ISSN 2319 - 5975

Volume 8, No.3, April - May 2019
International Journal of Networks and Systems
Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns02832019.pdf
https://doi.org/10.30534/ijns/2019/02832019

A SECURE DATA MANAGEMENT SCHEME FOR INTERNET OF VEHICLES

Parvathy R Nair[1], Divya Sunny[2]
[1]APJ Abdul Kalam Technological University, India, parvathy0702@gmail.com
[2]APJ Abdul Kalam Technological University, India, divyasunny@gmail.com

ABSTRACT

Internet of Vehicles(IoV) is a self-configuring network connecting vehicles in-order to achieve unified management. It helps in monitoring vehicles and provide communication among them. IoV offers several benefits such as travel comfort, safe driving, road optimization, traffic analysis etc. The number of vehicles are increasing day by day, so the network is growing very fast. The dynamic topology of the network add complexity to it. Authentication of vehicle nodes should be provided. Another security requirement is the privacy of the data in this network, the network should be trustworthy. Since it is an open network, attacks such as data falsification, Man in the Middle attack, replay attack etc may occurs. So efficient encryption techniques are needed to ensure privacy. Since we are living in an internet era, the data in this network become large in terms of size and dimension, hence scalability of this IoV is a big question. The existing IoT protocols fails to provide scalability for storing this Big data in large scale IoV. So a reliable and secure mechanism for Big data collection, processing and storing in Internet of Vehicles is to be developed.

Key words : Internet of Vehicles(IoV), Big Data.

1. INTRODUCTION

Internet of vehicles(IoV) is a network connecting vehicles over internet which helps in achieving efficient communication among them. The basic concept of loT in traffic management has been widely accepted and is being put to use in the construction on smart cities' infrastructures , so IoV can offer several advantages. IoV is said to be a superset of VANET(Vehicular Adhoc Network). The main features of IoV are its dynamic topology, huge network scale, non-uniform distribution of nodes, complex granularities and mobile limitation. Internet of Vehicles is a network which is growing day by day . The number of vehicles are growing very fastly. So the need for an efficient connection mechanism arrives. The different communications in this network are:

1. Communication between the vehicles and the vehicle owners.
2. Communication between different vehicles.
3. Communication between vehicles and data center.
4. Communication between server and third parties like police, ambulance etc.

The importance of big data is that the vehicular network is a huge one, the network is fastly growing and the data uploaded in this internet era is very high. With the spread and development of IoV, the collected contents involve not only personal, but also some important data including vehicle running parameter which is closely related to traffic safety. However, the fraudulent messages may be sent by malicious vehicle nodes to attack the traffic system or purse their own profit. Hence, it is significant to design a mechanism to ensure that the transmission of vehicle data resource is trusted and not tampered with. As the intelligent transportation system is continuously developing and big data applied in the IoV , big data collection between vehicle and application platform becomes more and more frequent through various communication technologies, which causes evolving security attack. How to secure the big data collection in large scale IoV is meaningful and deserves researching.

2. LITERATURE REVIEW

Use IoV[1] is an extension of IoT(Internet of things) to vehicular network. The main features of IoV are its dynamic topology, huge network size, nodes joins and leaves very fastly, non uniform distribution of nodes, mobile limitation etc. The advantage of IoV are road optimization, traffic management, theft avoidance, pollution checking etc. The diffrent communications involved in IoV are Vehicle to vehicle, Vehicle to vehicle owner, Vehicle to server, Server and third parties. The applications of IoV includes Early warning system, Detour application, Analysis to authority etc.The major disadvantage of this technology are security in wireless communication and failure of nodes.Since the data involved in the network include personal data like vehicle id, preserving this data is important. The node(vehicles) are highly mobile and they joins and leaves the network very fastly, also the distribution is not based on any topology so chances for node failures are very high. Figure 1shows IoV architecture

