xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.2472-2480
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.278

Blockchain Secured Vehicle Tracking using Wireless Sensor Network

Mayank Mrinal, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India
AbhishiktaPanja,Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India
Aditya Garg,Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India
Vivek DuraiswamyMaikandavel,Research Assistant Professor, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai, India

Abstract-Vehicle Tracking Systems give an instantaneous location or travel history to form a comprehensive picture of visited locations, stopping points, vehicle speeds, acceleration, etc. We propose a Wireless Sensor Network (WSN) requiring low processing power, reduced need for internet connectivity only to Base-Stations (sink node of WSN), and eliminate the use of constant GPS tracking. Geotagged Roadside Units (nodes of WSN), at regular intervals, capture vehicle movement via RFID tags and update the movement of each vehicle into a decentralized Blockchain Network formed at the Base-Stations (BSs). This network forms a detailed distributed ledger providing the license plate numbers of every vehicle, the location coordinates of the Roadside Units (RSUs) passed, and the instantaneous time at which the vehicle passes it. Similarly, data for all vehicles that pass a certain node, in a given time interval, can be retrieved. An immutable private Blockchain network secures data, maintains uniform databases at all BSs, and protects the privacy of the commuters by allowing such data access only to authorized personnel. In case of the collapse of an RSU the data is transmitted via an alternate path to another BS until the fault is repaired. Our solution focuses on optimization and fault tolerance of nodes and the security of gathered data. We also focus on various applications where this architecture can be deployed efficiently.

Keywords: Wireless Sensor Network (WSN), Radio Frequency Identification (RFID), Blockchain, Decentralized Network, Vehicle Tracking

I INTRODUCTION

The most prevailing and widespread method for a Vehicle Tracking System is the Global Positioning System (GPS). It relies on at least four satellites, requires a constant reliable internet connection to form an accessible database, and consumes high power in battery-operated devices. GPS may give a range of inaccurate values. In case they get connected to only three satellites, obstacles like skyscrapers, walls, buildings, etc may have an influence on its output. Moreover, GPS can be easily misused to tamper with locations or to track someone without their knowledge and exploit such information. Another conventional method for vehicle tracking is camera modulesinstalled along the roads at regular intervals. They are employed for vehicular detection and can be used to keep a record of the vehicle velocities. Such image processing requires high computation power and maintenance. Harsh environmental conditions like heavy rain, dense fog, mist, dust, etc considerably reduce visibility, which influences the camera's performance. To overcome these drawbacks, we propose a vehicle tracking system that requires low processing power and higher accuracy at any given time. A Wireless Sensor Network is created with nodes that monitor vehicular movements with an RFID reader. Geotagged Roadside Units (nodes) are installed at frequent intervals keeping a check on almost all vehicular movements. Base-Stations act like sink nodes in this architecture and are responsible for constantly updating the blockchain with location of the vehicles. The license plate number of every passing vehicle, the location coordinates of the node and the time at which a vehicle passes a given node is sent to the nearest Base-Station. The data received at the Base-stations is written into a decentralized database as transactions and is precisely and meaningfully documented. Data can be retrieved as desired, per say, specific to a single location (all vehicles passing a Roadside Unit) or specific to a single vehicle (all RSU coordinates it has passed). This decentralized database can easily store the travel history of vehicles up to many years. Once this infrastructure of Roadside Units and Base-Stations is established very little maintenance is required. Buildings, walls, flyovers or other infrastructure do not pose an obstacle in this system. In case of failure of Roadside Units data is routed through an alternate path to the Base-Station. Moreover, in case of Base-Station malfunction no data is lost since we have a Decentralized Architecture.

