ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Survey on Vehicular Ad Hoc Networks Security

Gaikwad Priti G.[1], Nilam Patil[2]

M. E Student, Department of Computer Engineering, DYPCOE, Akurdi, SPPU, Pune, India[1]

Assistance Professor, Department of Computer Engineering, DYPCOE, Akurdi, SPPU, Pune, India[2]

ABSTRACT: Recent advances in communication technology are enabling implementation of different types of network in various environments. One such network is Vehicular Ad hoc Network (VANET). It is a challenging subclass of Mobile Ad hoc Network (MANET) which enables intelligent communication among vehicles and also between vehicle and roadside infrastructures. It is a promising approach for the Intelligent Transport System (ITS). There are many challenges to be addressed when employing VANET. It has a very high dynamic topology and constrained mobility which makes the traditional MANET protocols unsuitable for VANET. The aim of this paper is to give an overview of the vehicular ad hoc networks.

KEYWORDS: I2V, VANET, V2I, V2V.

I. INTRODUCTION

With the increasing number of vehicles on the streets, an increasing population of vehicle manufacturers are looking for value-added services for providing their customers with increased safety and information. Toward this goal, Vehicular Communication (VC) is likely to play a major role. VC involves the use of short-range radios in each vehicle, which would allow various vehicles to communicate with each other and with road-side infrastructure. These vehicles would then form an instantiation of ad hoc networks in vehicles, popularly known as Vehicular Ad Hoc Networks (VANETs).

VANETs are envisaged to provide safety-related information, traffic management, and infotainment services. These are the major areas in which applications are likely to develop and find commercial deployment. The first two, that is, safety and traffic management, require real-time information, and this conveyed information can affect life or death decisions. Without security, a VANET system is vulnerable to a number of attacks such as propagation of false warning messages and suppression of actual warning messages, thereby causing accidents. This makes security a factor of paramount importance in building such networks.

VANETs are of prime importance, as they are likely to be among the first commercial application of ad hoc network technology. Vehicles will act as nodes that are capable of forming self-organizing networks with no earlier knowledge of each other. The potential of VANET technology is high with a range of applications being deployed in aid of consumers, commercial establishments such as toll plazas, entertainment companies as well as law enforcement authorities. However, without securing these networks, they would lend themselves to blatant abuse, leading to major problems and immense damage to life and property.

Major applications of VANETs include providing safety information, traffic management, toll services, location-based services, and infotainment. One of the major applications of VANET include providing safety-related information to avoid collisions, reducing pile up of vehicles after an accident, and offering warnings related to the state of roads and intersections.

VANETs can be used to prevent collisions between vehicles by providing information to the driver about whether the vehicle ahead is braking, if the speed is too high or the distance to other vehicles or objects is getting too close. Eight safety applications based on deliberations between government agencies and private industry have been identified in which are traffic signal violation warnings, curve speed warnings, emergency electronic brake lights, pre-crash

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

warnings, cooperative forward collision warnings, left-turn assistance, lane change warning, and stop-sign movement assistance.

Another attractive application is for traffic management, where it is ensured that the vehicles choose the shortest route to a destination, avoid busy and congested areas and also enable traffic diversions in case of traffic jams or accidents. VANETs also have the potential to make various toll services easier to implement by enabling online toll collection as well as to provide information to drivers on cheapest routes between a source and a destination.

Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network for data exchange – to the domain of vehicles. They are a key component of intelligent transportation systems (ITS). The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. VANETs support a wide range of applications – from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances.