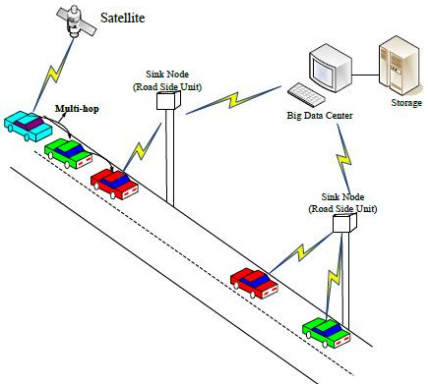

Figure 1:: IoV architecture

Internet of Vehicles(IoV) includes two types of data. They are sensory data and confidential data. Confidential data is the private data, which is needed to be protected. Sensory data is obtained using sensors. The different sensors used are Pieso sensor, Breath analyzer, Speed sensor, temperature sensor, humid sensor, tyre pressure sensor, GPS etc. GPSis used to track vehicle using its location. Pieso sensor is used to measure change in pressure and breath analyser estimate blood alcohol content. Speed sensor is used to detect speed of object by counting the wheel rotations. The control system used is Raspberry pi[2]. It is having high processing capacity and a memory capacity upto 1 GB. It uses Broadcom BCM 2836 processor. Data logging is an electronic device used to record data over time or in relation to location with help of sensor. They are battery powered equipment with internal memory and microprocessor. It is used to record atmospheric condition.Telegram application is a free cloud based service for messaging. Users can exchange different messages using end to end encryption.

Internet of Vehicles is a complex system involving different types of resources like vehicle, human etc. So chances of security attacks are also high. Security should ensure safety of vehicle as well as privacy protection of people. Some informations involve in IoV are public, at the same time some are private. The major security attacks[3] in IoV are Attacks on authentication, Availability attacks, Secrecy attacks, Routing attacks ,Data authenticity attacks. Authentication attacks are attacks like sybil attack in which a single node act with multiple id's and harm entire system. In GPS deception node with fake location information, speed etc damage the network. In masquerading an attacker send wrong informations to network etc. Availability attacks are attacks like denial of service, channel interfence etc. Secrecy attack includes stealing of data by interception. Routing attacks includes creating loops hole like grey hole, worm hole, black hole etc and routing path is mislead. Data Authenticity attacks are replay attacks that is modification of data. The major security requirements are Authentication, Integrity, Confidentiality, Non-repudiation, Authorization.

Counter Measures for above mentioned attacks are:
1. Threat model- known as attack modeling. They provide graphical representation to describe the relationships between different vehicles which help people to determine the behaviour of attack easily. Static asa well as dynamic graph based techniques are vwey well known threat models.

2. Intrusion detection system- Intrusion detection system (IDS) is an important counter measure to network security. Intrusion detection system provide protections against both internal and external attacks by collecting information from internal network systems.

3. Honey pot- Honeypots aim to divert attackers attention away from the system resources. Authorization and communication modules are the more attacked parts. Honey pot helps in absorbing the damage and records all the attack data.

4. Secure routing protocol- Inorder to protect our network from routing attacks, one solution is to use secure and efficient routing protocols like DCFM(Denial Contradictions with Fictitious Node Mechanism).

5. Key management- The goal of key management is to ensure the security of the key, that is authenticity and validity. Key management includes key generation, distribution, transmission, preservation, destruct and backup.

Large scale IoV generates large amount of data which can be called as big data. Big data[4] includes two types of data. The onboard data and onroad data. The onboard data deals with sensory data and on road data includes informations like inter vehicle data, blind points, traffic light, road map etc. The different sensors used are GPS, gyroscope etc. Big Data Collection includes collection of the data. A DSRC(Dedicated Short Range Communication) channel is used to collect data securely from vehicle nodes. DSRC channel consist of one control channel and more than one service channels which provide optimal bandwidth. Big Data Transmission aims at providing road safety and travel comfort. Every vehicle in the network needs to update their status informations like vehicle position, velocity, acceleration etc. Travel comfort parameters like traffic signal, nearby parking slot etc are transmitted using broadcast technique like plain flooding. In plain flooding every incoming packet is transmitted through every outgoing packet.

Big Data Storage is another major factor. Mainly there are three types of storage. They are Onboard storage, Roadside storage, Internet storage. Onboard units in vehicles are provided rich extensible storage. The road side units are

installed with onboard storage. Internet storage are storage through internet like cloud services which provide vast storage facility.Big data computing is done by computing devices which mainly focus on sensor data processing. The sensory data will provide road safety application while GPS data provide navigation. Apart from that HD map provides ease for self driving, multimedia contents provide infotainment, traffic data help in path planning etc.