II RELATED WORK

Reference [1] suggests a mathematical formulation of vehicle localization using received signal strength considering there is no transmission delay or packet loss. The anti-collision Aloha algorithm used for RFID tag has a very low efficiency [2]. It has a tedious installation, wherein every node has a wired connection to a computer to be connected to the Internet, for maintaining the database. Inaccuracy in conventional GPS methods can be brought about by verification of RFID positioning using radar and photoelectric switch [11]. To overcome such inaccuracies, RFID can be used as proposed in [10]. Its very limitation lies in usage of low frequency range leading to detection of vehicles only up to 2 meters. Reference [3] proposes a multi blockchain network. Data of different kind is gathered and updated in sub blockchain networks for different use cases. A complex mathematical model is used for detailed theoretical analysis and numerical results. Reference [6] suggests use of Blockchain in the server layer of LoRaWAN. LoraWan gateways are resource limited IoT devices which are not completely feasible for performing all blockchain operations. With the increase in Connected Vehicles as a Service (CVaaS) Reference [4] puts forward a secure and seamless service for online cab booking services by creating a vehicular network of autonomous vehicles. The information exchange between the cab driver and customer happens in a network of blockchains. A network of IoT devices contribute in maintenance and tracking of cabs. Reference [5] implements RFID technology to implement data acquisition,circulation and sharing in production, processing, warehousing, distribution and sales links of agri-food supply chain. This data is secured in a blockchain network to maintain a tamper proof database.

III PROPOSED MODEL

A. Methodology

1. Wireless Sensor Network (WSN):A Wireless Sensor Network is formed by numerous sensor nodes placed at different geographical areas that monitor physical or environmental conditions, in its respective ranges. These nodes communicate with each other via radio signals with multi-hop communication and route the gathered data to a Gateway or a Sink Node. This gateway is connected to an external network for observation and analysis by the user. A WSN can support hundreds or thousands of nodes. Each node has its own resources in terms of energy, memory, power components, computation, and communication capabilities.

2. Radio Frequency Identification (RFID):RFID is a wireless system with two components Reader and Tag. The Reader emits radio signals and captures radio signals emitted by the tag. Readers can have internal or external antennas as per the desired use case. Tags consist of a radio transponder, transmitter, and a radio receiver and communicate its unique identity to a nearby reader on the reception of an electromagnetic pulse from it. Tags can be classified as Active or Passive. Active tags have their own power source(batteries) while Passive tags draw power from the reader. The best suited RFID technology for vehicle tracking is Ultra High Frequency (UHF) RFID tags and receivers, which comes under the Far Field Communication category. RFID tag(s) installed on the vehicle can be passive UHF tags or Battery Assisted Passive (BAP) tags. Passive UHF RFID tags have a range easily upto 10 meters. BAP tags are bulkier than passive tags and have an embedded battery in them. These tags receive the signal from the reader's antenna and on backscattering, the transmitted signal from the tag is boosted by the battery of the tag. This increases the detection range of the tag significantly optimizing detection in harsh weather conditions. The battery of a BAP RFID tag can last over 5 years. After the battery is discharged a BAP RFID tag works as a normal passive tag so not much is lost.

3. External Antennas:The range of detection of the RFID tag also depends on the Gain and the Polarization of the Antenna. An antenna with a higher gain increases power received from the reader. Thus, a higher gain antenna (usually 9dB and higher) should be used for a longer range. The polarization of Antennas is classified as Linearly Polarized or Circularly Polarized Antenna. Linear polarization occurs when electromagnetic waves are broadcast on a single plane (either vertical or horizontal). These antennas must have a known RFID tag orientation which must be fixed upon the same plane as the antenna in order to get a consistent reading. Circular polarized antennas emit electromagnetic waves in a corkscrew pattern. They broadcast electromagnetic waves on two planesmaking one complete revolution in a single wavelength. Due to the concentrated emission, linear polarized antennas typically have a greater read range than circular polarized antennas of the same gain.

4. Blockchain*:* A blockchain is a digital, distributed ledger that is not controlled by a central authority; instead, it is distributed across various nodes on the network. It consists of a linked chain of records known as blocks which can be created by one or more transactions.

5. Structure of a Block:Each block consists of transaction data, the timestamp of when it is created, and the hash of the previous block. Each block has a reference to its previous block and thus tampering with any of the blocks will require change in all of the previous blocks and will be notified to all other nodes.
6.Decentralization and Consensus:For every new block to be added in the blockchain, a Consensus mechanism is used to validate it without the involvement of any intermediaries. A minimum of 51% of consensus is required for addition of a block in a blockchain. The ledger formed is shared with all nodes so that there is no data loss in case the state of a node is compromised.

