ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

A Robust, Flexible, and Efficient authentication Key Exchange Protocol for VANET Based on Law Executor

[1] Venkatamangarao Nampally, [2] Dr. Mamillapally Raghavender Sharma

[1] Research Scholar, Department of Computer Science, University College of Science, Osmania University, Hyderabad, TS, India

[2] Assistant professor, Department of Statistics, University College of Science, Osmania University, Hyderabad, TS, India

Abstract: currently no proposed work addresses all of the requirements for message and entity authentication in VANET system. This paper focuses on the authentication scheme which is based on number theory as it plays a vital role in network system communication. In this paper, we discuss a novel, robust and efficient authentication protocol which is based on number theory principles involving LE using novel key sharing scheme employing probabilistic random keys which allows an OBU to update its compromised keys. VANET is a type of Ad hoc network in which vehicles act as nodes for exchanging all type of information. Here, we experiment the NTBS with LE for obtaining Authentication mechanism for transferring and receiving resources of network. In VANETS the primary and crucial components of security are recognized as node authentication, message integrity, data availability, non-repudiation, and data confidentiality. From above node authentication mechanism is crucial challenge in VANET. So, we concentrate and invent a authentication protocol.

Index Terms— Ad hoc network, VANET, LE, NTBS, Authentication, TTRs, QoS, ASTM, TPD, ELP

1. INTRODUCTION

Technically speaking, A network is collection of four components in Ad hoc network as <N, *l*, R, M>. Here N means number of available nodes in that network, *l* is side of square of operation of that network, R means Uniform transform range of nodes, and M is mobility model which will be established in the network. Mobility model means free movement of vehicular node in the network. This depends on speed of vehicular nodes which are available in the network [1]. According to many surveys in U.S each year more than 7 million crashes are being occurred. Vehicular nodes maintenance on road costs more than $300 million dollars and at the same time traffic jams produce tremendous waste of time and wastage of fuel. So, in order to reduce the accident rate, it is needed to make that vehicle can communicate intelligently.

So, safety is the main and no.1 concern in DOT (Department of Transportation) of U.S nation. Safety is required not only in U.S nation but also in many other nations where VANET has developed. VANET means Vehicular Network which is a type of ad hoc network and modified version of MANET. An ad hoc network is self-configuring and Spontaneous creation of network devices forming arbitrary topology with P2P (Peer-to-Peer) connection [2]. Simply, it is a temporary network composed of mobile nodes fitted with a relay function. In this network, every node acts as a router and host because there is no dedicated centralized administration separately.

In this network a router or host is mandatory equipment to send and receive messages and all type of information related to that network. With fitting various sensors within a vehicular node, provides continuous monitoring of driving information such as speed, position, and direction. VANET enables the provision of services to improve the passenger's safety and decreases the traffic congestion. Moreover, VANET can achieve secure communication in ubiquitous computing environment and enhance the communication procedure using TTRs (Transitive Trust Relationships) concept [3].

Ad hoc network

The primary and ultimate goal of ad hoc network is increasing the mobility and flexibility in that network area. This network uses nodes to enable communication within some specified wireless transmission. Ad hoc

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

network would be classified as infrastructure based and infrastructure less networks. Infrastructure based ensures centrally controlled equipment [4]. The representing of layered architecture of Ad hoc network uses mainly four layers.

- Application layer: provides security
- Transport layer : provides QOS (Quality of Services)
- Network layer : provides routing
- Physical layer: provides power control

Routing algorithm plays very tremendous role in ad hoc networks and its sub-networks. Routing is the way of path of packets which are sent and receive for communication.

Ad hoc network main characteristics

- Self configuring network
- Dynamic topology
- No centralized administration
- Peer-to-Peer connection
- Every node acts as a router
- Power constraint operation

Types of ad hoc networks

Geographically, ad hoc network is available with two types of networks: one is MANET and Second is VANET. Difference between MANET and VANET is very simple: both networks have same characteristics in many cases. MANET is a temporary network which will be created for a special purpose mechanism. But VANET is highly dynamic topology and no power constraint. And also VANET is sub group of MANET.

