence of highly trusted and experienced vehicles in the network ensuring the dissemination of trusted messages.

SCOPE FOR FUTURE WORK

For enhancing the security in VANETs, which are vulnerable to attacks, robust learning methods against these attacks are required. The current VANET is not scalable, especially for large cities. It is feasible only for small environment.

BOOKS AND JOURNALS

[1] E. C. Eze, S. Zhang, E. Liu, and J. C. Eze, "Advances in Vehicular Adhoc Networks (VANETs): Challenges and Road-map for Future Development," International Journal of Automation and Computing, 2016.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," IEEE Communications Surveys Tutorials, vol. 13, no. 4, pp. 584–616, 2011.

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security Surveys," Computer Communications, vol. 44, no. Supplement C, pp. 1 – 13, 2014.

[4] J. Liu, J. Wan, Q. Wang, B. Zeng, and S. Fang, "A Time-recordable Crosslayer Communication Protocol for the Positioning of Vehicular CyberPhysical Systems," Future Generation Computer Systems, vol. 56, pp. 438 – 448, 2016, doi: https://doi.org/10.1016/j.future.2015.08.014.

[5] A. M. Vegni, M. Biagi, and R. Cusani, "Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks," in Vehicular Technologies - Deployment and Applications, L. G. Giordano and L. Reggiani, Eds. InTech, 2013, ch. 01. [Online]. Available: http://dx.doi.org/10.5772/55492

[6] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things Based Smart Cities: Recent Advances and Challenges," IEEE Communications Magazine, vol. 55, no. 9, pp. 16–24, 2017, doi: 10.1109/MCOM.2017.1600514.

[7] G. S. Khekare and A. V. Sakhare, "A Smart City Framework for Intelligent Traffic System Using VANET," in International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing. IEEE, March 2013, pp. 302–305.

[8] M. Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)," in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), December 2012, pp. 1–9.

[9] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. l. bin Ab Manan, "Classes of Attacks in VANET," in Saudi International Electronics, Communications and Photonics Conference (SIECPC), April 2011, pp. 1–5.

[10] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular Cloud Networks: Architecture, Applications and Security Issues," in IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), Dec 2015, pp. 571–576.

[11] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security Attacks and Solutions for Vehicular Ad Hoc Networks," IET Communications, vol. 4, no. 7, pp. 894–903, April 2010.

[12] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A Survey on Position-based Routing for