ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

Vehicular Ad Hoc Networks: An Approach to Provide Secure and Trusted Data

Paridhi Singhal, Manoj Diwakar, Manish Mahashi

Abstract*— A Vehicular Ad-Hoc Network (VANET) facilitates communication between vehicles and infrastructure. The aim of VANETs is to enable moving vehicles by providing safety and non safety messages. Due to the characteristics of VANET, the existing relative positioning techniques developed initially for Ad hoc or sensors networks are not directly applicable to vehicular networks. Vehicle-to-vehicle communications is used to collect data from neighborhood vehicle with the help of sub-VANET. In this paper we assess how can data providers earn their person's trust and provide the security, when a third party is processing sensitive data in a remote machine located in various location in the cities? A concept of utility of vehicle's data has been represented to provide the various services to the peers. Emerging technologies can help address the challenges of Security and Trust in data computing.

***Keywords*- Data Computing, Risk Management, Access Control Model, Quality Assurance.**

I. INTRODUCTION

Vehicular Ad hoc Network (VANets), considered as a subclass of mobile Ad Hoc networks (MANets), is a promising approach for future Intelligent Transportation System (ITS). These networks are characterized by highly mobile nodes and potentially large network. The nodes can recharge frequently, they are constrained by the road and traffic pattern. Until recently, road vehicles were the realm of mechanical engineers. But with the plummeting costs of electronic components and the permanent willingness of the manufacturers to increase road safety and to differentiate themselves from their competitors, vehicles are becoming "computers on wheels", or rather "computer networks on wheels". For example, a modern car typically contains several tens of interconnected processors; it usually has a central computer as well as an EDR (*Event Data Recorder*), reminiscent of the "black boxes" used in avionics. Optionally, it also has a GPS (*Global Positioning System*) receiver, a navigation system, and one or several radars. Due to its perceived open nature, VANET raises strong security, privacy and trust concerns, namely:

- How data safely stored and handled by VANET
- How data privacy being managed adequately?
- Are data providers adhering to laws and regulations?
- How is business disruption or outage kept to its minimum?
- Are data providers sufficiently protected against cyber-attacks?

Data interchanged over VANETs often play a vital role in traffic safety. Consider a peer, who reports the roads on his path as congested with the hope that other peers would avoid using these roads, thus clearing the path. Therefore one important issue among others that may arise in VANETs is the notion of trust among different peers. The goal of incorporating trust is to allow each peer in a VANET to detect dishonest peers as well as malicious data sent by these dishonest peers, and to give incentives for these peers to behave honestly and discourage self-interested behavior.

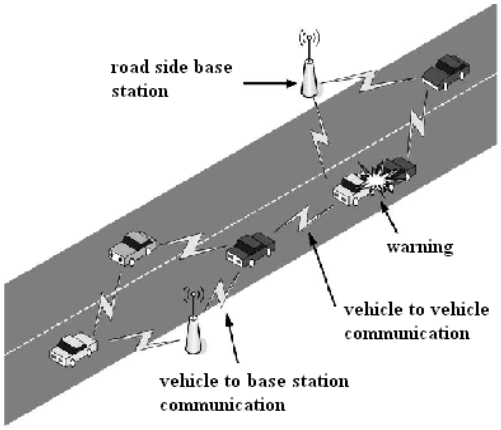

Fig. 1 A VANET Consists Of Vehicles and Roadside Base Stations That Exchange Safety Messages.

VANET share distributed information via the network in the open environment, thus it makes security problems important for us to develop the VANET application [2]. The VANET element derives from a metaphor used for the Internet, from the way it is often depicted in network diagrams. Conceptually it refers to a model of scalable, real-time, internet-based information technology services and resources, satisfying the computing needs of peers, without the peer incurring the costs of maintaining the underlying infrastructure. VANET have many opportunities for enterprises by offering a range of services. It shares massively scalable, elastic resources (e.g., data, calculations, and services) transparently among the peers over a massive network [3]. These opportunities, however, don't come without challenges. VANET has opened up a new frontier of challenges by introducing a different type of trust scenario. Today, the problem of trusting VANET is a paramount concern for most enterprises. It's not that the enterprises don't trust the data providers' intentions; rather, they question VANET capabilities. Yet the challenges of trusting VANET don't lie entirely in the technology itself. The projected benefits of VANET are very compelling both from a peer's consumer as well as a VANET services provider perspective: ease of deployment of services; low capital expenses and constant operational expenses leading to variable pricing schemes and reduced opportunity costs; leveraging the economies of scale for both services providers and peers of the VANET [4]. The gap between

