Reputation and Plausibility Verification based System for Providing Secure Vehicular Networks

V.S. Saranya
Research scholar,
Department of computer science & engineering,
karpagam university,
Coimbatore - 641006,
tamil nadu, india.

R. Saminathan, PhD
Assistant Professor,
Department of Computer Science & Engineering
Annamalai University
Annamalainagar – 608 002
Tamil Nadu, India.

ABSTRACT
In a Vehicular Ad Hoc Network (VANET), node cooperation in packet forwarding is required for the network to function properly. However, since nodes in this networks usually have limited resources, some selfish nodes might intend not to forward packets to save resources for their own use. To discourage such behaviour, we propose a reputation and plausibility verification based system to detect selfish nodes and isolate them. The trustworthiness of the messages are decided upon using sensors, decision making phase and the previous trust value of the node. In the proposed work, depending upon the kind of reputation information a source is attributed with a sender-based reputation level. Only if the event is thought to be prevalent, the trust opinion generator announces this event to the applications. First a node checks whether the event is in its own detection range. If not the decision is made on either the rule of majority or on the trust levels already assigned to the nodes. In case the event is not prevalent, the proposed algorithm also sends a malicious intent information packet in order to inform the neighbour nodes about the detection of a malicious activity. It is likely to be susceptible to more sophisticated attacks, such as collision attacks, because the situation-oriented reputation level allows long-lasting groups of attackers to manipulate a node's reputation database. The proposed algorithm is better equipped to handle such attacks. It can detect at least such attacks if the node is itself in the detection range. It eliminates attacks pertaining to false event generation completely by utilizing the plausibility of data collected through sensors as well as the trust value of the sending nodes. Reputation value based on mobility is contributed. If the neighbour is having high stability its reputation value is increased..

Keywords
VANET, selfish nodes, plausibility verification, reputation.

1. INTRODUCTION
With the increase in the number of vehicles in the world, the transportation system has become in-efficient. Increasing accidents and traffic jams are leading to loss of millions of lives, money, and time, year after year. This is one of the major problems being faced by the society today. Vehicular ad hoc networks (VANETs) [1] can be used to alleviate the problems of vehicle safety as well as the traffic control and optimization. VANET as proposed consists of mobile hosts equipped with wireless communication devices and Road Side Units (RSUs) and in both Vehicle to Vehicle communication (V2V) and Vehicle-to-Infrastructure (V2I) [3] communication is possible. Dedicated RSUs, because of their required investment in purchase, installation, and maintenance atleast for developing economies, have not been seen as an appropriate possible solution and thus work is still in progress that looks into implementing only V2V without infrastructure to reduce the implementation cost [2]. A robust V2V communication system can help us to create a network where one vehicle can inform other vehicles about various existing conditions like traffic jams, accidents, and implementation of brakes. The security [4] in VANETs is of primary concern since an attacker may try to insert or modify life-critical information. The major attacks in VANETs are message forging, impersonation, packet dropping, black hole, gray hole, worm hole, on-board tampering, and in-transit traffic tampering. Infrastructure-based VANET uses majorly infrastructure for handling security by providing private keys [10] to vehicles at real time. These keys can work well but need full infrastructure support. Storing keys in the vehicles can also not be a solution as it is totally open to attackers of the network. This paper proposes secured VANET data transfer protocol, which allows vehicles in VANET to communicate important information related to traffic jams, accidents, and break implementation to other nodes, with feature to detect as well as isolate the different malicious nodes which may be present in the network.

VARS defines the decision area where the trustworthiness of event messages has to be decided upon. Until now these areas are proposed to be of circular shape. Further development should map those areas to the layout of the streets. The trustworthiness of the messages are decided upon using sensors, decision making phase and the previous trust value of the node. In VARS [6], depending upon the kind of reputation information a source is attributed with a sender-based reputation level. The thresholds for the confidence decision are adjusted in relation to the relative position of the sender compared to the position of the deciding node. VARS distinguish between situations with respect to availability and quality of reputation in formation as well as familiarity of the area, i.e., rural/unknown or metropolitan/well-known areas. These levels are called geo/situation-oriented reputation levels. Moreover, no parameters have been defined in order to clearly identify these areas. No such reputation levels are there in the proposed algorithm. All the areas are of equal importance and the reputation levels are assigned on the basis of the number of good or malicious behaviors performed by a node previously.

2. VEHICULAR AD HOC NETWORK (VANET)

VANETs have certain differences with Mobile Ad hoc Networks (MANETS). Consequently, most of the work done on MANETS [8] cannot be directly applied to vehicular networks. Some of the challenges are network dynamics, resource constraints, high application requirements on data delivery, no confidentiality for safety information, infrastructure access, central registration and periodic technical inspection, liability identification, and security issues. VANETs [11] have tremendous potential and scalability and therefore a successful attack by an adversary might have disastrous effects leading to huge loss of life. Thus, security in VANETs is of primary concern since an attacker may try to insert or modify life-critical information. VANETS are designed to cater to a number of applications pertaining to passenger safety, ease, and comfort.

However, the most important application envisioned for VANETS is to provide safe and secure driving conditions to the passengers. Some other applications for VANETs are safety-related applications, traffic optimization, infotainment, electronic toll collection, and roadside service finder. However, the main challenge in VANETs remains security[12]. The possible misuse of VANETs can create a lot of problems and difficulties especially in situations where life critical information is involved. This paper propose a novel way of incorporating security in VANETs through a trust-based algorithm based on reputation using sensors.