7. Security and Encryption:The hash associated with each block is mined using powerful cryptography or complex mathematical puzzles requiring high computational power. Thus, it is almost impossible to decrypt hashes making the blocks immutable. The nodes in a blockchain have private keys which are subject to change in any suspicious circumstance and will be notified to the rest of the blocks.

8. Privacy:Blockchain can be Permissioned (Public) or Permissionless (Private or consortium). However, only authorized personnel can gain access to a permissioned blockchain.

B Architecture and Working

A Wireless Sensor Network Architecture is created on the roads by a combination of RSUs and BSs. The ratio of RSUs and BSs is decided depending upon the traffic density and road layouts of a given city or town. The RFID Readers in the RSUs read radio signals from the RFID tags mounted on vehicles as soon as any vehicle passes it. The License Plate Number and the time at which a vehicle passes the RSU is recorded and is sent to the nearest BS by multi-hop communication in the WSN. The BS updates the Smart Contracts with the gathered data and form immutable blocks storing the travel history of every vehicle passing every node. The RSUs are mounted at an elevated height to avoid obstacles and ensure minimum loss of data. In any special case if some hefty architecture acts as an obstruction in the routing of data between RSUs, a blank node (without any RFID reader or antenna) can be installed to facilitate seamless data transmission to the BSs.

a. RFID Tags on Vehicles: The Battery Assisted Passive (BAP) RFID tags will be placed on the roof in case of four-wheelers and on the windscreen or above the headlight in the case of two-wheelers.

b. Roadside Unit (RSU-Nodes of WSN): The coordinates of the location of an RSU are predetermined, that is, they are geotagged while installation. Every RSU has three components RFID Reader, External Antenna(s), and a Communication Node. They read the Registration Id of the vehicles and route the data to the Base stations.The RSU should be mounted at an elevation between a range of 5-6m from the ground. This is mainly done to maintain a lower obstruction level between the RFID tags and the readers. The majority of the roads have street lights and thus these can be used for mounting the RSUs instead of adding any extra infrastructure. For withstanding harsh environmental conditions, the components with a good IP rating are selected. The RSUs route the gathered data to a BS. License plate number, timestamp of reading and coordinates of the RSU are forwarded.

c. Base-Stations (sink nodes of WSN): The BS runs and manages a private blockchain network. It has a higher processing power and storage capacity as compared to RSUs. The data received from RSUs are stored in a Buffer Memory. The distributed ledger of the vehicle tracking system is formed using Smart Contracts. These Smart Contracts take data from the Buffer Memory and keep updating the blockchain continuously. In case of an internet connectivity error, the data gathered keeps queuing up in the buffer memory and there is no loss of data. It is updated in the blockchain later on.

d. Routing Protocol: The data gained by RFID readers at every RSU should reach the BS for updating the blockchain. This is achieved by multi-hop communication among the RSUs. We propose a routing protocol with very low complexity and low data loss. Between any two BSs, a cluster of 20 RSUs is created. Every RSU sends its data to the next RSU in line which is closest to the next BS. In case of failure of an RSU the data is transmitted to the previous RSU in the opposite direction. As shown in Figure. 1. the cluster of nodes is divided into 2 groups. 10 nodes in line send data to a BS in one direction and the other set of 10 nodes route data to another BS in the opposite direction. The data from any RSU reaches the nearest BS within milliseconds. Thus, in an ideal condition the maximum number of hops to route data to a BS is 10 which keeps decreasing linearly while approaching the BS. The case of failure of an RSU is described in section II.D.1.

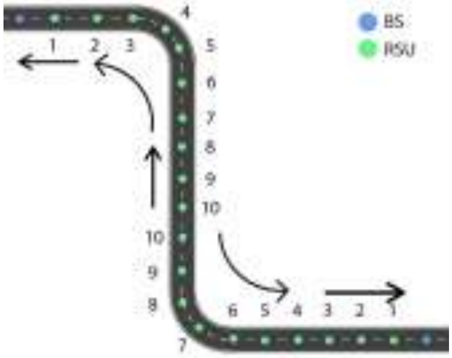

Figure 1. Routing Protocol followed in RSUs

e. Power: The BSs and the RSUs can be mounted on the street lights for elevation. The system draws power from the street light's power source. Nowadays, solar powered street lights are a common occurrence and hence most of the power requirements can be satisfied by renewable energy without levying a high cost. A considerable amount of energy is saved at the BS by using a Proof-of-Authority (PoA) consensus algorithm. It has a high transaction rate with low energy consumption. A battery backup can be provided at regions of unavailability of street lights. We are using the existing infrastructure to supply power to our system to reduce the cost.