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

adoption and innovation is so wide that VANET consumers don't fully trust this new way of connecting information. To close this gap, we need to understand the trust issues associated with VANET from both a technology and vehicle's perspective. Then we'll be able to determine which emerging technologies could best address these issues.

II. SECURITY CHALLENGES OF VANET

VANET is not secure by nature. Security in the VANET is often intangible and less visible, which inevitably creates a false sense of security and anxiety about what is actually secured and controlled. The off-premises computing paradigm that comes with VANET has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as service providers may have complete control on VANET infrastructure that underpins the services [5]. Accordingly, the various security challenges as shown in Fig-2, related to VANET are worth of a deeper attention and can relate to many different aspects.

Fig. 2 Security Challenges of VANET

A. Cryptographic Authentication

VANET peers typically have no control over the vehicles used and there is an inherent risk of data exposure to third parties on the data or the data provider itself. Some policies are:

- Whether there exists a Data security policy, which is approved by the management, published and communicated as appropriate to all.
- Whether it states the management commitment and set out the organizational approach to managing data security.
- Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.
- Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.

B. Data Security Infrastructure

The VANET architecture requires the adoption of identity and access management measures. Some issues:

- Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within area.
- Whether there is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.
- Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.
- Whether there is a management authorization process in place for any new information processing facility. This should include all new facilities such as hardware and software.
- Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators were maintained to ensure that appropriate action can be quickly taken and advice obtained, in the event of a security incident.
- Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.

C. Source Location

To access the source location some challenges:

- Whether risks from third party access are identified and appropriate security controls implemented.
- Whether the types of accesses are identified, classified and reasons for access are justified.
- Whether security risks with third party contractors working onsite was identified and appropriate controls are implemented.
- Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards.
- Whether security requirements are addressed in the contract with the third party, when the organization has outsourced the management and control of all or some of its information systems, networks and/ or desktop environments.

D. Virtualization and Grid Technologies

The virtual network essentially implements shared and coordinated task-spaces, which coordinates the scheduling of jobs submitted by a dynamic set of research groups to their local job queues [6]. Virtualization and grid technologies expose VANET infrastructures to emerging and high-impact threats against hypervisors and grid controllers.

E. Local Sensors

The VANET architecture requires the adoption of identity and access management measures. When data are trusted to a third party especially for handling or storage within a common network environment, appropriate precaution must be in place to ensure uninterrupted and full control of the data owner over its data. Position is a key

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

piece of information in vehicular ad-hoc networks (VANETs), and the use of radar will substantially augment the amount of trust that can be given to the received position information. The goal is to achieve local security by using onboard radar to detect neighbors and to confirm their announced GPS coordinates. Global security is achieved by exchanging packets among cell members and verifying neighboring vehicles' positions using oncoming traffic. Each vehicle generates information about the state of the traffic based on both what is seen and what is received from other vehicles in the system. This technique will improve security in VANETs by preventing malicious peers from falsifying their position information.

F. Infrastructure Validation Security

Although traditional searchable encryption schemes allow peers to securely search over encrypted data through keywords, these techniques support only Boolean search, without capturing any relevance of data files [7]. General purpose software, which was initially developed for internal use, is now being used within the virtual environment without addressing all the fundamental risks associated to this new technology. As with most technological advances, regulators are typically in a "catch-up" mode to identify policy, governance, and law [8]. Migrating onto a VANET may imply outsourcing some security activities to the Data provider. This may cause confusion between data provider and peers regarding individual responsibilities, accountability and redress for failure to meet required standards. Means to clarify those issues can be contracts, but also the adoption of policies, "service statements" or "Terms and Conditions" by the data provider, which will clearly set forth obligations and responsibilities of all parties involved. Currently there is still a lack of generally-admissible VANET standards at worldwide level. The consequence of this is uncertainty regarding the security and quality levels to be ensured by data providers, but also provider's dependency for peers given that every provider uses a proprietary set of access protocols and programming interfaces for their VANET services.

