ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

VANET (Vehicular Ad-Hoc Networks): Avoidance of Risk Factor in Secure Communication

Manoj Diwakar, CSE Department, DIT University, India
Ajay Kumar, CSE Department, DIT University, India
Dhirender Kumar, MCA Department, DIT University, India
Nitin Thapliyal, CSE Department, DIT University, India

Abstract: ***Recent advances in development of Wireless Communication in Vehicular Ad-hoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular ad-hoc networks are multi-hop networks with no fixed infrastructure. It comprises of moving vehicles communicating with each other. One of the main challenges in VANET is to route the data efficiently from source to destination. Also because of wireless medium it is vulnerable to several attacks. Since attacks mislead the network operations, security is mandatory for successful deployment of such technology. This paper has two parts: first part, introduce an approach to provide secured message transaction in VANET and second part covers the risk management at the time of message transaction in VANET.***

Keywords: **VANET, Public-Key, Digital Signature**

I. INTRODUCTION

The vehicular ad-hoc networks [VANET] is very popular among the networks due to their interesting and promising functionalities like vehicular safety, traffic congestion avoidance, and location based services as shown in figure 1. The main object of the architecture for VANET is Safety driving, Traffic congestion avoidance and Location based services, the vehicle generates a warning message and distributed in to all vehicles in a certain geographical region, potentially using wireless multi-hop communication. The delay control for VANET and data aggregate is an efficient technique for minimizing the redundant data and improve communication efficiency by using adaptive forwarding delay control scheme known as the catch-up scheme [2]. The safe driving and infotainment services on the move can be develop by the usage of hash chaining concept of cryptography [4]. Security and Reliability like road travel collision, traffic congestion, and fuel consumption are overcome by destination making systems which are created by physics, vehicle dynamic and historical data collected from GPS system [5]. Cooperative approach to get self-management to enhanced the privacy and integrity, detecting the nodes and distributing the network operation [6]. For the development of security and privacy the public key infrastructure protocol are used which defines the security requirements and detailed definitions the security requirements and detailed definition of the scheme for the security and privacy by using shared asymmetric keys [7]. In order to decrease the delay in geodynamic group based authentication the symmetric key based cryptography is introduced as group communication by creating groups and maintaining then geodynamic ally by group leader [8].

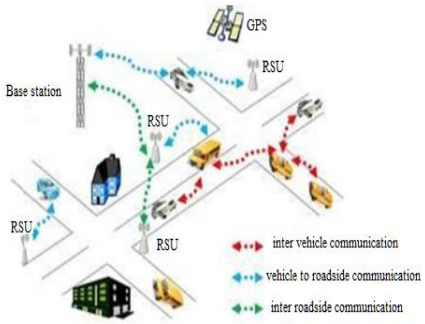

Fig 1: Vehicular Ad-Hoc Network (VANET)

Effective vehicular communication can be done by message authentication scheme which enhance cooperation, privacy, and vehicular communication, a separate edited message authentication scheme is introduce [10]. In the safety driving application, vehicles broadcast safety messages every 300ms [14].The authors propose a promising protocol which let vehicles have to verify message cooperatively by verification of digital signature. However, in order to guarantee efficient cooperation, vehicles have to verify at least twenty –five messages within 300ms which is still a heavy computation burden for the on-board unit (OBU) installed on a vehicle.

II. PUBLIC-KEY CRYPTOGRAPHY APPROACH

Authentication; - Authentication Protocols are used to convince parties of each other's identity and to exchange session keys. They may be one-way or mutual. Central to the problem of authenticated key exchange are two issues: confidentiality and timeliness. To prevent masquerade and to prevent compromise of session keys, essential identification and session key information must be communicated in encrypted form. This requires the prior existence of secret or public keys that can be used for this purpose. The second issue, timeliness, is important because of the threat of message replays.

Digital Signature Standard

A digital signature may be formed by encrypting the entire message with the sender's private key, or by encrypting a hash code of the message with the sender's private key. Confidentiality can be provided by further

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

encrypting the entire message plus signature using either public or private key schemes. It is important to perform the signature function first and then an outer confidentiality function, since in case of dispute, some third party must view the message and its signature. But these approaches are dependent on the security of the sender's private-key. Will have problems if it is lost or stolen and signatures forged. Need time-stamps and timely key revocation.