The different IoT protocols[5] for data collection are Message Queue Telementry Transport(MQTT), Extensible Message and Presence Protocol(XMPP), Constrained Application Program(CoAP). The comparison between the three protocols are given below. The major disadvantage of the existing system is the scalability problem. Since IoV is a huge network, the data belonging to the network will be large. Inorder to handle massive data in IoV an MQTT broker is introduced. MQTT PROTOCOL: MQTT is an open source protocol for connected devices and low bandwidth, high latency networks. It is a publish/subscribe messaging transport that consumes only less power. The sensor layer connects diffrent IoT decices. They publish data to MQTT broker. Then the service layer works based on an MQTT broker. MQTT broker provides interaction among agents. It is the heart of this communication. A broker can handle upto thousand of clients. MQTT broker requires username and password for authentication. The final layer is Application client layer,which consist of client and application. They subscribe the data published by diffrent sensors to MQTT protocol.

Privacy protection is one of the major factor for a secure communication network. The identity of the vehicle should be preserved using efficient mechanism. Use of pseudonym keys[6] is one method for protecting vehicle identity. Initially nodes should be registered to the network. Each non overlapping cell contains a server. The server is responsible for managing the pseudonyms. Server maintains a set of pseudonyms for the particular cell . A capacity planning scheme is used for managing pseudonym. It allows the server to predict the probability of required pseudonyms and based on the prediction pseudonyms are generated.

HLAR PROTOCOL: Hybrid location-based adhoc routing (HLAR) protocol is a combination of AODV(Ad hoc On-Demand Distance Vector Routing) protocol and greedy forwarding geographic routing protocol. It is used for calculating the routing path. Each node in HLAR protocol have two tables.

1) A neighbor table, used to perform geographic routing.

2) An ETX table, which is used to construct the AODV route(the AODV routing table) upon request to obtain good scalability performance.

DIFFIE HELLMAN KEY EXCHANGE: The Diffie Hellman Key Exchange Scheme publishes a shared secret key to unknown vehicles nodes over an insecure communication channel. It improves protection of privacy in wireless networks especially the passive attacks. Here the sender and receiver are unknowns. So Diffie Hellman Key Exchange is an efficient method to provide communication among anonymous users.

Malicious nodes in vehicular network may mislead the communications and creates attacks. Data falsification attack[7] is one of the security attack in which data is attacked and modified by other nodes. The information dissemination in IoV must occur quickly and ensure security. As a solution for Data falsification attack hashing method is used. Hashing of data helps in preventing tampering of data.

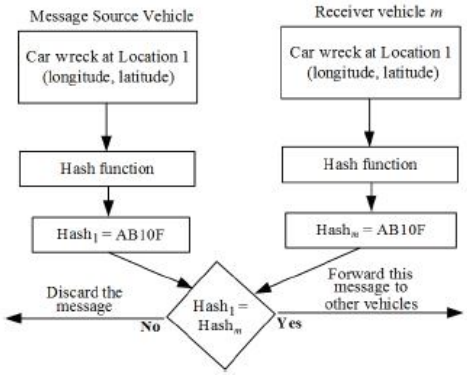

Figure 2: Detection of data falsification

Figure 2 shows Detection of data falsification. The source vehicle and receiver vehicle are in different locations. When the source vehicle send data, using a hash function the hash value is also computed and send along with the data. The receiver vehicle while receives the data computes the hash value locally using some other hash function. Then the both hash values are compared. If the hash value are same then the message is forwarded to other vehicles, else if the hash values are not same then the message is discarded. Thus vehicular communication can be protected from data falsification attack.

Data Confidentiality and Users Location Privacy[8] are the two major attributes to be protected in a vehicular network. This scheme consist of three steps. They are Creating the VANET environment, Route discovery, Vehicular communication using RSU Creating the VANET environment: The VANET environment consist of vehicle nodes, RSU(Road Side Unit) and a TA(Trusted Authority). Route discovery: Using a routing protocols the routing path is discovered.Here the source vehicle will generate RREQ and find the neighbours. Vehicular communication using RSU: All the users in the network should register their details into the RSU. After completing registration the RSU provides an

initial packet key to each user and using this initial packet key, the user can get data about the other nearby vehicles from the TA. Two Algorithms are designed, each For participating of a vehicle node in a session and to switch connection between different RSU while nodes are mobile.

