FAST RECURSIVE TRANSMISSION ALGORITHM USING VANETs

P. Santhiya[1], P. Rajeswari[2], K.Soundharya[3], K.Sowndharya[4]

[2-4]UG Scholar, Dept. of CSE, Paavai Engineering College
[1]Assistant Professor, Dept. of CSE, Paavai Engineering College, Tamil Nadu, India

---

Abstract: Vehicular ad-hoc networks (VANETs) technology has emerged as an important research area over the last few years. A reliable transmission protocol is presented based on any cast routing. Using Optimizing Route Request Response Technique as a contribution, control overhead is minimized in the proposed protocol. Signal from the fall detection system is transmitted. This method is used for vehicle node to be able to upload the sensor Data to the management center for storage is such a security risk, such as malicious tampering and data leakage is susceptible. In order to address the challenges of these security, we, on the basis of the fast recursive transmission algorithm (FRTA) of the consortium, and suggests the sharing and storage system of data security. Fast routing protocol is proposed to guarantee the multi-hop wireless link between the source and destination using fast recursive transmission algorithm. Based on bilinear characteristics, the digital signature technology pairing for elliptic curve is used to ensure the reliability and integrity when transmitting data to the nodes. Emerging Consortium block chain technology, decentralized maintained by the entire network node, a safe, and provides a reliable data smart contract is used to limit the trigger condition for assigning data coin involvement vehicle contribution of data for a preselected node stores transmission and data. Security analysis and performance evaluation, our FRTA solutions, from the viewpoint of the storage and sharing of data, has demonstrated that the more secure and reliable.

1. INTRODUCTION

Vehicular ad-hoc networks are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network of mobile devices – to the domain of vehicles. VANETs were first mentioned and introduced in 2001 under "car-to-car ad-hoc mobile communication and networking" applications, where networks can be formed and information can be relayed among cars. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services. VANETs are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs are referred to as Intelligent Transportation Networks. Vehicular networks special characteristics make them susceptible to a wide range of attacks. The most common attacks are: impersonation, bogus information injection, non-integrity, non-confidentiality, and Denial of Service (DoS). Two classes of attacks are likely to occur in vehicular networks i) external attacks, in which attackers not belonging to the network jam the communication or inject erroneous information. ii) Internal attacks, in which attackers are internal compromised nodes that are difficult to be detected. Both types of attacks may be either passive intending to steal information and to eaves drop on the communication within the network, or active modifying and injecting packets to the network. As a counter-measure against most of these attacks, the following security considerations should be satisfied: providing a trust infrastructure between communicating vehicles, mutual authentication between each communicating pair whether two vehicles or a vehicle and a fixed element of the infrastructure, efficient access control mechanisms allowing not only the authorization to the network access but also the authorization to the service access, and confidential, secure data transfer.

1.1 AUTHENTICATION, AUTHORIZATION AND ACCESS CONTROL

Authentication and authorization are important counter-attack measures in vehicular networks deployment, allowing only authorized mobile nodes to be connected and preventing adversaries to sneak into the network, disrupting the normal operation or service provision. A simple solution to carryout authentication in such environment is to employ an authentication key shared by all nodes in the network. Although this mechanism is considered as a plug and play solution and does not require the communication with centralized network entities, it is limited to closed scenarios of small number of vehicles, mostly belonging to the same provider. For wide scale commercial deployment of vehicular networks, the shared secret authentication has two main pitfalls: firstly, an attacker only needs to compromise one node vehicle to break the security of the system and paralyze the entire network. Secondly, mobile nodes vehicles do not usually belong to the same community, which leads to a difficulty in installing/pre-configuring the shared keys. In fact, distributed authentication and authorization schemes with secure key management are required in such environment. A possible approach for distributed authentication is the Continuous discovery and mutual authentication between neighbors, whether they are moving Vehicles or fixed architectural elements access points or base stations. Nevertheless, if mobile nodes vehicles move back to the range of previous authenticated neighbors or fixed nodes, it is necessary to perform reauthentication in order to prevent an adversary from taking advantage of the gap between the last association and the current association with the old neighbor to launch an impersonation attack. The re-authentication procedure should be secure and with the minimum possible delay in order to assure services' continuity.