We can differentiate MANET with VANET in terms of topology, routing mechanism and energy constraint [5]. VANET is very high dynamic topology than MANET; it requires fast routing algorithms than MANET, and in VANET, no power constraint problem occurs like MANET.

Applications of ad hoc network

An ad hoc can be applicable in many environments. But main applicable are:

- Home networking
- PAN (Personal area network)
- Bluetooth
- Conferencing
- Embedded computing applications

Vehicular Ad hoc Network

It is new technology in which vehicle are connected with each other in an ad hoc manner to form a wireless network. In other words, it is known as assortment of vehicular nodes and modified version and a sub-group of MANET. Motivation for VANET is lack of inter-vehicular communication.

If communication exists within vehicular node with tremendous sensing devices available in that vehicular node: then this communication is treated as intra-vehicular communication whereas communication among vehicular nodes in whole network is termed as inter-vehicular communication. It uses moving vehicles as nodes and transmits the communication among nodes in network within some range specified by the protocol used [6].

It provides any time, any where access environment. Its topology changes very frequently. Main benefit of VANET is it increases traveler safety and provides comfort services along with entertainment services very well in emergency situations. In this network hello messages propagate periodically are called beacons. Objectives of VANET are:

- Increases traveler safety providing good mobility model along with flexibility in network.
- Providing more efficient driving with GPS (Global Positioning System) and DGPS (Dynamic GPS)
- By letting the driver knows about traffic conditions in all conditions.
- Provides services with entertainment and infotainment.

In VANET environment, main components available are:

- OBU (On-Board Unit): it is a monitoring sensing device which monitors all types of operations in network communication. It is responsible for showing what is going on in communication mechanism. It is like heart of VANET system environment. Without this we cannot precede further operations in VANET. In receiving or sending information in the form of messages it uses many modern technologies like 3G, 4G/LTE. OBU enable vehicular nodes not only communicate with each other but can also communicate with dedicated infrastructure by deploying modern mechanisms or algorithms in network.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

- RSU (Road Side Unit): These are infrastructures deployed on road sides to provide services to its network users. Road Side Infrastructure allows vehicular nodes communicate more nodes simultaneously. It is responsible for providing the internet service and to provide communication facility among vehicular nodes. Moreover, it receives internet access from AS and provides internet access service to OBUs within specified range.
- AS (Authentication Server) : Its important functionality is providing internet access to vehicles directly or indirectly, providing services through communication by using RSU, and storing the key values i.e. It is responsible for not only the Authentication keys but also other keys in network environment.

In VANET environment a vehicular node plays vital role in obtaining, receiving, and sending communication. Some times OBU and vehicular nodes are used interchangeably. VANET allows us to categorize the vehicles into three types in order to provide best facilities to its users i.e. drivers as well as passengers.

Vehicle can be categorized into three types in VANET are: MV (Mistrustful Vehicle), TV (Trustful Vehicle), and LE (Law Executor). From above list, LE is very important in VANET system environment. It is a public transportation vehicle which provides authentication to nearby vehicle. And also it generates secure keys for authentication. If authentication mechanism will be established successfully among vehicles then it is called trustful.

Technically, vehicles which are successful in authentication process are termed as TV otherwise deemed to be MV. A MV is a vehicle either unsuccessful authentication procedure entity or normal vehicle entity. To participate in network communication with other vehicles a MV should be authenticated. A TV can act as temporary LE means it can authenticate near by vehicle within some specified range and distance.

VANET authentication

In VANET, It is necessary that privacy should be protected for driver and passenger valuable information when they involved with the network. Privacy protection in VANET has always been a research hotspot, especially the issue of authentication. In order to achieve the security of VANET and its applications, (mainly in safety related applications): it is very crucial to authenticate transmitted messages and identities of their senders. Otherwise, any unauthorized vehicular node could disseminate bogus message which may cause serious damage to drivers, passengers as well as pedestrians.