Digital Signature Schemes

- public key signature schemes
- the private-key signs (creates) signatures, and the public-key verifies signatures
- only the owner (of the private-key) can create the digital signature, hence it can be used to verify who created a message
- anyone knowing the public key can verify the signature (provided they are confident of the identity of the owner of the public key - the key distribution problem)
- usually don't sign the whole message (doubling the size of information exchanged), but just a **hash** of the message
- digital signatures can provide non-repudiation of message origin, since an asymmetric algorithm is used in their creation, provided suitable timestamps and redundancies are incorporated in the signature

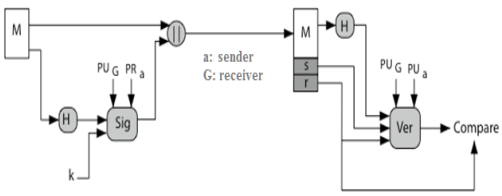

Fig 2: Dss Approach

To create a signature, a user calculates two quantities, r and s, that are functions of the public key components (p, q, g), the user's private key (PR) and public key (PU), the hash code of the message H, and an additional integer k that should be generated randomly or pseudo-randomly and be unique for each signing as shown in figure 2. The signature (r, s) is then sent with the message to the recipient. Note that computing r only involves calculation mod p and does not depend on message hence can be done in advance. Similarly with randomly choosing k's and computing their inverses, a digital signature can be created. At the receiving end, verification is performed using the formulas shown. The receiver generates a quantity v that is a function of the public key components, the sender's public key, and the hash of the incoming message. If this quantity matches the r component of the signature, then the signature is validated. Note that the difficulty of computing discrete logs is why it is infeasible for an opponent to recover k from r, or x from s. Note also that nearly all the calculations are mod q, and hence are much faster save for the last step. The structure of this function is such that the receiver can recover using the incoming message and signature, the public key of the user, and the global public key.

III. PROPOSED ARCHITECTURE

A. PROPOSED FRAMEWORK

The proposed framework uses the algorithm for secure communication of messages, the algorithm are hash and Digital Signature as shown in figure 3. The hash key technique is used because the framework does not need a specific range. Why because the key length is fixed and larger which is defined in the RSU. The nodes are ordinary vehicles on the road that can communicate with each other and RSU's though radio. In a highway scenario RSU are normally away from each other.

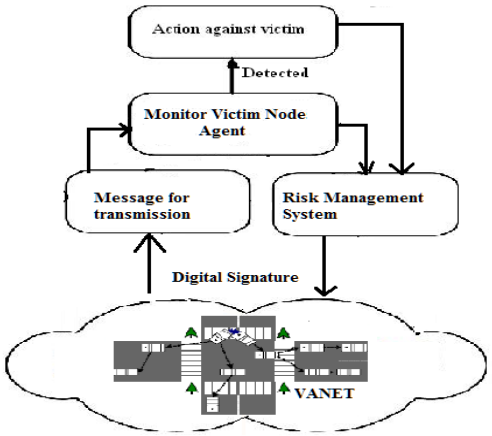

Fig 3: Proposed Framework

A message can be transmitted over VANET but user must ensure that message is authenticate. For authentication, Digital signature concept can be included. For that user's public key and private key should be used and a time-stamp value should be generated for a particular session. As session is finished, user's public key and private key should be destroyed. And acknowledgement should be send to sender as message failed. For a successful transmission, first a message should be appended with digital signature and also encrypted in the same framework. After that it should be verified by session value for secure transmission.

B. RISK MANAGEMENT MODEL

Figure 4 shows the model of risk management. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable Executive Orders, directives, policies, regulations, standards, or guidelines [1].

- Implement the security controls
- Describe how the controls are employed within the information system and its environment of operation.
- Assess the security controls using appropriate assessment procedures to determine the extent to which the controls

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations.
- Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, and reporting the security state of the system to designated organizational officials.

