Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.948 – 953

REVIEW ARTICLE

SECURITY PROTOCOLS FOR VEHICULAR ADHOC NETWORKS: A REVIEW

[1]Shubham Gandhi, [2]Shalini

[1]Assistant Professor (Department of ECE), [2]M.Tech Scholar, Department of ECE
Baba Mastnath College of Engineering

Abstract- VANET is the technology of building a robust Ad-Hoc network between mobile vehicles and each other, besides, between mobile vehicles and roadside units. Throughout the world, there are many national and international projects in governments, industry, and academia devoted to the development of VANET protocols. In this paper I have reviewed the various security protocols used for vehicular ad hoc networks, along with their characteristics and challenges.

Keywords: VANETS, protocols, ad hoc network

I. INTRODUCTION

VANET is the technology of building a robust Ad-Hoc network between mobile vehicles and each other, besides, between mobile vehicles and roadside units. There are two types of nodes in VANETs; mobile nodes as On Board Units (OBUs) and static nodes as Road Side Units (RSUs). An OBU resembles the mobile network module and a central processing unit for on-board sensors and warning devices. The RSUs can be mounted in centralized locations such as intersections, parking lots or gas stations. They can play a significant role in many applications such as a gate to the Internet.

VANET presents a new and promising field of research, development and standardization. Throughout the world, there are many national and international projects in governments, industry, and academia devoted to the development of VANET protocols. These projects include consortiums like 'The Dedicated Short Range Communications (DSRC)' (USA) [7], the 'Car-to-Car Communication' (Europe) [8] and the 'Intelligent Transportation Systems' (Japan), and standardization efforts like the IEEE 802.11p'Wireless Access in Vehicular Environment' (WAVE).Communication researchers have been recently working on a prominent step; if each vehicle has a device that can communicate with other vehicles; vehicles will have a gigantic new source of information that extends beyond the capabilities of all previously mentioned devices. For example, all of these devices cannot warn the driver of a stopping vehicle in the next turn and of course cannot let travellers enjoy video chatting and file sharing at no charge.

II. RELATED WORK

Catalin Gosman et.al. [1] presented a security protocol designed for VANET environments. It guarantees the content of messages against possible attackers. Because privacy of the passengers must be preserved in VANET, the security protocol is designed not to rely on the driver's identity. The protocol also proves the time and location when a message was sent. The researchers present the evaluation results demonstrating that the protocol is able to correctly handle different security threats. The security protocol considers the particular characteristics of VANETs. It ensures data integrity, reliability, non-repudiation, preserves privacy and links a message to a particular time and place the message was generated. The security protocol is implemented in VANET simulator and the evaluation result shows its capability to handle a wide range of attacks that are characteristic to such environments. In the future, the research can be extended to consider various other alternatives of signing and validating messages in VANETs.

Farzad Sabahi [2] discussed security issue as one of the most important problems in Vehicular Ad hoc network. The VANET is a combination of computing, communication which introduces the benefit of using several kinds of its technology. Moreover, VANET is a new technology and has considerable vulnerabilities certainly which give great chances to attackers to break it. These malicious users always try to challenge the networks with their selfish behaviour. Ad hoc protocols play the main role in VANET but they have size limits and are always smaller than the VANETs. The size of VANETs and their characteristics inherited from ad hoc make difficulties in implementing security capabilities and policies. All issues which exist in VANET and mentioned in this paper may have solutions. However, there are two major issues which should be considered. Firstly, there is difficulty of implementation and secondly, there is a probability of lacking economic justification for the company which provides VANET-based services. In addition, there are many cases where those solutions are difficult or impossible to implement.

Ghassan Samara et. al.[3] reviewed that Vehicular Ad Hoc Networks is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. This paper gave a wide analysis for the current challenges and solutions, and critics for these solutions, the researchers proposed a new solution that will help to maintain a securer VANET network.

Gongjun Yan et. al.[4] contributed a novel approach for enhancing position security in VANET. The researchers achieved local and global position security by using the on-board radar to detect neighbouring vehicles and to confirm their announced coordinates. The researchers computed cosine similarity among data collected by radar and neighbours reports to filter the forged data from the truthful data. Based on filtered data, they created a history of vehicle movement. By checking the history and computing similarity, a large number of Sybil attacks and some combinations of Sybil and position-based attacks can be prevented.