To authenticate not only it but also other vehicular nodes, commonly vehicular nodes have to maintain and follows key exchange mechanism based on some technique which will be stored in TPD (Tamper Proof Device) on a vehicle [7]. A TPD also provides separate service to save secure information in a different location itself.

Let's try to understand clearly what the authentication is and what the authorization is. Authentication is the process of determining whether users are who they claim to be whereas authorization determines what users can access and cannot access. For best example: when you want to travel in a flight then at airport you have to show your ID to authenticate your identity so that authorities can authorize you to board the flight.

- ***What does VANET provide***
  - Warnings
  - Good traffic and road conditions
  - Safety
  - Efficiency
  - Local information (GPS)
  - Entertainment with infotainment services

- ***Communication standards***

In VANET, communication will be possible using communication standards. Communication approaches will be possible in two ways: communication using dedicated infrastructure and communication using cellular systems [8]. ASTM (American Society for testing and materials) and IEEE (the Institute of electrical and Electronics Engineering) are responsible for propose standards for VANET system.

In 2002 ASTM proposes a protocol DSRC (Dedicated Short Range Communication) for VANET and thereafter it has been migrated to IEEE for further enhancement. Mainly, VANET communication will be provided by two protocols: WAVE (Wireless Access in Vehicular Environment) and DSRC. WAVE uses IEEE1609 series of standards and DSRC uses IEEE 802.11 family of standards. FCC (Federal Communications Commission)

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

allocated 5.9 GHz (5.850-5.925 range) ISM (Industrial Scientific and medical) band.

FCC regulates interstate and international communications by using television, wire, radio, cable and satellite in all 50 states, the places of Colombia and U.S territories and the ISM radio bands are parts of the radio spectrum reserved internationally for industrial, scientific, and medical purposes other than telecommunications. In particular, IEEE 802.11p standard defines the MAC (Medium Access Control) and PHY (Physical) layers whereas 1609 series defines multichannel operation [9].

For multichannel operation, it is specified to use the CCHs (Control Channels) for safety operations and SCHs (Service Channels) for commercial operations. Furthermore, VANET uses J2735standard for defining message sets, data frames and elements which are used for communication. And SAEJ2945 standard is used for safety applications. In working of DSRC, first a RSU announces applications to OBU 10 times per second. Then OBU listens on channel 172 and executes safety application first if available then switches other channels which provide non-safety applications, for executing non-safety applications. At last it returns to channel 172 and starts listening again [10].

- ***VANET applications***

.Mainly, VANET applications are categorized as safety and non-safety applications. Moreover, there are plenty of applications which can be available in safety related such as collision avoidance, automatic driving and traffic navigation and infotainment. Besides these, some applications are listed below:

- Collision warning
- Line change warning
- Intersection collision warning
- Approaching emergency vehicle
- Rollover warning
- Work zone warning
- Coupling/decoupling
- Electronic toll collection
- Traffic control services
- Automatic driving control
- Safety control services
- Access of internet
- Infotainment services
- ***Unique characteristics of VANET***

The unique characteristics of VANET differ from MANET. These unique characteristics are:

- High mobility and very high dynamic topology
- No significant power constraint
- Frequent exchange of information with periodic update
- Unbounded network size
- Dynamic and geographical constraint
- Better physical protection
- Time-sensitive data exchange with large scale

The remainder of this paper is organized as follows. Section II describes state of the art of network. And section III explains methodology which explains about the basic idea of our proposed authentication protocol and also simulation tools used for see the animation of network. Section IV summarizes the experimental results. At last we have given references which are used in this paper.