III. TRUST CHALLENGES OF VANET

The Security challenges discussed above are also relevant to the general requirement upon VANET suppliers to provide trust worthy services. If data providers find adequate solutions to address the data privacy and security specificities of their network model, they will have met in a certain way the requirement of offering trusted services. Yet, there are a few other challenges which, if tackled properly, would enhance peer's confidence in the application of VANET and would build peers trust in the VANET service offerings fig-3.

A. Trust in Infrastructure

One key to providing a trusted infrastructure is by provisioning a protected execution and content environment. Trusted VANET Group (TVG) and related open specifications and development efforts for data providers, and pervasive devices to provide a hardware "root of trust" that can leverage up the stack. Bindings that support end-to-end trust chains for web services and grid transactions. It is based upon use of certificates based upon central authority. Also needs presence of road-side units. TVG-enabled integrity reporting provides several capabilities for the trust framework to enable *trust in infrastructure*, including

- Authentication of system configuration change origins.
- Assertion of system platform identity and configuration.
- Assertion of origin of execution image.
- Verification of execution context.
- Secure destruction of execution context.
- IDS signature verification.
- Signed, verifiable audit records.
- Proof that audit logs were not tampered.
- Validation of service provider.
- Secure content management and distribution.

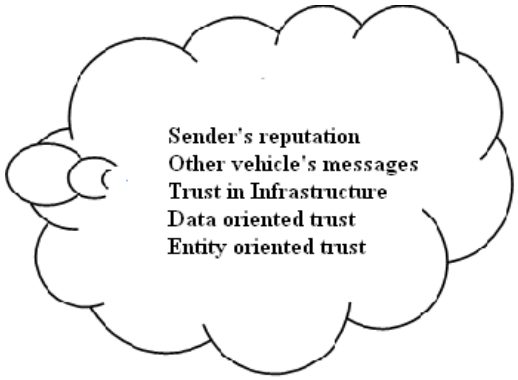

Fig. 3 Trust Challenges of VANET

TVG support also provides a trust basis to support server cluster provisioning, to cover issues such as:

- Do I let this new vehicle into the network?
- Does the vehicle meet the trust requirements?
- Does this system have the proper execution environment to interoperate in the VANET?
- Has the system been tampered? Is the system running as it was originally set up?

B. Data Oriented Trust

The root sometimes is busy with lot of traffic. First analyze the root and make the policy which time is most busy schedule for path. Suddenly changes create the problem to the network.

C. Entity Oriented Trust

VANET cannot guarantee full, continuous and complete control of the vehicles. A trusted entity with expertise and capabilities data owners do not possess can be delegated as an external vehicle to assess the risk of outsourced data when needed [16].

D. Other Vehicle's Messages

Vital information and assets must be assessed and classified based on the consequences of loss, damage, or failure. Assign the appropriate levels of security protection

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

and assess the vulnerability of Manufacturing and Control System Information loss or compromise.

E. Sender's Reputation

All security functions integrated into the process control system must be tested to prove that they do not introduce unacceptable vulnerabilities. Adding any physical or logical component to the system may reduce reliability of the control system, but the resulting reliability should be kept to acceptable levels. Consider immediate investment in research and development activities to accelerate the maturation of the following commercial capabilities.

- Development and acceptance of trust policy languages and trust management/negotiation protocols.
- Development and acceptance of trust inference engines and definition of trust level semantics and assurance standards.
- Development and acceptance of privacy management technology.
- Development and acceptance of trusted identity management solutions that support federation (cross domain entity resolution, credentialing, and access management).
- Development and acceptance of secure development environments.
- Development and acceptance of key management/key exchange systems that can interoperate across trust domains and heterogeneous platforms.