Jason J.Haas et.al. [5] used recordings of actual vehicle movements on various roadways. Many results have been published in the literature based on performance measurements obtained from simulations of VANETs. These simulations use as input traces of vehicles movements that have been generated by traffic simulators which are based on traffic theory models. Till now, no one has published any work based on actual large-scale recordings of vehicle movements. In order to enable analysis on this scale, the researcher developed a new VANET simulator, which can handle many more vehicles than NS-2. To use their own simulator, the researcher presented results of a cross-validation between NS-2 and their simulator, showing that both simulators produce results that are statistically the same. They used their simulator to analyse the proposed authentication mechanism, which relies on ECDSA signatures, comparing it to broadcast authentication using TESLA. The evaluations are performed using real vehicle mobility, which is the first simulation using real vehicle mobility. The comparison shows strengths and weaknesses for each of these authentication schemes in terms of the reception rates and latency of broadcast packets.

Surabhi Mahajan et. al.[6] discussed the problems of Security, Privacy in VANET. The authentication scheme-proxy re-encryption is reviewed which helps in reducing authentication overheads in rapid roaming networks with the use of public key assigned to the “delegate” and private key assigned to the “delegator”. Further the new proxy re-encryption scheme is presented in which the public key is replaced by the private key so as to get better result for authenticity and privacy in rapidly changing networks. The private keys are assigned to both delegator and delegate, which will prove secure email forwarding with less overhead in the information transmission. It is observed that the new proxy re-encryption scheme is better than the earlier one on the basis of the privacy; security and authentication and reduce overheads while roaming networks.

III. CHARACTERISITCS OF VANETS

- **Potentially high number of nodes**:
  Regarding VANETs as the technical basis for envisioned intelligent transportation system (ITS) we expect that a large portion of vehicles will be equipped with communication capabilities for vehicular communication. Taking additionally potential roadside units into accounts, VANET needs to be scalable with a very high number of nodes.
- **High mobility and frequent topology changes**:
  Nodes potentially move with high speed. Hence in certain scenarios such as when vehicles pass each other, the duration of time that remains for exchanging of data packets is rather small.
- **High application requirement on data delivery**:
  Important VANET applications are for traffic safety to avoid road accidents, potentially including safety of life. These applications have requirements with respect to real time and reliability. An end-to-end delay of seconds can render safety information meaningless.
- **No confidentiality of data information**:
  For safety application, the information contained in a message is of interest for all road users and hence not confidential.

IV. CHALLENGES

VANETs are an instantiation of mobile ad hoc networks (MANETs) [9]. MANETs have no fixed infrastructure and instead rely on ordinary nodes to perform routing of messages and network management functions. However, vehicular ad hoc networks behave in different ways than conventional MANETs. Driver behaviour, mobility constraints, and high speeds create unique characteristics of VANETs. These characteristics have important implications for designing decisions in these networks. Thus, numerous challenges need to be addressed for inter-vehicular communications to be widely deployed.

- **Node Velocity:**
  One of the most important aspects of mobility in VANETs is the potential node velocity. Nodes either denote vehicles or road side units (RSUs) in this case. Node velocity may range from zero for stationary RSUs or when vehicles are stuck in a traffic jam to over 200 km per hour on highways. In particular, these two extremes each pose a special challenge to the communication system. In case of very high node velocities, the mutual wireless communication window is very short due to a relatively small transmission range of several hundred meters [10]. For example, if two cars driving in opposite directions with 90 km/h each, and if we assume a theoretical wireless transmission range of 300m, communication is only possible for 12 seconds. Moreover, the transceivers have to cope with physical phenomena like the Doppler effect. In the review of issues related to inter-vehicle communication in [11], it is show that routes discovered by topology-based routing protocols get invalid (due to changing topology and link failures at high speeds) even before they are fully established. High node velocities mean frequent topological changes. However, slow movements usually mean stable topology, but a very high vehicle density, which results in high interference, medium access problems, etc. For such reasons, very scalable communication solutions are required.
- **Movement Patterns:**
  VANET are characterized by a potentially large number of nodes that are highly mobile (i.e. according to cars' speed). This high mobility can be more or less important depending on road nature (small streets vs. highways). Vehicles do not move around arbitrarily, but use predefined roads, usually in two directions. Unpredictable changes in the direction of vehicles usually only occur at intersections of roads. We can distinguish three types of roads [10]:

a. City roads:
Inside cities, the road density is relatively high. There are lots of smaller roads, but also bigger, arterial roads. Many intersections cut road segments into small pieces. Often, buildings right beside the roads limit wireless communication.

b. Rural roads:
These roads usually have much larger segments, which means that intersections are rarer than in cities. Traffic conditions often do not allow the formation of a connected network, because too few vehicles are on the road. The overall direction of rural roads changes more frequently than the direction of highways.

c. Highways:
Highways typically form a multi-lane road, which has very large segments and well-defined exits and on-ramps. High speed traffic encountered here.