1.2 VEHICULAR APPLICATION AND INTERNET IMPLEMENTATION

Vehicles in a grid are only a few hops away from the infrastructure Wi-Fi, cellular, satellite. Protocol and application design must account for easy access to the Internet during normal operation.

At the same time, the vehicles are among the few communications nodes that can continue to operate when the Internet goes away, during urban emergency, with enough reserve power to establish a vehicle based emergency network.

To this end we examine innovative peer to peer content sharing applications that can still operate with intermittent connectivity and sporadic vehicular traffic and connectivity. Peer to peer applications have so far been confined to the fixed Internet.

The storage and processing capacity of modern vehicles make such applications feasible also on mobile platforms. In these dynamic scenarios we must understand the role of the Internet in facilitating the smooth transition from full Internet connectivity to full autonomy.

This is a radical concept in ad hoc networks traditionally designed for exclusively autonomous operation and thus unable to exploit the interconnection and resource sharing of the wired Internet. In the sequel, we consider a number of emerging VANET applications and study their interdependence with the Internet.

1.3 ROUTABLE ADDRESSES AND POISITION BASED ADDRESSING

Addressing is a major challenge in the management of vehicular network mobility and an important enabler of interconnection to and through the Internet. First, we must distinguish between Unique Identifier, license plate, Vehicle-ID, and Routable Address or unique ID (typically IP address) for conventional routing AODV. It is becoming apparent that the dominant form of routing in the vehicle grid will be position based geo-routing. This is because of the emergence of location aware communications, i.e., the need to establish connections and 5 route packets to entities and resources characterized by location rather than a specific ID. More traditional MANET routing schemes, AODV and OLSR, will also be used in the vehicle grid. These schemes currently use IP address as the routable addresses to set up/maintain the routes. The IP address is an extremely effective routable address in the static, hierarchical Internet structure enabling, for example, prefix routing. It is not very helpful in finding (hierarchical) routes in a constantly changing network like the vehicle grid unless it is combined with the Mobile IP construct, with provides the desired redirection.

2. EXISTING SYSTEM

Vehicles form a network node in VANET. Traffic management center can be distributed in road resources through distributed synchronization and coordination. As part of the Intelligent Transport Systems, VANET's aim is to enhance traffic flow to improve road safety and reduce congestion.

In existing system, the sender as well as the receiver did not know the path in which the data has been transmitted. If any of the data is lost, the existing system cannot find the route at which the fault occurs.

Traffic and end-to-end transmission delay is the result observed from the above scheme.

2.1 DISADVANTAGES

- Delay Packets Transmission
- Cost Effective
- Reliability is Less
- Efficiency and computational overheads
- Receiving Duplicate Packets

3. PROPOSED SYSTEM

Many routing protocols have been proposed to meet the different requirements and scenarios. They also use path markers scheme which is used by the selected optimal controller, also known as an interface northbound and southbound. In various scenarios, various topology tree has been designed using the ring and spanning tree. The switch arrangement is done for each of the topology. All of these routing protocols, usually have to deal with frequent link break problems caused by any movement or 22 instability of the node. Using a fast recursive transmission algorithm (FRTA) probability optimization method, it can be optimized to obtain the automatic search space, self-adaptation adjusts the search direction.