II. RELATED WORK

Li, Wenjia et. al.[6] describes an attack-resistant trust management scheme (ART) for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Engoulou et. al.[2] a survey of the security issues and the challenges generated in VANETs. The various categories of applications in VANETs are introduced, as well as some security requirements, threats and certain architectures that are used to solve the security problem. Chen, Ray et. al.[10] describes a trust-based routing protocol that is able to deal with selfish behaviours and is resilient against trust related attacks and also protocol can be effectively trade off message overhead and message delay for a significant gain in delivery ratio. Taha, Sanaa et. al.[11] describes a scheme which involves fake-point- and cluster-based sub-schemes, and its goal is to confuse the attackers by increasing the estimation errors of their RSSs measurements and hence preserving mobile network nodes (MNNs) location privacy.
Lu, Rongxing et.al.[14] describes a DIKE scheme, which gives a privacy preserving authentication technique that not only provides the vehicle users anonymous authentication but enables double registration detection as well.

A. *STANDARDS FOR WIRELESS ACCESS IN VANET*

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows:

1) Dedicated Short Range Communication (DSRC)

It provides a communication range from 300m to 1Km. The V2V and V2R communication takes place within this range. DSRC uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channel is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

2) IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE)

It is also known as IEEE 802.11p. It supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. It contains the standard of IEEE 1609 [7, 8, 9]. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

signal into various narrow band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels [4][5].

III. VANET ARCHITECTURE

VANET architecture employs two types of communication devices: (1) On-board Units (OBUs) and (2) Road-side Units (RSUs). As name suggests, OBU is installed in a vehicle and RSUs are placed on roadside. Each OBU consists of an Event Data Reco rder (EDR), Global Positioning System (GPS) receiver, computing platform, and a radar. GPS receiver provides information about geographic location, speed, direction of movement, and acceleration of a node at specified time intervals. EDR device records the transmitted and received messages. Information stored in EDR can assist in recreation of an accident/emergency situation for subsequent analysis after the occurrence of an event. The computing device is used to take appropriate actions in response to messages received from other nodes. Radar is used for detecting obstacles near the vehicle. Each vehicle also has an omni-directional antenna that the OBU uses to access a wireless channel. An RSU is similar to an OBU in that it has an antenna, computing device, transceiver, and sensors. It is a stationary device mounted on roadside. An RSU may be installed at road intersections or embedded in traffic-light for traffic control. It can be deployed for commercial use also. For example, a restaurant can use an RSU for advertisement of its presence. An RSU may use either directional antenna or omni-directional antenna depending on the type of application [1].

VANET architecture can be divided into three categories:

1) **The cellular/WLAN:** If the infrastructure consists of a cellular gateway or a WLAN or a WIMAX access point, the network will be considered a pure cellular/ WLAN.
2) **Ad hoc:** When no infrastructure is available, the nodes must communicate with one another without relying on an infrastructure. This denotes a pure ad hoc architecture.
3) **Hybrid architectures:** Sometimes, various access points, such as cellular gateways, will be available for communication. In this case, nodes can communicate with these infrastructures or they may also communicate directly with one another. This is called a hybrid architecture [3].

A. *COMMUNICATION TYPES IN VANET*

There are three types of communication to consider in VANETs as shown in the below figure 1:

1) Vehicle-to-Vehicle (V2V):

In V2V communication, vehicles can communicate with each other directly in wireless range or indirectly in a multi-hop mode. For example, when a car using V2V communication encounters a dangerous situation, it communicates with other cars and provides useful information, by suggesting that they avoid the area. Furthermore, V2V communication can be classified into two distinct categories depending on the positions of the sender and the receiver: single-hop and multi-hop. The vehicle's local broadcasts send safety warnings through single-hop V2V communication while non-safety related messages are exchanged through multi-hop V2V communication.