A node can quickly join or leave the network in a very short time leading to frequent network partitioning and topology changes. These movement scenarios pose special challenges particularly for the routing. Even on a highway, that gives smooth traffic in one direction, frequent fragmentation was encountered in [12]. In the simulation of 9.2 miles of a highway, in [12], a link lifetime of only about 1 minute was obtained even when driving in the same direction (assuming 500 ft radio range).

- **Node Density:**
  Apart from speed and movement pattern, node density is the third key property of vehicular mobility [10]. The number of other vehicles in mutual radio range may vary from zero to dozens or even hundreds. If we assume a traffic jam on a highway with 4 lanes, one vehicle at every 20 meters and a radio range of 300m, every node theoretically has 120 vehicles in his transmission range. In case of very low density, immediate message forwarding gets impossible. In this case, more sophisticated information dissemination is necessary, which can store and forward selected information, when vehicles encounter each other. In this case, the same message may be repeated by the same vehicle multiple times. In high density situations, the opposite must be achieved. Here, a message should be repeated only by selected nodes, because otherwise this may lead to an overloaded channel [10].

V. APPLICATIONS

The VANET applications are grouped into three categories:

1. Safety applications
2. Traffic applications
3. User applications

Some of the Safety application feature requirements are:

- Security:
  Besides the introduction and management of trust also the security of message content is a big issue for vehicle to vehicle communication. The content of a received message has to be verified within a short time to be able to use the information as soon as possible.
- Authentication:
  The authentication service is concerned with assuring that the communication is authentic in its entities. Vehicle should react to events only with disseminating messages generated by legal senders. Therefore we need to authenticate the senders of these messages.
- Integrity:
  The integrity service deals with the stability of a stream of messages. It assures that messages are received as sent, without modification, insertion, reordering, or replays.
- Confidentiality:
  This service provides the confidentiality to the communication content. It guarantees the privacy of drivers against unauthorized observers.
- Accessibility:
  A kind of attacks can result in the loss in the accessibility. Even a robust communication channel can still suffer some attacks which can bring down the network. Therefore, availability should be also supported by alternative means. An important feature of VANET security is the digital signature.

Some of the traffic applications are:

- Co-operative collision warning:
  Co operative collision warning is an OBU to OBU safety application, that is, in case of any abrupt change in speed or driving direction, the vehicle is considered abnormal and broadcasts a warning message to warn all of the following vehicles of the probable danger. This application requires an efficient broadcasting algorithm with a very small latency.
- Lane changing warning:
  Lane changing warning is an OBU to OBU safety application, that is, a vehicle driver can warn other vehicles of his intention to change the travelling lane and to book an empty room in the approaching lane.
- Intersection collision warning:
  Intersection collision warning is an OBU to RSU safety application. At intersections, a centralized node warns approaching vehicles of possible accidents and assists them determining the suitable approaching speed. This application uses only broadcast message.
- Traffic management:
  In vehicle, navigation is a non-safety application that is designed to reduce driving time and fuel consumption by exchanging real-time information about traffic conditions in the driving route.

Some of the user applications are:

- Inter vehicle communication:
  Inter vehicle communication is an OBU to OBU non-safety application that enables travellers to communicate with each other using instant file transfer, voice chatting or even video chatting.
- Electronic toll collection (ETC):
  Electronic toll collection is an OBU to RSU non-safety application that supports the collection of payment to toll plazas using automated system to increase the operational efficiency.
- Parking lot management:
- Parking lot payment is an OBU to RSU non-safety application that provides benefit to parking lot operators, simplify payment for customers, and reduce congestion at entrance and exits of parking lots.