The exponential growth of data with the increase in number of vehicles result in the need for a scalable technology for processing and storing data. Data is generated very fast and also need to be processed fast.The traditional databases fails to process large volume of data. Hadoop is a big data technology that provides scalability. Hadoop[9] provide reliable and distributional storage through Hadoop Distributed File System (HDFS) and distributed computing through Map Reduce. A HDFS cluster consist of two types of node. They are NameNode (the master) and DataNodes (workers). File system namespace is managed by the NameNode. Namenode contains location information about the datanodes. When HDFS receives a file it cuts the file into diffrentblocks. Each block is stored in different datanodes. The replicas of every block is stored in some other datanodes which helps in recovery from failure of datanodes. To read a file from HDFS, the client need to contact the NameNode and obtains the information. MapReduce is a linearly scalable programming model which process massive data in parallel by using idle resources. Thus reduces the time for processing. MapReduce works mainly using two functions,the Map function and the Reduce function. Map function takes a set of input and map it into key/value pairs. The reduce function then reduce the output of map function into unique key/value set. Map Reduce provides ease-of-use, scalability, and failover properties.

Big Data Analytics Architecture[10] consist of three layers namely Infrastructure layer, Processing layer, Application Layer. The Infrastructure layer consist of Multi-sensor Information Fusion Gateway and road side sensors. Multi-sensor Information Fusion Gateway function as GUI between human and machine, it is used for acquiring signals from diffrent sensors and input output monitoring. Roadside sensor nodes include cameras to monitor traffic, humid sensor, speed sensor, temp sensor, distance sensor, audio sensor, magnetometers etc. They obtain data from the road like road conditions, inter vehicle sistance, atmospheric conditions. The Processing layer provides preprocessing funtionality and reduces the query pressure. Application Layer Store the analysis result to cloud sevices. Spark integrated solution helps in providing scalability for big data processing. It contains three layers and they are batch layer, speed layer and serving layer. Batch layer combines HDFS with Spark core. HDFS is for storing big data and spark core produces the batch view of the data. The speed layer performs Spark Streaming and Real time data processing. Serving layer stores output view of batch layer and speed layer and it merges batch view with the real time processing view.

Data collection mechanisms should be secure enough to handle privacy data. The increase in number of vehicle nodes consumes and produces large amount of data. These data are collected by the big data center by using secure mechanisms and stores in distributed storage system with help of Hadoop architecture.The initialization phase[11] consist of registration of vehicles into the network for ensuring authentication,and protect from malicious nodes. After registration vehicle nodes want to login into the sink node using single sign on algorithm. The data collection model is represented in figure. Data collection is done by using hash message authentication code. Two types of data are included in this network namely confidential data and business data. Business data are data obtained from sensor nodes and need no encryption. But confidential data include data like vehicle identity . This type of data should be protected. The Hadoop architecture consist of namenode and data nodes. The namenode is also known as master node. It contains meta data, that is the informations about the different data nodes and their locations. The hdfs firstly cut the files into different blocks and store their replicas in different nodes in order to overcome datanode failure. The clients directly approach namenode and obtain informations about the locations of data and then approach datanode and acquire data. The major advantage provide by this mechanism is its scalability.

With the growth of data size in this Internet era, collection, storage, analysis, and processing of big data are becoming strong topics in research fields. Almost all big data processing[12] platforms uses the MapReduce programming model to perform big data processing. Initially Hadoop collects data using some data collection mechanisms and stores files in distributed storage systems. they are storage nodes situated in different clusters. Then, the compute nodes read data from the clusters and perform processing operations. The big data preprocessing consist of mainly four modules. They are Resource Monitoring Module, Task Distributing Module, Task Processing Module, Input Analysis Module. The Resource Monitoring Module monitors resource utilization informations like cpu usage, disk usage etc and maintains node list. Task Distributing Module distributes the task among different nodes and then maintain task list. Task Processing Module is the core of this system. It performs preprocess task and generate input files. The final module, Input Analysis Module process the preprocessed data file format

3. DISCUSSION

The various issues regarding each paper is shown in the above table. To provide security to the data secure encryption techniques are to be used. Table 1 shows Issues and solutions of each paper.