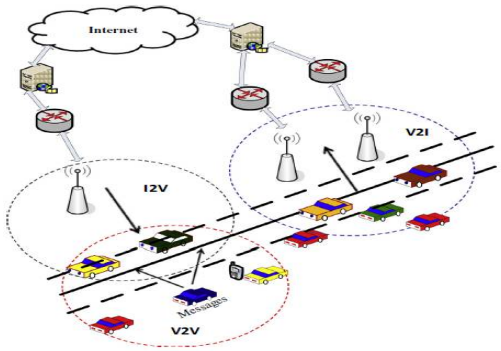

Figure1. System Architecture of VANET.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

2) Vehicle-to-Infrastructure (V2I):

V2I safety message communication refers to the wireless exchange of critical safety and operational data between vehicles and highway infrastructures, which are primarily intended to avoid or mitigate motor vehicle crashes but also to enable a wide range of other safety, mobility and environmental benefits. V2I communication applies to all types of vehicles and roads and it transforms infrastructure equipment into "smart infrastructure" through the incorporation of algorithms that use data exchanged between vehicles and infrastructure elements to perform calculations that recognize high-risk situations in advance, resulting in the production of alerts and warnings for drivers through specific counter measures. One particularly important advance is the ability of traffic signal systems to communicate the Signal Phase and Timing (SPAT) information to vehicles in order to deliver active safety notices and warnings to drivers. An early implementation of the SPAT application can enable near-term benefits from V2I communication in the form of a reduced number or car crashes which in turn show that it may be beneficial to accelerate the deployment.

3) Infrastructure-to-Vehicle (I2V):

In I2V communication, the infrastructure can broadcast diverse messages to moving vehicles regarding road conditions as well as various, traffic information. Wireless Access points (RSU) are used as the network infrastructure. Different protocols can be used: to maximize the throughput for the drivers and the passengers, a Medium Access Control (MAC) protocol, or Wi-MAX (802.16e) provides a reliable end-to-end link, or the Cooperative Strategies for Low-Power Wireless Transmissions Between Infrastructure and Vehicle [2].

IV. SECURITY IN VANET

A. *SECURITY REQUIREMENTS*

The following major security requirements for a VANET:

1) **Authentication** is a major requirement for VANETs. This is simply because it ensures thatcvarious messages are sent by actual nodes and not by a node representing multiple identities or a node impersonating as someone else. Sybil attacks are also avoided if authentication is assured, as a malicious node cannot send messages from nonexistent nodes. This attack can be used by greedy drivers to divert traffic from their routes by simulating a congested road by sending false messages.
2) **Message integrity** is important, as it needs to ensure that the message is not modified in transit. This, coupled with authentication, assures VANET nodes that the messages they receive are not false.
3) **Message nonrepudiation** is required so that sender cannot deny having sent that message. This, however, further exacerbates the identity management issue. Only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends.
4) **Entity authentication** is a property that enables a receiver to ensure that the sender generated a message and is still active in the network. This is required to ensure that a particular message was generated by a sender within a small time interval just before the receipt of the message at the receiver.
5) **Access control** is required to ensure that all nodes function according to the roles and privileges authorized to them in the network. Toward access control, authorization specifies what each node can do in the network and what messages can be generated by it.
6) **Message confidentiality**, though strictly not very essential, in a VANET, can still be utilized when certain nodes want to communicate with each other in private. Such a case can arise when law enforcement vehicles communicate with each other for disseminating private information regarding suspected location of criminals or speed check points.
7) **Privacy** is important to ensure that the user information is not leaked or distributed to parties not authorized to access such information. Third parties should also not be able to track vehicle movements as it is a violation of personal privacy. Therefore, a certain degree of anonymity should be available for messages and transactions of vehicles. Location privacy is also important so that no one should be able to learn the past or future locations of vehicles.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

8) **Availability** is essential to enable VANET services to be operational in the presence of faults and attacks. This implies that VANETs should be resilient to denial of service (DoS) attacks by having alternate means of communication and redundant infrastructure.
9) **Real-time guarantees** are essential in a VANET, as many safety-related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety-related applications such as collision avoidance is met.