f. Tag Anti-Collision Algorithm: Numerous vehicles near an RSU leads to a dynamic arrival of RFID tags near a reader. In such cases collision of RFID tags for fast identification may lead to missing data. To overcome this problem a tag anti-collision algorithm known as DAS-DFSA [2] can be used. It is based on blocking technology, dynamic frame-slotted Aloha (DFSA) algorithm, and the first-come-first-serve (FCFS) idea [2]. At the end of each frame, the optimal frame length and the arrival rate of the next frame is decided along with an estimation of the number of unidentified tags. The next frame is divided into arrival and waiting slots. This reduces the conflict of slots; the arrival tag is identified in the ongoing frame and the unidentified waiting tags (in the previous frames) wait for a lesser amount of time.

g. Storage: The BSs have onboard storage to store the Blockchain data locally. For optimizing storage space at a BS, at the end of every year, a snapshot of the travel history database is copied to a secured server. Then the existing copies of the blockchain are deleted from the BSs. After the deletion process is complete a new blockchain is formed.

C Cases of Rsu Deployment

Considering different kinds of road planning we propose different RSU deployment strategies to reduce infrastructure cost and power consumption.

1. Single Lane Roads and Narrow Roads: The RSUs are mounted at an elevation with a single, directional antenna, all placed on a single side of the road. The antenna will have an inclination of 45 to 60 degrees pointing towards the road. This results in the alignment of the reader's antenna with the plane of the tags for maximum absorption of RF energy.

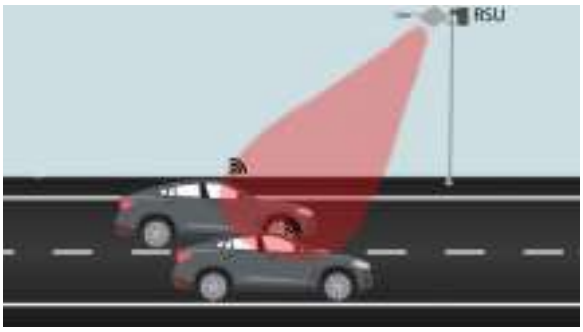

Figure 2. RFID Reader with directional antenna on only one side of the road

2. Multiple lane Roads and Wide Roads: The elevated RSUs will be mounted in the middle of the road (lane dividers) with omnidirectional antennas. These antennas have a 360-degree field of view. This enables a single node to capture vehicle movement of all lanes and reduces the number of nodes and antennas required for monitoring wide roads, as shows in figure 2.

Figure 3. RFID Reader with omnidirectional antenna installed in the middle of the road

3. Curvy Mountain Roads: In hilly regions vehicle tracking using satellite communication is cumbersome and highly inaccurate. The steep hills act as obstacles in the process of triangulation, as shows in figure 3. Thus, we propose a special case of node placement in such terrains. Considering a road similar to Figure. 4. wherein the road makes steep turns and horizontal communication among RSUs can be difficult and obstructed. Since such roads follow a single route, the route of a vehicle can be predicted easily in a given direction. Thus, a lesser number of RSUs can be deployed for optimizing the cost. Also, the RSUs are fixed at elevated poles with an outward horizontal extension to avoid obstacles and maintain a line-of-sight communication among nodes to ensure seamless routing and low data loss. A BS is set up at the foot of the hill to keep the ledger updated.

Figure 4. RSU placement on hilly regions.

4. Interstate Highways: Highways usually span over several kilometers without too many diversions and the vehicle can travel in a specific direction only. Thus, the number of RSUs can be reduced without affecting the accuracy of vehicle travel history records by installing them only at entry points, exit points, and toll booths.