STATE OF THE ART

Function of literature

There are plethora of publications available for privacy, security but not available for authentication based on key exchange. None of the published solution guaranty utmost security with authentication [11]. Providing the security feature with authentication mechanism is not possible in ill-defined network, because both do not combine in any condition [12]. In authentication usage of symmetric key makes non repudiation more difficult in some times [13]. With modern technological advancement in wireless networking and software development, VANETs have made a tremendous development in recent years. By introducing and using ELP (Electronic License Plates) that is unique identification in network [14] proposed a different perspective for VANET security focusing on privacy position issues. SEVECOM (Secure Vehicle COMmunication) feature aimed to define a consistent and future proof solution to the problem of VANET security focusing on [15]. SEVECOM will focus on communications specific to road traffic. In [16] described new traffic security features with mobility models. Block-burst-based multi-hop protocol for VANET system is proposed for communication [17]. [18] provides a collision avoided mechanism in VANET communication

ISSN (Online) 2394-6849

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 7, Issue 8, August 2020

scenario.In [19] author presented a novel protocol for secure communication in VANET system environment based on number theory.

METHODOLOGY

Authentication is the process of verifying who user is and authorization is the process of verifying what they have access to. The authentication mechanism follows schemes in four categories mainly. They are: key exchange scheme, cryptographic techniques, digital signatures and message verification techniques. Here we concentrate on first scheme which is key exchange scheme. To address the range of needs within VANET system environment, we propose a new authentication protocol which is based on number theory with involving LE with random key exchange. In order to achieve general authentication and to make it use in secure communication among nodes of VANET system, we have proposed Number Theory Based Secure (NTBS) clustering protocol method for achieve authentication using LE, and key exchange. Before a vehicle can join in a VANET system environment, its OBU must be authenticated by an LE. If the authentication process done successfully, the vehicle turns into trustful vehicle (TV), otherwise it is considered as mistrustful vehicle (MV).The MV needs an authentication procedure in order to change its state from MV into TV. Thereafter, the trustful vehicles change the MVs into TVs performing the authentication procedure by using Transitive Trust Relationships (TTRs) concept.

Sub Procedures

The Proposed authentication Scheme involves with the following sub-procedures.

- LE Registration
- NTBS Protocol Key Generation
- Node Authentication
- Transitive Trust Relationships

An LE can give authentication to all nearby vehicular nodes. It is public transport vehicle which gets authentication power from manufacture time. So, it can give authentication permanently any time, any where. Then, after from that it can provide authentication to nearby all vehicles by following specific authentication protocol. Here, Authentication algorithm follows number theory principles involving LE. After, it enhances the communication in network by using TTRs (Transitive Trust Relationships) concept.

Simulation Tools

A simulator is used for predict the behaviour and properties of a network. If in original assets are not available in network then we can show the execution of that specified work in simulator under some conditions. In both conditions, the results are same i.e. when assets are available in specified network and obtain results in simulator are 100% same. We can use many simulators in order to show the execution of specified work. Generally, in every simulator we can input the simulation scripting file written by special language and obtain the results. We show animation in NAM (Network AniMator) and plot the graph with the help of trace file. We design parameters to show the output in real time.

EXPERIMENTAL RESULTS

In this experimental results section we see the results of TTRs in NAM and implementation of proposed authentication protocol in nibble bits. 1 nibble is equal to four bits or half byte. If we use greater than or equal to nibble then authentication mechanism will be vulnerable to malicious attacks. And also we see consequent final animation of authentication protocol in NAM. Although, many researches has been conducted in the area of authentication for VANET, it poses unique challenges such as frequently changing senders.

CONCLUSION

We do the authentication process to challenges the user to validate credentials. Authentication transmits the information through an identity i.e. ID or keys but authorization transmits information through an access token system. Generally authentication process does before authorization. By getting experimental results in NAM, we can conclude that security is directly proportional to the number of bits used in authentication process. In future, we have to develop new methods not only increasing the communication but also increase the communication range and development of cost-effective VANET system without TTRs concept so that effective communication is possible. In future, new protocol mechanism standards will be explored using number theory to avoid disconnection in network because of fast topology. In future, a mechanism developed to avoid frequent disconnection in network because of fast topology based on number theory.