B. *CHALLENGES*

For implementing VANET security, it is essential to understand the unique challenges faced in such networks. The major challenges are outlined below:

1) **Tradeoff between authentication and privacy:** To ensure that certain nodes do not impersonate another node, it is essential to authenticate all message transmissions. However, this leads to identification of vehicles from the messages they send. This can enable tracking of vehicles, which most consumers would not like to enable in their systems. Privacy is a major issue in a VANET, because cars are highly personal devices. This has to be balanced with the need for establishing accountability and liability of vehicles and their drivers. This requires an authentication system to be designed that enables messages to be anonymous for general nodes but also enables identification by central authorities in liability-related cases like accidents.
2) **High mobility:** VANETs are characterized by highly mobile nodes which will result in frequent changes in topology and brief connectivity between the nodes. In such situations, VANET protocols cannot be handshake based. Most of the communications are between nodes that have never interacted before and will probably not interact again in future. This characteristic rules out learning- or reputation-based schemes where nodes learn about each other's behavior.
3) **Scale of network:** VANETs are likely to be among the largest ad hoc networks, requiring scalable solutions for an adequate availability and a sufficient performance. This aspect rules out having prestored information about other nodes or distribution of centralized information to all nodes. Also, security and privacy policies will differ from region to region owing to the worldwide deployment of this network. Coordination of such a network will be difficult and would require specific relationships between various regions.
4) **Real-time guarantees:** The major VANET applications are safety related for collision avoidance, hazard warning, and accident warning information. These applications require strict deadlines for message delivery. Any security protocol implemented for VANETs would need to take this into consideration and have low processing and message overheads.
5) **Incentives:** For effective deployment of VANET technology, it is imperative to offer incentives to the involved parties for them to adopt the system. With security the cost and the complexity of this system would further increase. It, therefore, becomes imperative to offer all concerned the correct incentives to adopt this technology and the security being implemented.
6) **Location awareness:** For most VANET applications to be truly effective, certain location-based service is essential. This increases the reliance of the VANET system on GPS or other specific location-based instruments. Any error in these is likely to reflect in the VANET applications.

C. *ADVERSARIES*

Before developing a VANET security system, it is imperative that we understand what type of adversaries would target the system and type of attacks they are capable of launching against the system. In this section, we discuss the probable adversaries and attacks they can launch.

The attackers can be divided into the following general categories:

1) **Selfish drivers:** Even though majority of the drivers in a system would be honest and adhere to the rules, it is natural that some drivers would try to gain specific advantages from the system. In such a situation, the driver may send false information to divert traffic and gain a free path on his route. This is the most common form of attacker, but can easily be put off with a basic authentication system and fear of law enforcement authorities if he believes that there is high probability of getting caught.
2) **Eavesdroppers:** These adversaries would like to collect information about drivers and use this to understand drivers' behaviors and traffic pattern. Also, commercial firms can use this to offer content in infotainment

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

services, when the customer or driver has no interest in getting such services as in mobile networks. Moreover, drivers would not like their personal information to be divulged to third parties.

3) **Teenage hackers:** These adversaries try and hack into any major system that gets deployed publicly. They try to find bugs in the software and cause traffic disruptions just for fun.
4) **Insiders:** These adversaries include persons working in car companies and installing the VC system. They are capable of loading malicious software in cars that could cause immense damage. Also, if manufacturers are entrusted with the responsibility of key distribution, then an insider may create keys acceptable to all users for his cars, that is, compromise private keys of vehicles in a Public Key Infrastructure (PKI) setting.
5) **Malicious attackers:** These attackers could be criminals or terrorists having access to more sophisticated tools and hardware than normal attackers. Criminals may have specific targets for financial gains or would like to carry out personal harm to rivals. Terrorists can use sophisticated technology to disrupt vehicular traffic to cause maximum damage when using bombs or launching gun attacks. These are the most dangerous of attackers and specific measures need to be taken to guard the system against such attacks.