F. An Approach to Provide Secure and Trusted Data

As mentioned before, Trust and non-repudiation are conflicting security goals. On the one hand, vehicle drivers are concerned with the identity and location privacy when involved in VANET applications, such as life-critical message exchanges, congestion avoidance, detour notification, navigation, toll payments, infotainment, *etc*. On the other hand, non-repudiation is necessary for the deployment of VANETs since the law enforcement departments require the vehicle identity to be disclosed for investigating the cause of accidents or crimes, and the trusted network authorities may require the same disclosure for punishing misbehaving vehicles. As Fig-4 shows a model to check verification and validation tor trust into VANET:

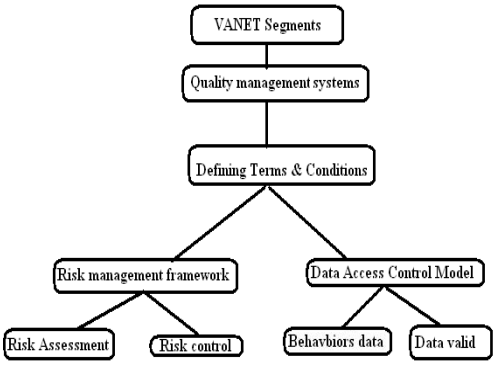

Fig: 4 A Model To Check Verification and Validation

The security program includes developing design models to describe the minimum acceptable recommended practices to be used in constructing a secure system as shown in fig-5. The suggested models:

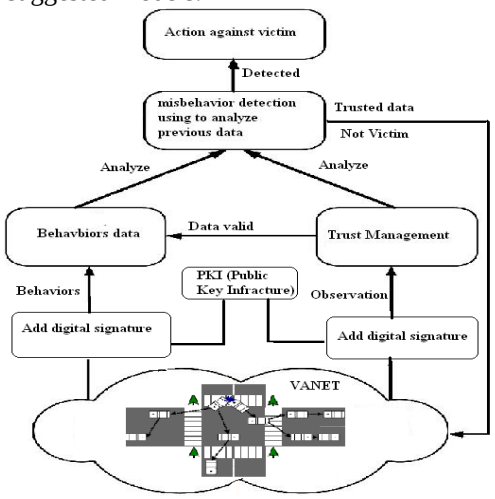

Fig. 5 Steps for Designing and Implementing a Secure Plan

1. VANET Segments

The network comprising of a series of logical and physical layers can be divided into network segments to simplify the approach to designing secure network architecture. The network segments can be further classified as follows:

a) Enterprise Network Segment consisting of enterprise computer systems.
b) Process Information Network Segment consisting of Manufacturing Execution System computers.
c) Control network Segment consisting of controllers and Human Machine Interface devices.
d) Field network Segment consisting of sensors and actuators.
e) Process Segment consisting of pipes, valves, and transportation belts.

2. Data Access Control Model

This describes the recommended practices for accessing Manufacturing and Control Systems. This topic can be further sub-divided into the following topics:

a) Peer Access Management
b) Peer responsibilities
c) Network Access Control
d) Operating System Access Control
e) Application Access Control
f) Monitoring System Access and Use

The potential for security violations by providing greater control over the peer's access to information and resources of multiple devices in a network. We apply to enable secure network information through VANET. Our risk based approach deals with these challenges:

a) How to control vehicles from VANET resources.
b) How to secure the private data.
c) How to use new technologies.
d) How to use and control the data.
e) How to provide security for confidential data.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

f) How to maintain activities for Security models on VANET.

Combining a sound integrated Security and Privacy Management with a clear view on the "to-be" architecture puts us in a unique position to define and execute a comprehensive security and privacy strategy. The design and implementation of security and privacy controls in an integrated manner cover a wide variety of methods that enable new VANET models while controlling the risks:

a) Determine if the strategy focuses on Network Disaster Recovery Planning, which may be limited to restoring VANET infrastructure at an alternative location.

b) Gather management's perception of the most critical business processes (and why), and management's formal/ informal assessment of the effectiveness of the company's ability to resume business operations in the event of a disruption. Determine if the business risks and impacts of unexpected disruptions have been identified and quantified by management.

c) Review the analysis of the organization's previous business continuity tests. Determine if the tests were successful. If not, why not? Identify recurring issues or other potential problem areas and understand the reasons for their existence.

d) Review documentation the organization has developed regarding business continuity processes, policies, standards and service level agreements. Determine if the processes are adequately documented, maintained and communicated to appropriate personnel.

e) Determine if a Business Continuity Plan exists and assess the degree to which it has been defined, documented, tested, maintained and communicated.

f) Determine the degree to which the organization uses software tools to facilitate Business Continuity Management processes.