D Case of Failure

1. RSU Failure:In this situation, the RSU behind the failed node starts sending the data through the alternate path in the opposite direction to another BS. The BS checks the number of RSUs from which it is receiving the after every few hours, throughout the day. If it notices a change in this number, an alert will be raised for the failed node.

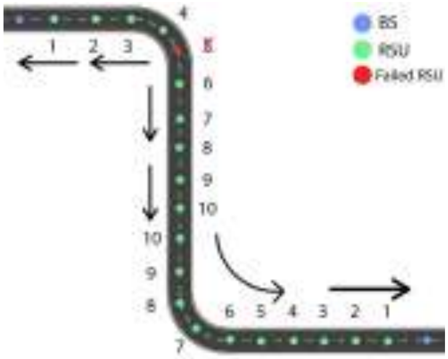

Figure 5. Routing in case of Failure

2. Base station Failure: The blockchain is to be accessed by an access point which also monitors the BS. The BSs are programmed to ping the access point after regular intervals several times a day. If the access point notices that a BS is missing for a prolonged time period, an alert will be raised by the access point for the corresponding BS, as shows in figure 5.
3. Internet Shutdown at Base-Stations: An internet connection is not required by the RSUs to communicate between each other and to the BS. If the BS loses its connection to the internet, it will keep receiving the data from the RSUs. This data is to be stored in a Buffer. After restoration of the internet access at the BS, the sync routine is started by the blockchain then it starts clearing the buffer after updating the blockchain with stored data.

E Workflow

Step 1	The RFID tag on the vehicle communicates it's License Plate number to every node it passes.
Step 2	The geotagged RSUs collect data of all vehicles moving past them with instantaneous timestamps.
Step 3	RSUs route all data to the nearest BSs through multi-hop communication.
Step 4	Base-Stations update a private Blockchain network using PoA Consensus mechanism.
Step 5	Distributed ledgers specifying License plate numbers, location coordinates, and timestamps are formed.
Step 6	Data Retrieval by authorized personnel.

IV EXPERIMENT

RSUs: The ESP32 board is used for communicating with other nodes. It has a dual core processor which plays a vital role in multitasking and thus speeding up the processes. It communicates on 2.4 GHz bandwidth which gives a large range for data transmission. When any core is in idle mode then it can be used to shut down the peripherals that are not in use at that time thus decreasing power consumption. The two 32-bit TensilicaXtensa LX6 microprocessor of the ESP32 operates at 160 or 240 MHz and performs at up to 600 DMIPS, running at 3.3 volts.

BSs: For prototyping BSs Raspberry Pi 4 [8][9] is used. It has a quad core Cortex-A72 (ARM v8) 64-bit SoC which clocks at 1.5 GHz. A 4GB RAM variant is used to have enough system memory to run the processes smoothly. It has a capacity of 128 GB for storing a copy of the blockchain and the buffer memory.

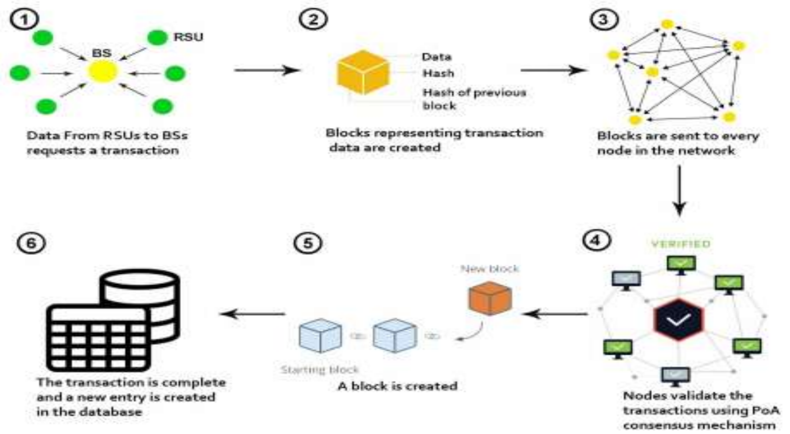

Figure 6. Formation of Blocks and updating of the Database.