VI. SECURITY PROTOCOLS

The Security Protocols available are:

- Cognitive security protocol for sensor based VANET
- Real-World VANET security protocol
- Secure VANET MAC protocol for DSRC applications
- Group based secure source authentication protocol
- Security protocol for vehicular distributed system

The advantages of the protocols are:

- The protocols ensure data integrity, reliability, and non-repudiation.
- The protocols are robust and can handle various security threats.
- The protocols induce little performance loss on the vehicular infrastructure.
- The protocols address the major requirements of VANETs, namely: efficient use of spectrum, minimization of packet delay, as well as authentication and prioritized delivery of safety messages.
- The protocols provide efficient quality of service (QoS) and robustness against denial-of-service attack.
- The protocols are designed to guarantee the freshness of the messages, privacy and anonymity of the sender.

The disadvantages of the protocols are:

- VANETs possess unique challenges, such as real time constraints, processing limitations, Memory constraints, and requirements for interoperability with existing standards. No currently proposed protocol addresses all these requirements.
- Digital signatures are one of the fundamental security primitives in VANETs because they provide authenticity and non-repudiation in broadcast communication. However, the current broadcast authentication protocols in VANETs are vulnerable to signature flooding: excessive signature verification requests that exhaust the computational resources of victims.

Among all the protocols studied, “A Security Protocol for Vehicular Distributed Systems” has the maximum advantages and minimum disadvantages.

VII. CONCLUSION

Vehicular ad hoc networks (VANETs) have great potential to improve road safety, traffic congestions, and fuel consumption, as well as increase passenger convenience in vehicles. But because they use an open medium for communication, they are exposed to security threats that influence the reliability of these features. In this paper we have briefly reviewed the characteristics, challenges security protocols and applications of the vanets.

FUTURE WORK

In future we will be modifying an existing protocol for securing communication in such environments. The security protocol considers the particular characteristics of VANETs. It ensures data integrity, reliability, non-repudiation, preserves privacy and links a message to a particular time and place the message was generated. The security protocol will be implemented in a VANET simulator and we present evaluation results of its capability to handle a wide range of attacks that are characteristics to such environments. Researchers are developing new secure vanet protocols and a lot more work can be done in this field.

REFERENCES

[1] Catalin Gosman, Ciprian Dobre, Valentin Cristea,“A Security Protocol for Vehicular Distributed Systems”, 12th international conference on symbolic and numeric algorithms for scientific computing (SYNASC), 2010, IEEE digital library.

[2] Farzad Sabahi, 2011, “The Security of Vehicular Adhoc Networks”, Third international conference on computational intelligence, communication systems and networks (CICSyN), 2011, IEEE digital library.

[3] Ghassan Samara, Wafaa A.H. Al-Salihy, R.Sures, “Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)”, National Advanced IPv6 Centre, University Sains Malaysia.

[4] Gongjun Yan, Gyanesh Choudhary, Michele C.Weigle, Stephan Olariu, “VANET’ 07 Poster: Providing VANET Security through Active Position Detection”, Department of Computer Science, Old Dominion University, Norfolk, USA.

[5] Jason J.Haas, Yih-Chun Hu and Kenneth P.Laberteaux, “Real-World VANET security protocol performance”, Globecom 2009, IEEE digital library.

[6] Surabhi Mahajan, Prof. Alka Jindal, “Security and Privacy in VANET to reduce Authentication overhead for Rapid Roaming Networks”, International Journal of Computer Applications (0975-8887), Volume 1-No.20, February 2010.

[7] Rajani Muraleedharan and Lisa Ann Osadciw,”Cognitive Security Protocol for Sensor Based VANET Using Swarm Intelligence”, Asilmore,pp.288-290,2009.

[8] Qing Xu, Tony Mak, Jeff Ko, and Raja Sengupta,”Vehicle-to-vehicle Safety Messaging in DSRC in VANET ‘04’, Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pages 19-28, New York, NY,USA, 2004, ACM Press.

[9] H.Deng, W.Li, and D.Aggarwal,” Routing Security in the Wireless Ad Hoc Networks”, IEEE Communications Magazine, Vol. 40, NO. 10,2002.

[10] Shankar Yanamandram, Hamid Shahnaseer,” Analysis of DSRC based MAC protocols for VANETs”, International conference on ultra modern telecommunications and workshops, pp.1-6,2009, IEEE digital library.

[11] C.K.Toh," Ad Hoc Mobile Wireless Networks: Protocols and Systems", Prentice Hall Englewood Cliff, NJ 07632, 2002.
[12] Catalin Gosman, Ciprian Dobre, Valentin Cristea," A Security Protocol for Vehicular distributed systems", 12th international conference on symbolic and numeric algorithms for scientific computing (SYNASC), pp.321-327, 2010,IEEE library.