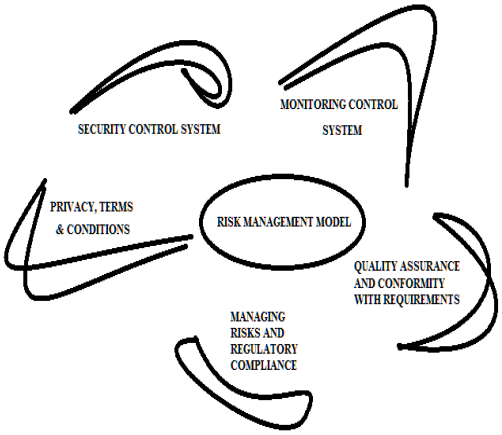

Fig 4: Risk Management Model

IV. SECURITY CONTROL SYSTEM

The following steps are used for security controls:

- Common control-related considerations
- Technology-related considerations
- Public access-related considerations
- operational/environmental-related considerations

Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system [15] [16]. Security controls that can be supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. Security controls that are based on specific assumptions about the operational environment are applicable only if the information system is employed in the assumed environment. For example, certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems. When public access to organizational information systems is allowed, security controls are applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to public access.

V. MONITORING CONTROL SYSTEM

In particular, the organization revisits on a regular basis, the risk management activities described in the Risk Management Framework. In addition to the ongoing activities associated with the implementation of the Risk Management Framework, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls.

- Reconfirm the security category and impact level of the information system.
- Assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.
- Plan for and initiate any necessary corrective actions.
- Consider reauthorizing the information system.

The security plan for the information system is updated to reflect any initial changes to the original plan. A plan of action and milestones is developed for any noted weaknesses or deficiencies that are not immediately corrected and for the implementation of any security control upgrades or additional controls. The authorizing official may choose to conduct a limited reauthorization focusing *only* on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials have sufficient information available from security control assessments to initiate, with an appropriate degree of confidence, necessary corrective actions.

VI. PRIVACY, TERMS & CONDITIONS

The increasing availability of bandwidth allows new combinations and opens new IT perspectives. Our team of world renowned lawyers specialized in Data Protection, Privacy, information technology law and outsourcing agreements develops pragmatic contractual templates that protect the business relationship. Additionally, we help government agencies and companies in data protection notifications for local data protection authorities regarding the collection and use of personal identifiable information. We have extensive experience in dealing with such issues:

- Sensitivity of entrusted information.
- Localization of information and applicable law
- User access rights to information
- Cross border and third party data transfers
- Externalization of privacy
- Workable contractual rules with privacy implications

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

VII. MANAGING RISKS AND REGULATORY COMPLIANCE

Risk management framework is one of security assessment tool to reduction of threats and vulnerabilities and mitigates security risks. The risk management industry spans all other industries. A quick internet search shows risk management associated with insurance, banking, financial services, IT, mining, environmental management, human resources, medicine, travel, forestry, asset management, energy, construction, sports, pharmaceuticals; basically risk management spans all of society. Despite this wide-spread referencing, the most common association is between risk and insurance and/or financial services. Issues like:

- Risks are effectively identified and evaluated.
- Risk management processes are both effective and efficient.
- Key risks are appropriately reviewed and reliably reported to those who need to know
- While increasing attention is being paid to improving effectiveness, many companies are looking both to improve efficiencies and reduce the costs of effective governance, risk, and compliance activities.

VIII. QUALITY ASSURANCE AND CONFORMITY WITH REQUIREMENTS

By providing approach Quality management systems, quality assurance and verification of conformity we tackle these challenges:

- Determining the needs and expectations of customers and interested parties.
- Establishing the quality policy and quality objectives of the organization.
- Determining the processes and responsibilities necessary to attain the quality objectives.
- Determining and providing the resources
- Establishing methods to measure the effectiveness and efficiency of each process.
- Applying these measures to determine the effectiveness and efficiency of each process.
- Determining means of preventing nonconformities and eliminating their causes.
- Establishing and applying a process for continual improvement of the quality management system

IX. CONCLUSION

This paper has addressed, cooperative message authentication, where the participating keys are given priority. In this method, the message is allowed to authenticate by using Risk management system. RSA and digital signature algorithm is used for message authentication. Risk Management system also create a trust between node to node by using reauthorizing the information system, public access-related considerations, system component allocation-related considerations and Defined Security Control Parameters. Secure message transaction and Risk management system provide safety and security in VANET.

REFERENCES

[1] http://csrc.nist.gov/publications/PubsSPs.html#800-53.

[2] Youg Hao, Yu Cheng ,Chi Zhou and Wei Song, "A Distributed key management framework with cooperative message authentication in VANETs" IEEE Journal on selected areas in communications, vol.29, no.3, march 2011.

