THESIS PROGRESS REPORT (2nd year)

PhD student: Hadi JIBBAWI

Thesis Title: Integrating Big Data Technologies for Securing Data Collected in VANET

Type de thèse : Codirection at the Université de Haute-Alsace in collaboration with the Lebanese University (LU) in Lebanon

Directeurs et encadrants de thèse : Prof. Abdelhafid ABOUAISSA (UHA, director), Dr. Hassan HARB (LU, supervisor), Dr. Ali JABER (LU, supervisor).

Year of Registration : 2nd Year

Beginning of the thesis : December 2020

Planned Defense Date : December 2023

Keywords: VANET ; Security ; Network Attacks, Cryptography, Blockchain, Privacy-Preserving Authentication

Introduction

In today's digital world, intelligent transportation system (ITS) plays a very important role in making the life of the citizens easy in every facet. ITS aims to achieve higher traffic efficiency by minimizing traffic problems and controlling unpleasant events. The ITS offers pervasive and robust services in terms of providing road and traffic safeties, reducing traffic congestion and improving traffic flow, and providing entertainment services on the vehicles, etc. Recently, the integration of smart sensing devices into the vehicles has led to a revolution in the transportation and traffic systems. As a result, we witnessed the generation of a new type of networks called as Vehicular Ad Hoc Networks (VANET). Basically, VANET is a special type mobile networks (MONET) with road routes, which depends on registration mechanism, roadside units (RSUs), and onboard units (OBUs). The OBUs are the radios that are installed in every vehicle as a transmitter to communicate with each vehicle, while RSUs are installed along the street with network devices. RSUs are used to communicate with the infrastructure and contain the network devices for dedicated short-range communication (DSRC). VANETs are classified into two categories: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. The main responsibility of VANETs is to produce effective communication; basically, the nodes require specific features to acquire information, to communicate with the neighbors, and then to take decisions based on all information collected by using sensors, cameras, global positioning system (GPS) receivers, and omnidirectional antennas.

Problem

Despite of its advantages, VANET is subjected to numerous risks :

1) **System Performance :**

The salient features of VANET (e.g., varying node density, high mobility) makes it challenging to coordinate VANETs to efficiently provide services with diverse Quality of Service (QoS) requirements. Indeed, the data collected in VANET are characterized by its massive size, high speed generation, and diversity (numerical, images, and videos). Unfortunately, such characteristics provide several challenges for data analysts and decision makers; first, the traditional data warehousing systems cannot store such amount of big data streaming. Second, data processing is another challenge in transport systems due to the huge computation power needed to handle such amount of data. Third, data analysis is a very complicated task because much of the generated data is of no interest, meaningless and redundant. Hence, the system architecture is becoming key enablers for VANETS to support inter-operation among underlying heterogeneous networks, conduct resource allocation tasks, and effectively manage a vast number of mobile nodes (or users) with heterogeneous smart devices. Recently, the Big Data technologies have been proposed as efficient solutions to overcome the Big data challenges in VANET. Subsequently, the rise of Big data technologies like Hadoop ecosystems allows to build systems based on clusters that use parallel computing. This can ensure a high scalability and reliability of the collected data as well as a fast and huge data storage. In addition, the parallel computing ensures a rapid data processing especially when the volume of data becomes bigger.

2) **Secure data collection and transmission:**

One of the most important challenges in VANET is security. Indeed, VANET has several weaknesses against major security attacks that violates security services such as availability, confidentiality, authentication, and data integrity. Therefore, there are several kinds of attacks that threaten VANET systems including the DDoS, forgery, jamming, impersonation, malware injection, sinkhole, sybil, and replay attacks. Hence, the VANET systems must ensure that the data are collected in a secure manner, thus none of malicious sources/events are happened. Furthermore, security during transmission means that no one should be able to read or change data during along the path to the end user. Therefore, introducing new security and data encryption methods should take a great attention from researchers when dealing with data collected in VANET. Recently, with the emergence of blockchain technology, VANET has tackle a new trend in securing the data and ensuring a high level of confidentiality for the transmitted data. The blockchain technology has led to a revolution in VANET security by providing a distributed security solutions, i.e. the case of mobile vehicles communication, rather than a centrally controlled solution. Thus, with blockchain, there will be no need for a central administrator but all the vehicles are in control of all their information and transactions. Furthermore, since VANET deals with confidential mobile information and requires quick access to information, blockchain can streamline these communicated records and enable their sharing in a secure way.