D. *ATTACKS IN THE VANET*

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below:

1) **Impersonate:** In impersonate attack attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network. This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or transport layer vulnerability. This attack can be performed in two ways:
    a. **False attribute possession:** In this scheme an attacker steals some property of legitimate user and later with the use of attribute claims that it is who (legitimate user) that sent this message. By using this type attack a normal vehicle can claim that he/she is a police or fire protector to free the traffic.
    b. **Sybil:** In this type of attack, an attacker use different identities at the same time.
2) **Session hijacking:** Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.
3) **Identity revealing:** Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.
4) **Location Tracking:** The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.
5) **Repudiation:** The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.
6) **Eavesdropping:** It is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.
7) **Denial of Service:** DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways.
    a. **Jamming:** In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.
    b. **SYN Flooding:** In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.
    c. **Distributed DoS attack:** This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.
8) **Routing attack:** Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

a. **Black Hole attack:** In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.
b. **Worm Hole attack:** In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.
c. **Gray Hole attack:** This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two type:
   i) A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.
   ii) The malicious node can drop the packet on the basis of probabilistic distribution.

V. CONCLUSION

The need for safer driving conditions and better traffic management has helped development of smart cars and VANET technology. The potential of VANET applications is immense, considering the large amount of vehicles on the road. However, most of the VANET applications such as safety messages and hazard warning have stringent time requirements and malfunctioning systems and malicious attackers can cause loss of life and injury due to accidents. It is, therefore, imperative to develop a strong security system for VANET. VANET technology has the ability to transform the way vehicles travel from one place to another and offer a whole gamut of services from safety messaging to infotainment. In this paper various aspect of VANET like its environment, standards and network architecture has been discussed. It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET. Security is the major issue to implement the VANET. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data.

REFERENCES

1. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” Journal of network and computer applications, vol. 37, pp. 380-392, 2014.
2. R. G. Engoulou, M. Bellche, S. Pierre, and A. Quintero, “Vanet security surveys,” Computer Communications, vol. 44, pp. 1-13, 2014.
3. Khalid, Osman, et al. “Comparative study of trust and reputation systems for wireless sensor networks.”Security and Communication Networks vol. 6., no.6, pp. 669-688, 2013.
4. M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.
5. Yau, P., and Chris J. Mitchell. “Security vulnerabilities in ad hoc networks.” The Seventh International Symposium on Communication Theory and Applications, pp 99-104, 2003.
6. W. Li and H. Song, “Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 960-969, 2016.
7. Vijayakumar, Pandi, et al. “Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks.” IEEE Transactions on Intelligent Transportation Systems vol. 17, no.4, pp 1015-1028, 2016.
8. Huang, Zhen, et al. "A social network approach to trust management in VANETs." Peer-to-Peer Networking and Applications vol. 7, no.3, pp 229-242, 2014.
9. Douceur, John R. “The sybil attack.” International Workshop on Peer-to-Peer Systems. Springer Berlin Heidelberg, pp. 251-260, 2002.
10. R. Chen, F. Bao, M. Chang, and J.-H. Cho, “Dynamic trust management for delay tolerant networks and its application to secure routing,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200-1210, 2014.
11. G. Rebolledo-Mendez, A. Reyes, S. Paszkowicz, M. C. Domingo, and L. Skrypchuk, “Developing a body sensor network to detect emotions during driving,” IEEE transactions on intelligent transportation systems, vol. 15, no. 4, pp. 1850-1854, 2014.
12. Z. Li, C. Liu, and C. Chigan, “On secure vanet-based ad dissemination with pragmatic cost and effect control, IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 124-135, 2013.
13. S. Taha and X. Shen, “A physical-layer location privacy-preserving scheme for mobile public hotspots in nemo-based vanets,” IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 4, pp. 1665-1680, 2013.
14. R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location-based services in vanets,” IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127-139, 2012.
15. W. Li, A. Joshi, and T. Finin, “Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach,” in 2010 Eleventh International Conference on Mobile Data Management, pp. 85-94, IEEE, 2010.
16. A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, “A data intensive reputation management scheme for vehicular ad hoc networks,” in 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1-8, IEEE, 2006.