[3] Bo Yu, Cheng-Zhong Xu,and Minyi Guo, "Adaptive forwarding delay control for VANET data aggregation"IEEE Transaction vol .23,no.1,january2012.

[4] Irshad Ahmed Sumra, halabi hasbullah, Jamalul-Iail Ab Manan "VANET Security Research and Development Ecosystem "International conference 2011.

[5] Vighnesh N V,N Kavita, Dr.Shalini R.Urs "A Novel Sender authentication Scheme Based On Hash chain For Vehicular Ad-hoc Networks " IEEE Transaction 2011.

[6] Vineetha Paruchuri, "Inter-vehicular communications: Security and reliability issues" International conference2011.

[7] J.Molina-Gil, C.Caballero-Gil, and p.Caballero-Gil "Cooperative Approach to Self-managed VANETS" International conference 2010.

[8] Ali Osman Bayrak, Tankut Acarman "S3P: A Secure and Privacy Protecting Protocol for VANET" International conference 2010.

[9] Marshall Riley, Kemal Akkaya and kenny Fong "Delay-efficient geodynamic group-based authentication in VANETs"International conference 2010.

[10] Cristina Gil,Leticia Gonzalez,Neftis Atallah,Juan Antonio Abanades,Nicolas Jean Leconte, " Self-Recusation Protocol for Blockage of Misbehaving Applications in Vehicular Networks" International conference 2010 .

[11] Chenxi Zhange ,Xiaodong Lin,Rongxing Lu, "An efficient message Authentication scheme for vehicular communications" IEEE Transaction on vehicular technology", vol.57, no.6, nov 2008 .

[12] Y. Hao, Y. Cheng and K. Ren, "Distributed key management with protection against RSU compromise in group signature base VANETs," In Proc.IEEE Globecom, New Orleans, Nov., 2008.

[13] S. Park and C.C.Zou, "Reliable traffic information propagation in vehicular ad-hoc networks," IEEE Sarnoff Symposium, Apr. 2008.

[14] Sampigethava, L.Huang, M.Li, R.Poovendran, K.Matsuura and K.Sezaki, "AMOEBA: Robust location privacy scheme for VANET,"in IEEE J. Sel. Areas Commun., vol. 25,no. 8, pp.1569-1589, 2007.

[15] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007 .

[16] B. Xiao, B. Yu and C. Gao, "Detection and localization of sybil nodes in VANETs," in Proc. ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, 2006.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 1, July 2013

AUTHOR'S PROFILE

Manoj Diwakar received B.Tech in Computer Science & Engineering from Dr. R. M. L. Awadh University, U.P. India in 2003 and M.Tech in Computer Science & Engineering from MITS Gwalior, M.P. India in 2006. Currently He is an Assistant Professor at Computer Science & Engineering Department, DIT University, Dehradun India. His research interests include Image processing, Information Security, Cellular Automata. He has published more than 15 research papers in various national and international journal having 8 years teaching experience.

Ajay Kumar received B.E. in Information Science & Engineering from SJCE Mysore, VTU Karnataka, India in 2005 and M.E. in Software Engineering from BIT Mesra Ranchi, India in 2007. Currently He is an Assistant Professor at Computer Science & Engineering Department, DIT University, Dehradun India. His research interests include web technology, security, and wireless network. He has presented many research papers in international conference and published in international journal having total 6 years industrial and teaching experience. He is a life member of ISTE & CSI.

Dhirender Kumar received Bachelor of Science in Physics, Master of Science in Physics from Delhi University in 2003 and 2005 respectively. He also received Bachelor of Education (B.Ed) from GGSIP University, Delhi in 2007. Subsequently he received M.E. in Computer Technology & Applications from Delhi College of Engineering, Delhi India (now DTU Delhi) in 2009. Currently He is an Assistant Professor in the department of computer application, DIT University, Dehradun India. His research area includes Multimedia System, Soft Computing, and Computer Organization. He has presented few research papers in IEEE international conference having total 5 years teaching experience.

Nitin Thapliyal received B.Tech in Information Technology from H.N.B.garhwal University, Srinagar, Uttarakhand, India in 2009 and M.Tech in Computer Science & Engineering from UTU Dehradun India in 2011. Currently he is an Assistant Professor in the department of Information Technology, DIT University, Dehradun India. His research field includes Green Database, Mobile Computing, Operating System. He has published 6 research papers in reputed international journals having 4 years teaching experience.