3. Defining Terms & Conditions

The regulatory landscape for VANET is under continuous change and will still continue to evolve over the coming years. As such, contractual provisioning and Terms & Conditions are key components to seal trust, privacy and service levels in network relationships. The increasing availability of bandwidth allows new combinations and opens new networks [19]. 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:

a) Sensitivity of entrusted information.
b) Localization of information and applicable law
c) Peers access rights to information
d) Cross border and third party data transfers
e) Externalization of privacy
f) Workable contractual rules with privacy implications

4. Risk Management Framework

Risk management framework is one of security assessment tool to reduction of threats and vulnerabilities and mitigates security risks [20]. Despite this wide-spread referencing, the most common association is between risk and insurance and/or financial services. Issues like:

a) Risks are effectively identified and evaluated.
b) Risk management processes are both effective and efficient.
c) Key risks are appropriately reviewed and reliably reported to those who need to know.
d) 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.

5. Approach For Quality Management Systems

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

a) Establishing the quality policy and quality objectives of VANET.
b) Determining the processes and responsibilities necessary to attain the quality objectives..
c) Determining and providing the resources.
d) Establishing methods to measure the effectiveness and efficiency of each process.
e) Applying these measures to determine the effectiveness and efficiency of each process.
f) Determining means of preventing nonconformities and eliminating their causes.
g) Establishing and applying a process for continual improvement of the quality management system

6. Digital Signatures with Digital Certificates

Messages or hashes over the respective messages are signed with the message originators private keys. By using private key, it is guaranteed that the messages originate from nodes holding the required cryptographic key material and the messages have not been altered by intermediate forwarding nodes. The message receiver verifies the integrity and authenticity of the messages, by using the corresponding public keys. The node cannot be impersonated because the node only knows private key. The main advantage is the requirements for digitally signature are very small i.e. the nodes need a possibility to receive or create and store cryptographic key pairs. They need the processing power for creating and verifying message signatures. Main disadvantage is Message forging and denial of service (DoS) attacks are possible. The signatures can be combined with digital certificates provided by a trusted third party. The basic assumption with certificates is that nodes, which include certificates in their messages, are trusted by other nodes that are able to verify the certificates. The distribution of certificates is limited to valid VANET nodes, e.g. communication systems inside vehicles or roadside equipment. Since nodes having obtained a valid certificate can only create new valid active safety messages, this excludes outside attackers. Obviously, this statement holds only, if we can assume that

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

those attackers have no certified keys and if they are unable to extract any from valid nodes. Owner identification might also be used for other legal aspects, not directly linked to active safety application, which is out of scope for this document. The advantages of the digital signature with certificate are:

- The possibility to exclude external attackers from the system,
- The ability to remove malicious or defective nodes.

7. Misbehavior Detection

In this framework, Detection technique is used to distinguish misbehaving nodes from well-behaved nodes. From Figure 5 we may find that there are two key operations in this framework, namely *Behavioral Data and Misbehavior Detection*. Each node initially derives a preliminary view of misbehaving nodes based on the local behavioral data observed by it, and the local behavioral data is exchanged among its neighbors at the same time. Once a node receives for behavioral data from its neighbors, it integrates those behavioral data into its own behavioral data using the previous data of those neighbors. The updated behavioral data will then be fed into the misbehavior detection machine, and an updated view of misbehaving nodes is obtained as the new output of the misbehavior detection machine. Next, the updated view is compared with the previous view, and the updated behavioral data should be broadcast to all neighbors if the two views are not identical. When all the nodes find that there is not any change in their local views when they receive foreign behavioral data, the procedure terminates and all the nodes hold the same global view of misbehaving nodes.