Blockchain: A private blockchain is created on Ethereum using a Proof-of-Authority (PoA) consensus mechanism [7] is created with Base stations as its primary nodes. Figure. 6. Shows how a blockchain will keep getting updated with every data entry. PoA is highly favoured in privateblockchains since all nodes are pre-authenticated. Unlike the Proof-of-Work consensus algorithm, which requires high computation intensive mining and has a low transactions per second (TPS) value, PoA gives a designated number of blockchain nodes to update the distributed registry solely dependent on its reputation. It has a high TPS value and requires negligible computation power and thus almost no electricity.

The Smart Contracts play a vital role in storing the transferred records and then retrieving the data in a meaningful way only accessible to authorizedorganizations. Smart contracts are self-executing computer protocol intended which digitally facilitates, verifies, and enforces the negotiation of a contract. It is a business-logic component running in the backend and can be extended by a GUI into a decentralized application. Figure. 7. shows a dashboard for data retrieval. This data can be viewed only by authorized bodies.

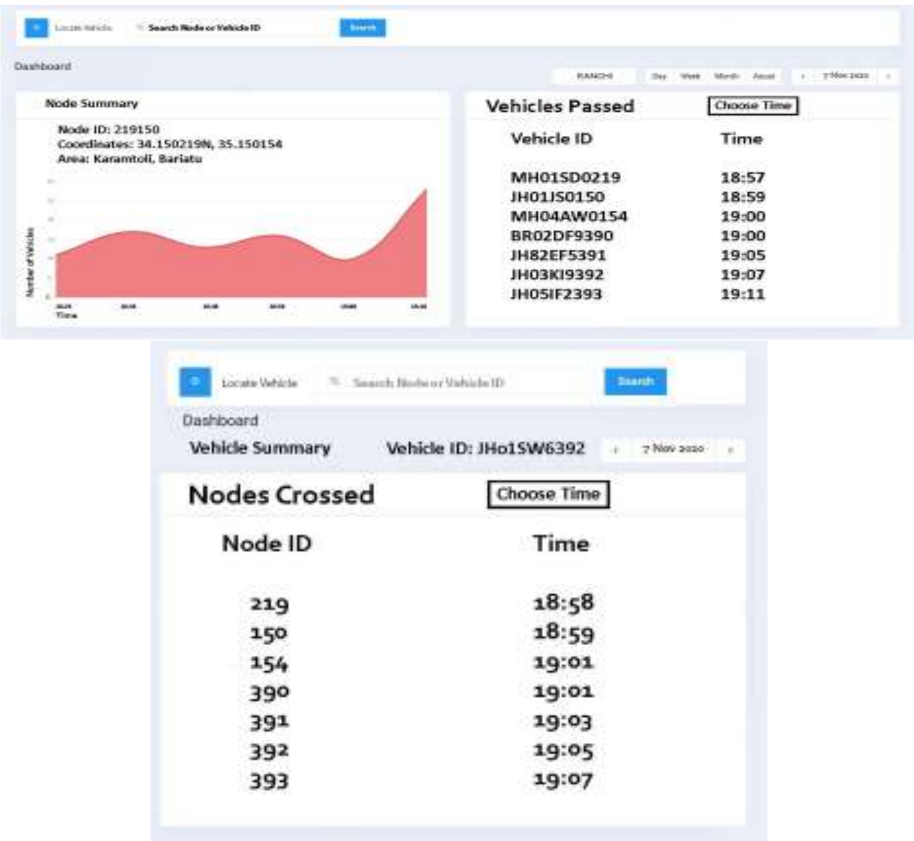

Figure 7. Dashboard for Data Retrieval

V APPLICATIONS

1. Vehicle Tracking and Travel History: The travel history of the vehicles is tracked by using this system. One can keep a track of the locations the vehicles have been to. Also, an accounting report of the travels can be produced if the travel history of the vehicle is known. Hence, information such as location, speed, distance covered, duration per stop, etc. can be tracked.

2. Automatic Digital Payment System: The proposed system can be used to make payments at toll booths and petrol pumps directly from the linked bank accounts. Once the car ID is successfully verified, the acquirer host would compute the exact transaction amount and then initiate a debit request. This debit request would then be sent to the financial organizations (using the organization's API) to complete the debit request.