REFERENCES

[1] C. Wu, K. Kumekawa, and T. Kato, "A novel multi-hop broadcast protocol for vehicular safety applications, Journal of Information Proceedings, vol.18, pp.110-124, 2010.

[2] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "Rudimentary Concepts of Cloud Computing Approaches and Future Challenges for VANET", International Journal of Scientific & Research (IJSTR), Volume. **8**, Issue. **9**, **2019.**

[3] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, *"Achieving Fast Communication Mechanism by Using Transitive Trust Relationships for VANET"*, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Vol.**2**, Issue.**5**, pp.**349-355**, **2017.**

[4] Kang kai, Wang Kong, Luo Tao, "Fog computing for Vehicular ad hoc networks:paradigms, scenarios, and issues", in the journal of china universities of posts and telecommunications, vol. 23, issue .2, pp.56-65, april 2016.

[5] An Intelligent Transportation system [ITS] project by Intelligent Consulting Armengol Torres, R.B.S.

[6] B. Yu et al., "Detecting sybil attacks in VANETs", Journal of parallel Distrib. Comput.., vol.73, pp.746-756, 2013.

[7] X.Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications", IEEE transactions on vehicular technology, vol.56, no.6, pp.3442-3456, 2007.

[8] Venkatamangarao Nampally, Dr. M. Raghavender Sharma , "Increasing Information Sharability by Using NTBS Clustering Approach for VANET", IPASJ International Journal of Computer Science (IIJCS), Vol.**5,** Issue.**10**, pp.**001-017**, **2017.**

[9] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "Information Sharing Standards in Communication for VANET", International Journal of Scientific Research in Computer Science Applications and Management Studies (IJSRCSAMS), Vol.**7**, Issue.**4**, **2017.**

[10] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two factor light weight privacy-preserving authentication scheme for VANET", IEEE transactions on vehicular technology, vol.65, no. 2, pp.896-911, 2016.

[11] Dok, H., Fu. H, Echevarira. R, and Weerasinghe.H, "Privacy issues of Vehicular Ad-Hoc Networks ", International Journal of Future Generation Communication and Networking, vol.3, no.1, pp.17-31, 2010.

[12] Choi. H. K, Kim. I. H, and Yoo. J. C, "Secure and Efficient protocol for vehicular ad hoc networks with privacy preservation", EURASIP Journal on Wireless Communications and and Networking, Hindawi Publishing Corporation , Article ID:716794, pp.1.15, 2011.

[13] Studer. A, Bai. F, Beller. B, and Perring. A, "Flexible, Extensible, and Efficient VANET authentication", 6th Conference Embedded security in cars, Hamberg, Germany, pp.22-27, 2008.

[14] Hubaux, J-P, Capkun. S, and Luo. J, "The security and privacy of smart vehicles", IEEE Security and Privacy Magazine, vol.2, issue.3, pp.49-55, 2011.
http://www.sevecom.org/

[15] Stanica et al., " Simulation of Vehicular Ad hoc networks: challenges, review of tools and recommendations", in computer networks, vol. 55, pp. 3179-3188, July 2011.

[16] G. Korkmaz, E. Ekici, and F. Ozguner, "Black-burst-based multi-hop broadcast protocol s for vehicular networks", IEEE Transactions on Vehicular Technology, vol.56, no.5, pp.3159-3167, 2007.

[17] W. Zhu, D. Jao, C. H. Foh, W. Zhao, and H.zhang, "A collision avoidance mechanism for emergency message broadcast in urban VANET", in proceedings of the 83rd IEEE Vehicular Technology Conference, VTC Spring 2016, China, 2016.

[18] Venkatamangarao Nampally, Dr. M. Raghavender Sharma, "*A Novel Protocol for Safety Messaging and Secure communication for VANET System: DSRC",* International Journal of Engineering Research & Technology (IJERT), Volume. **9**, Issue. **1**, **2020.**