3.1 ADVANTAGES

- Transfer data efficiently in bulk across a network

- Progress is not lost, even if the connection is timed out.
- Send multiple file directories at the same time
- Move files around easily and in an organized fashion
- Easy to use

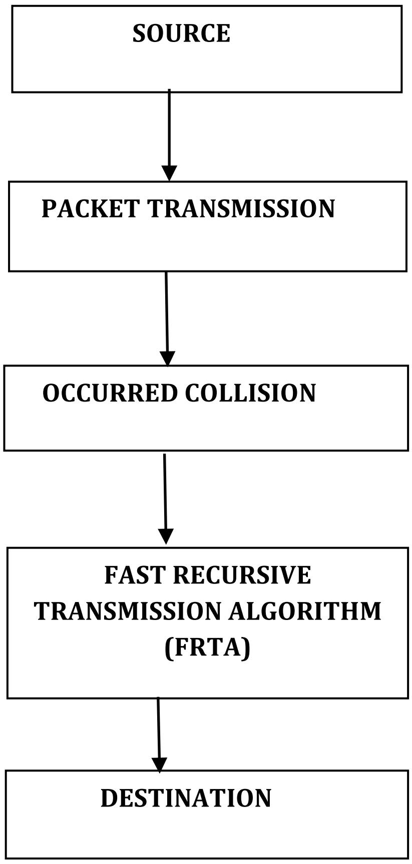

FIG 1.1: BLOCK DIAGRAM OF PROPOSED SYSTEM

4. CONCLUSION

Fast routing protocol has been proposed to ensure multi hop radio link between the source and destination using a fast recursive transmission algorithm. Based on bilinear characteristics, pairing of digital signature technology for the elliptic curve is used to ensure the reliability and integrity when transmitting data to the nodes. Consortium block chain technologies emerging, the overall network node, maintained by the safety, and in order to limit a trigger condition for allocating the contribution data coin involvement vehicle data for transmission data smart contract to store pre-selected node distributed to provide reliable data to be used.

5. REFERENCES

[1] F. Bai, D.D. Stancil, and H. Krishnan, “Toward Understanding Characteristics of Dedicated Short Range Communications (DSRC) from a Perspective of Vehicular Network Engineers,”Proc. ACM MobiCom, 2010.

[2] Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, “Exploiting Ubiquitous Data Collection for Mobile Users in Wireless Sensor Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 2, pp. 312- 326, Feb. 2013.

[3] M. Li and Y. Liu, “Rendered Path: Range-Free Localization in Anisotropic Sensor Networks with Holes,” IEEE /ACM Trans. Networking, vol. 18, no. 1, pp. 320-332, Feb. 2010.

[4] L. Chisalita and N. Shahmehri, “A Peer-to-Peer Approach to Vehicular Communication for the Support of Traffic Safety Applications,” Proc. Fifth IEEE Conf. Intelligent Transportation Systems, pp. 336-341, 2002.

[5] Z. Li, Y. Zhu, H. Zhu, and M. Li, “Compressive Sensing Approach to Urban Traffic Sensing,” Proc. IEEE 31st Int’l Conf. Distributed Computing Systems (ICDCS), 2011.

[6] H. Zhu, Y. Zhu, M. Li, and L.M. Ni, “SEER: Metropolitan-Scale Traffic Perception Based on Lossy Sensory Data,” Proc. IEEE INFOCOM, 2009.

[7] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, “The Pothole Patrol: Using a Mobile Sensor Network for Road Surface Monitoring,” Proc. ACM Sixth Int’l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[8] P. Gibbons, B. Karp, Y. Ke, S. Nath, and S. Seshan, “Irisnet: An Architecture for a Worldwide Sensor Web,” IEEE Pervasive Computing, vol. 2, no. 4, pp. 22-33, Oct.-Dec. 2003.

[9] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, “Mobeyes: Smart Mobs for Urban Monitoring with a Vehicular Sensor Network,” IEEE Wireless Comm., vol. 13,no. 5, pp. 52-57, Oct. 2006.

[10] I. Leontiadis and C. Mascolo, “GeOpps: Geographical Opportunistic Routing for Vehicular Networks,” Proc. IEEE Int’l Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-6, 2007.