Summary of work conducted this year :

The focus of our work this year was on exploring the VANET domain with its challenges, mainly on the security challenges. Then we studied the bibliography of VANET ‘s security solutions incollaboration with the blockchain technology.

Part of this year was studying the blockchain technology in order to investigate the existing VANET-Blockchain solutions.

A security and performance comparison between the major existing solutions was summarized in a table. According to this table we have a clear view on what solution should be proposed to hold such security challenge in VANET.

- **Study of VANET domain :**

  As a part of Intelligent Transportation System, VANET is characterized by its high mobility, dynamic network topology, time criticality, storage and processing essentiality, etc.

  VANET's basic architecture is composed of: Trust Authority (TA), Roadside Unit (RSU) and Vehicles (On Boarded Unit – OBU).

  VANET faces several challenges such as Network Management, Environmental Impacts, Real-time processing of data, and security challenges.

- **VANET Security:** VANET faces several security attacks and illegal access due to its nature and characteristics. We can summarize the security study in VANET by the following:
  1. **Categories:** Security can be categorized into 3 main categories:
     - Network Management and trust
     - Data protection (generated and exchanged messages, privacy preservation)
     - Balance between security solution and performance of the network
  2. **Services:** Any security solution should guarantee the presence of Confidentiality, Data Integrity, Availability, Authentication and Privacy.
  3. **Some attacks and threats:** Denial of Service, Identity Spoofing, Spamming Attack, Sybil Attack.

- **Summary of Existing VANET-Blockchain solutions:**

	Performance			**Security**		
	Computational Cost	**Communicational Cost**	**Packet Delivery Rate**	**Authentication**	**Message Security**	**Privacy Preservation**
BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs	0.49 ms for anonymous authentication of 100 user	2048 bits (authentication phase)		PKI and CA based authentication	Blockchain security	Real identities stored in TA
Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET	0.49 ms		Enhance 2.4 % from existing solutions	Leightweight authentication based on smart cards	Blockchain security	Public key and digital signature based communication

A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET	0.1 ms		0.99	PKI based authenitcation plus vehicle registration in mobile vehicle driver and TA	protected by hash function, signature and match functions	Real identity is not revealed in communicatio n
Blockchain-Based Pseudonym Management Scheme for Vehicular Communicatio n	Reduce authentication delay	Increased message exchange Not efficient for high laods		Lightweight absed authentication	Blockchain security	Real identity is not revealed in communicatio n
A Secured Message Transmission Protocol for Vehicular Ad Hoc Networks		Max throughput 12Mbps Safety messages sent through internet Whole network is for non-safety messages		PKI and CA based authentication	Messges encrypted by RSA-1024 cryptographi c algorithm. Blockchain security	real identity is stored only in the CA and not used in communicatio n
DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts	time for SHA-256 is less than 0.01ms per 1 KB of input storage overhead for one blockchain is 1602 MB/year			PKI and CA based authentication	Blockchain security	Real identity is not revealed in communicatio n

References

- Arif, Muhammad and Wang, Guojun and Bhuiyan, Md Zakirul Alam and Wang, Tian and Chen, Jianer. **"A survey on security attacks in VANETs: Communication, applications and challenges"**. Vehicular Communications, 19, pp. 100179, 2019.

- Sheikh, Muhammad Sameer and Liang, Jun. **"A comprehensive survey on VANET security services in traffic management system"**. Wireless Communications and Mobile Computing, 2019.