IV. CONCLUSION

In this paper, we have presented a secure and trusted data management scheme for VANETs. Essentially, the difference in propagation speed helps reports encounter each other, and we formulate this issue as a distributed problem where vehicles adaptively choose forwarding delays to make nearby reports have a better chance to meet each other. VANET technology has a great potential in facilitating road transport safety and other vehicle communication's in real scenario. Detecting false information and reducing the chances of attack is the key to the success of VANETs [20]. Radar acts as the eye of the system and allows a vehicle to trust the information received from the vehicles within its range. Our approach is efficient in identifying compromised vehicles and reduces the burden on channel available. Responsible management of personal data is a central part of creating the trust that underpins adoption of VANET services. We have analyzed the trusted computing in the VANET environment. The advantages of our proposed approach are to extend the trusted VANET technology into the VANET environment to achieve the trust form the networks. Furthermore, the less trust an enterprise has in the data provider, the more it wants to control its data—even the technology. However, it's crucial that consumers and providers change their mindsets. Trusting network might differ from trusting other systems, but the goal remains the same. Any new technology must gradually build its reputation for good performance and security, earning vehicles trust over time. We will make more protocol to provide high security for Security management, Identity & access management, Privacy & data protection and application Integrity in the future.

REFERENCES

[1] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems," Comput Commun., vol. 31, no. 12, pp. 2838–2849, Jul. 2008.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.

[3] R. K. Schmidt, T. Kollmer, T. Leinmüller, B. Boddeker, and G. Schafer, "Degradation of transmission range in VANETs caused by interference," PIK—Praxis der Information's verarbeitung und Communication, Special Issue on Mobile Ad-hoc Networks, vol. 32, no. 4, pp. 224–234, Dec. 2009.

[4] G. Durgin, T. S. Rappaport, and H. Xu, "Measurements and models for radio path loss and penetration loss in and around homes and trees at 5.85 GHz," IEEE Trans. Commun., vol. 46, no. 11, pp. 1484–1496, Nov. 1998.

[5] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," in Proc. 3rd Int. Workshop Veh. Ad Hoc Netw., Los Angeles, CA, 2006, pp. 57–66.

[6] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification Approaches for vehicular ad hoc networks," IEEE Wireless Commun., vol. 13, no. 5, pp. 16–21, Oct. 2006.

[7] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Secure Localization algorithms for wireless sensor networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 96–101, Apr. 2008.

[8] L. Lazos, R. Poovendran, and S. Èapkun, "ROPE: Robust position Estimation in wireless sensor networks," in Proc. 4th Int. Symp. Inf. Process. Sens. Netw., 2005, pp. 324–331.

[9] W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly detection for wireless sensor networks," in Proc. 19th IEEE Int. Parallel Distrib. Process. Symp., 2005, p. 41a.

[10] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of Location claims," in Proc. 2nd ACM Workshop Wireless Security, San Diego, CA, 2003, pp. 1–10.

[11] D. Singelee and B. Preneel, "Location verification using secure Distance bounding protocols," in Proc. IEEE Int. Conf. Mobile AdhocSens. Syst. Conf., 2005, pp. 834–840.

[12] Y.Wei, Z. Yu, and Y. Guan, "Location verification algorithms for wireless sensor networks," in Proc. 27th Int. Conf. Distrib. Comput. Syst., 2007, pp. 70–77.

[13] S. C˘ apkun, K. B. Rasmussen, M. Cagalj, and M. Srivastava, "Secure Location verification with hidden mobile base

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

station," IEEE Trans. Mobile Comput., vol. 7, no. 4, pp. 470–483, Apr. 2008.

[14] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 88–95, Apr. 2008.

[15] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, IEEE Std. 1609.2, 2006.

[16] J. P. Hubaux, S. Cˇ apkun, and J. Luo, "The security and privacy of Smart vehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May 2004.

[17] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw., Philadelphia, PA, 2004, pp. 19–37.

[18] B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil Nodes in VANETs," in Proc. Workshop Dependability Issues Wireless Ad Hoc Netw. Sens. Netw., Los Angeles, CA, 2006, pp. 1–8.

[19] G. Yan, S. Olariu, and M. Weigle, "Providing VANET security through active position detection," Comput. Commun., vol. 31, no. 12, pp. 2883–2897, Jul. 2008.

[20] J.-H. Song, V.W. S.Wong, and V. C.M. Leung, "Secure location Verification for vehicular ad-hoc networks," in Proc. IEEE Global Telecomm. Conf., 2008, pp. 1–5.