3. Fleet management: The governing body can provide commercial companies with fleet management solutions by giving them access to the tracking information of the vehicles in their fleet. This information can be used by the companies to reduce working costs, increase safety, implement cost-effective maintenance, and achieve higher fleet operational efficiencies.

4. Fast vehicle recovery: The proposed system would continue to track the vehicle location even if the vehicle is off. So, in case of any stolen vehicle, its whereabouts can be determined.

5. Police RFID scanner: Traffic police can be equipped with a handheld RFID scanner. If they want to check the details of any vehicle, they simply have to scan the Car ID and all the details of the vehicle and the driver ranging from the driving license to vehicle registration can be accessed and viewed. In the case of penalty/fine, a ticket can be raised in the name of the driver.

6. Security of Restricted Areas: There are many private areas, both military and civilian, where access to normal vehicles is restricted. If in case any suspicious vehicle tries to enter, it can be tracked and penalized.

VI CONCLUSION

We propose a uniform vehicle tracking system which can be efficiently deployed in almost all terrains. This in turn contributes to the formation of a detailed database of all vehicles travelling to various locations throughout the country. It stores the travel history of vehicles taking into consideration security of data and privacy of the people using state-of-art Blockchain technology. Since the database is stored in a blockchain, the data is tampering proof and the decentralized storage highly scales down the loss of data. The node deployment in the Wireless Sensor Network is varied in accordance with road planning and alternating terrain to optimize the cost and the power consumed. An analysis of possible faulty scenarios and their suitable solutions are discussed to form a highly fault tolerant system with minimal data loss. The system architecture can be easily integrated with the existing infrastructure of roads reducing power consumption and relying on renewable energy. Moreover, it is capable of numerous other applications through a single consolidated system.

VII FUTURE WORK

The Wireless Sensor Network Architecture can be utilized for monitoring further parameters like velocity and acceleration of the vehicles. Furthermore, the gathered data can be extended to form a map navigation system to attain higher accuracy.

REFERENCES

1. A.Riyazdeen, B.Padmasri, “Wireless Sensor Network Based Vehicle Tracking and Identifying System”, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Volume 2, Issue 5, May 2013, ISSN: 2278 – 909X.
2. Guofeng Zhang, Sha Tao, Lina Yu, Wan’ang Xiao, Qiang Cai, Wanlin Gao, Jingdun Jia, Juan Wen, "A Fast RFID Tag Anti-collision Algorithm for Dynamic Arrival Scenarios Based on First-Come-First-Serve", Mobile Information Systems, vol. 2019, Article ID 4625758, 17 pages, 2019. https://doi.org/10.1155/2019/4625758.

3. T. Jiang, H. Fang and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640-4649, June 2019, doi: 10.1109/JIOT.2018.2874398.
4. A Blockchain Framework for Securing Connected and Autonomous Vehicles by Geetanjali Rathee[1], Ashutosh Sharma [2], Razi Iqbal [3], Moayad Aloqaily[4], Naveen Jaglan[2] andRajiv Kumar[2]. Mdpi Sensors 2019, 19(14), 3165.
5. Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, 2016, pp. 1-6, doi: 10.1109/ICSSSM.2016.7538424.
6. Lin, Jun, et al. ”Using blockchain to build trusted lorawan sharing server.”International Journal of Crowd Science 1.3 (2017): 270-280
7. Private Blockchain Consensus Mechanisms:
https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb
8. Fernando, Erick &Meyliana, Surjandy.(2019). Blockchain Technology Implementation In Raspberry Pi For Private Network. 154-158. 10.1109/SIET48054.2019.8986053.
9. NiclasKullig, Philipp Lämmel, Nikolay Tcholtchev, “Prototype Implementation and Evaluation of a Blockchain Component on IoT Devices” The 15th International Conference on Future Networks and Communications (FNC) August 9-12, 2020, Leuven, Belgium.
10. Jaco Prinsloo and Reza Malekian ,”Accurate Vehicle Location System Using RFID, an Internet of Things Approach”MDPI 2016.
11. Wang, Jianqiang& Ni, Daiheng& Li, Keqiang. (2014). RFID-Based Vehicle Positioning and Its Applications in Connected Vehicles. Sensors (Basel, Switzerland). 14. 4225-38. 10.3390/s140304225.