Table 1: Issues and solutions of each paper

No	Name of paper	Issues	Solutions
1	Internet of Vehicles(IoV) forTraffic Management.	Security issues. Failure of network.	-
2	Internet of Vehicles(IoV): Implementation details.	Privacy. Security.	-
3	Security and Privacy in the Internet of Vehicles.	Attackon authentication. Availability attack. Secrecy attack.	Threat models. Intrusion detection systems. Honey pot. Key management.
4	Internet of Vehicles in Big Data era.	Data storing schemes. Reliable protocol to carry data from source to destination.	Cloud storage.
5	IoT Protocols for Data Collection.	Poor scalability. Traffic in network.	MQTT Broker.
6	Privacy Protection against Man In The Middle Attacks in VANET.	Man in the middle attack.	Capacity planning scheme.
7	On the Security of Information Dissemination in the IoV.	Data Falsification attack.	Hashing.
8	Data Confidentiality and Users Location Privacy in VANETs	Security of data.	An algorithm for vehicular communication.
9	Use of Big Data Technology in Vehicular Ad-hoc Networks.	Large volume of data. Latency	HDFS. Map Reduce.
10	Big Data Analytics Architecture for Internet of Vehicles.	Scalability.	Spark integrated solution.
11	A Secure Mechanism For Big Data Collection in Large Scale IoV.	Storage.	Hadoop.
12	Research and Implementation of Big Data Preprocessing System Based on Hadoop.	Data size in internet era. Data transmission rate. Latency.	Big data preprocessing using Hadoop.

4. CONCLUSION

IoV(Internet of Vehicles) helps in achieving unified management in vehicular communication. It have several more features like traffic management, road optimization, theift control etc. The major issues regarding this network is the security of the data and scalability of the storage system. The data included in this network contains sensory data, which is public and private data like vehicle id, driving routes etc. So the data should be protected by an efficient cryptographic system. Authentication of every vehicular node is another security requirement. Storing and processing should be secure and efficient enough to handle big data in size and dimension. So here some security techniques and mechanisms for providing scalable storage and processing in large scale internet of vehicles are discussed.

REFERENCES

1. Dhananjay Singh, Madhusudan Singh, **Internet of vehicles for smart and safe driving,** International Conference on Connected Vehicles and Expo (ICCVE), 07 April 2016.
2. Sakhil P George, Nivya Wilson, **Social Internet of Vehicles,** International Research Journal of Engineering and Technology(IRJET) Volume: 04 Issue: 04, Apr-2017.
3. Yunchuan Sun, LeiWuShizhong, **Security and Privacy in the Internet of Vehicles**, International Conference on Identification, Information, and Knowledge in the Internet of Things, 2015.
4. Qing Xu, Tony Mak, **Vehicle-to-Vehicle Safety Messaging in DSRC**, VANET '04 Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks Pages 19-28, 2004.
5. Ghyzlane Cherradi, **Smart Data Collection Based on IoT Protocols**, www.researchgate.net/publication/32086914, December 2016.

6. R.Jebima Ravi, **Privacy Protection against Man In The Middle Attacks in Vehicular Ad hoc Networks**, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, April 2014.
7. Danda B.Rawat, Moses Garuba, **On the Security of Information Dissemination in the Internet-of-Vehicles**, Tsinghua science and technology Volume 22, Number 4, August 2017. https://doi.org/10.23919/TST.2017.7986946
8. Saranya.G, Mrs. P. Nathiya Devi, **Data Confidentiality and Users Location Privacy in VANETs**, International Journal of Engineering Development and Research Volume 2, Issue 2 ISSN: 2321-9939,2014.
9. Punam Bedi, Vinita Jindal, **Use of Big Data Technology in Vehicular Ad-hoc Networks,** International Conference on Advances in Computing, Communications and Informatics (ICACCI),2014. https://doi.org/10.1109/ICACCI.2014.6968352
10. Liu Dan, **Big Data Analytics Architecture for Internet of Vehicles**, International Conference on Intelligent Transportation, Big Data Smart City, DOI 10.1109/ICITBS.2018.00011, 2018. https://doi.org/10.1109/ICITBS.2018.00011
11. Longhua Guo, Mianxiong Dong, **A Secure Mechanism for Big Data Collection in Large Scale Internet of Vehicle**, IEEE Internet of Things Journal,DOI 10.1109/JIOT, 2017.
12. Huadong Dai, Shu Zhang, **Research and Implementation of Big Data Preprocessing System Based on Hadoop**, IEEE International Conference on Big Data Analysis (ICBDA), 2016.