- Sheikh, Muhammad Sameer and Liang, Jun and Wang, Wensong. **"A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)"**. Sensors, 19, pp. 3589, 2019.

- Jaballah, Wafa Ben and Conti, Mauro and Lal, Chhagan. **"A survey on software-defined VANETs: benefits, challenges, and future directions"**. arXiv preprint arXiv:1904.04577, 2019.

- Manivannan, Dakshnamoorthy and Moni, Shafika Showkat and Zeadally, Sherali. **"Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)"**.

Vehicular Communications, 25, pp. 100247, 2020.

- Zhang, Xiaohong and Chen, Xiaofeng. **"Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network"**. IEEE Access, 7, pp. 58241--58254, 2019.

- Adhikary, Kaushik and Bhushan, Shashi and Kumar, Sunil and Dutta, Kamlesh. **"Hybrid Algorithm to Detect DDoS Attacks in VANETs"**. Wireless Personal Communications, pp. 1--22, 2020.

- Schmidt, David A and Khan, Mohammad S and Bennett, Brian T. **"Spline Based Intrusion Detection in Vehicular Ad Hoc Networks (VANET)"**. 2019 SoutheastCon, pp. 1--5, 2019.

- Baza, Mohamed and Nabil, Mahmoud and Mahmoud, Mohamed Mohamed Elsalih Abdelsalam and Bewermeier, Niclas and Fidan, Kemal and Alasmary, Waleed and Abdallah, Mohamed. **"Detecting sybil attacks using proofs of work and location in vanets"**. IEEE Transactions on Dependable and Secure Computing, 2020.

- Bhatia, Jitendra and Kakadia, Parth and Bhavsar, Madhuri and Tanwar, Sudeep. "SDN-enabled Network Coding Based Secure Data Dissemination in VANET Environment". IEEE Internet of Things Journal, 2019.

- Singh, Pranav Kumar and Gupta, Shivam and Vashistha, Ritveeka and Nandi, Sunit Kumar and Nandi, Sukumar. **"Machine learning based approach to detect position falsification attack in vanets"**. International Conference on Security \& Privacy, pp. 166--178, 2019.

- Khan, Uzma and Agrawal, Shikha and Silakari, Sanjay. **"Detection of malicious nodes (DMN) in vehicular ad-hoc networks"**. Procedia computer science, 46, pp. 965--972, 2015.

- Thigale, Somnath B and Pandey, Rahul K and Gadekar, Prakash R and Dhotre, Virendrakumar A and Junnarkar, Aparna A. **"Lightweight novel trust based framework for IoT enabled wireless network communications"**. Periodicals of Engineering and Natural Sciences, 7, pp. 1126--1137, 2019.

- Bhatia, Jitendra and Dave, Ridham and Bhayani, Heta and Tanwar, Sudeep and Nayyar, Anand. **"Sdn-based real-time urban traffic analysis in vanet environment"**. Computer Communications, 149, pp. 162--175, 2020.

- Akhter, A. F.M.Suaib and Shah, A. F.M.Shahen and Ahmed, Mohiuddin and Moustafa, Nour and Cavuoglu, Unal and Zengin, Ahmet. **"A Secured Message Transmission Protocol for Vehicular Ad Hoc Networks"**. Computers, Materials and Continua,68, pp.229-246, 2021.

- Talib, M. N. and Ravi, Nikhil and Verma, Sahil and Kavita Jhanjhi, N.Z. "**Securing VANET Using Blockchain Technology"**. 2021

Abdelhafid Abouaissa
Professeur des universités à l'UHA
Responsable de la LP Administration
des Réseaux Multimédia (ARM)
Email : abdelhafid.abouaissa@uha.fr
Téléphone : +33 (0)3 89 20 23 71

Hassan Harb
Maitre de conférences à
l'Université Libanaise
Email : hassan.harb.1@ul.edu.lb
Téléphone : 03399252