Establishing security in VANETS is dependent on a number of parameters that include minimum delay, trust, cost, and gradual deployment. A lot of effort has been put into research in this area that focuses on secure protocols for routing as well as one-hop communication. A number of methods have been proposed [9] to achieve security in VANETs such as cryptographic schemes, reputation-based systems, and plausibility and sensor-driven techniques. As security being a [13] major concern in VANETs, researchers have proposed a number of secure protocols that are based on either one of the above mentioned schemes or a combination of them. A framework provides security based on hardware that uses symmetric as well as asymmetric cryptography for message exchange[14].

The neighbor discovery, data dispatching, decision making and trust updating, and neighbor monitoring to establishes security in a VANET through accomplishment of trust levels for nodes in the network using reputation and plausibility checks.

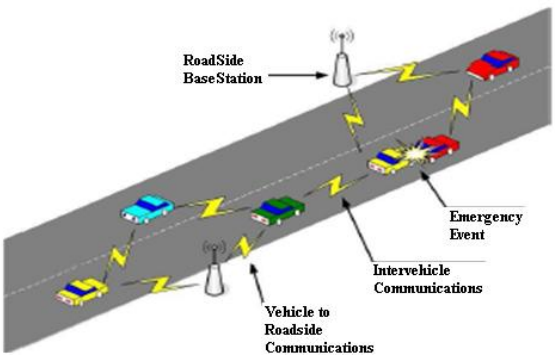

Fig. 1 Architecture of VANET

Fig. 1 shows the architecture of VANET. Roadside base station can senses the emergency event. Two or more vehicles can be able to communicate with each other on roadside. i.e., a inter-vehicle communication. Roadside base station monitors that inter-vehicle communication to detect the false event.

2.1 Attacks in Vanet

2.1.1 False Event Generation

False event generation is a type of attack in which a vehicle generates [14] information about an event that actually does not exists.

2.1.2 Data Modification

Data modification is a type of attack in which a vehicle purposely modifies the type of event that is a traffic jam to an accident or vice versa. For this a vehicle changes the type of event field in the data packet.

2.1.3 Data Dropping

Data dropping is a type of attack in which a vehicle does not forward the information it is supposed to forward.

2.1.4 Data Aggregation

Data aggregation is a type of attack in which a vehicle continuously sends or rather floods packets in the network.

2.2 Detection of Dropping Attack

Data dropping is a type of attack in which a vehicle does not forward the information it is supposed to forward. In our algorithm neighbor monitoring is a continuous feature in which the nodes simultaneously monitor their neighbor nodes. Thus, if a node has received a packet, but is not forwarding it the neighbor nodes can safely assume it to be a data dropping node.

2.3 Detection of Data Aggregation Attack

Data aggregation is a type of attack in which a vehicle continuously sends or rather floods packets in the network [7]. In order to handle this, whenever a Neighborreq packet is received from the same node, the counter maintained is incremented by one. This counter is checked at every pre-specified interval of time and if the counter value is found to exceed the threshold value, data aggregation by the malicious node is detected.

2.4 Data Forwarding through Stable Neighbor

In Vehicular Ad-hoc Networks based on the proposed routing mechanism, if forwarding vehicles have high mobility, there is the chance for local topology inaccuracy. If the vehicle involved in the forwarding path [13] vehicle moves frequently then there is the situation of link failure which leads to packet loss. Hence it is required to select the vehicles with low mobility which means selection of stable vehicle as forwarder based on its mobility. Mobility based forwarding vehicle selection scheme improves the routing performance.

Source vehicle predicts the distance of each neighbor from itself at particular time (t) using the current location of neighbor and speed of the neighbor. After certain time (t+T) it predicts the distance again using the current location of neighbor and speed of the neighbor. In both times if the vehicle comes under neighbor status then it is highly stable neighbor. To apply highly stable greedy forwarding distance between destination and highly stable neighbors are calculated. The neighbor which is having the minimum distance is selected as forwarder and its reputation value is increased.

3. PROPOSED SYSTEM

The proposed algorithm establishes security in a VANET through accomplishment of trust levels for nodes in the network using reputation and plausibility checks. The algorithm has been designed primarily for safety related information that are broadcasted in single hop and relayed in multihop through intermediate nodes. The packets to be sent will always be broadcasted and a unicasted packet will be taken as malicious information. The algorithm follows an event oriented approach, that is, a node initiates the communication when it observes an event through its sensors. The types of events have been classified as follows. Information about the events such as application of brakes needs to be communicated by a node only in its one hop neighborhood. Information about the events such as traffic jams and accidents is to be communicated by a node in its one hop neighborhood which is to be further relayed by the intermediate nodes to a threshold range, where this is the range up to which the packet can be relayed.

When a node detects malicious behavior either through the information gained through its own sensors or through checks performed by it after a packet has been forwarded, it communicates this information to its neighbors. The proposed algorithm in the case of traffic jams and accidents is divided into four phases: neighbor discovery, data dispatching, decision making and trust updating, and neighbor monitoring. In the case of information related to brakes the algorithm is divided into three phases: data dispatching, decision making and trust updating, and neighbor monitoring. VSRP which is based on the trust assigned to nodes will perform better in terms of deployment as no additional infrastructure is needed and the calculation time will also be reduced as no cryptographic schemes are employed.Whenever a node needs to forward some event which is either sensed through its own sensors or is forwarded by some trusted node, it initiates the neighbor discovery phase. In this phase, the sensing node broadcasts a Neighborreq packet and waits for the Neighborrep packets with which it recognizes its neighbors. In this phase, on receiving a Neighborreq packet a node checks in its trust table for that particular node. If the sending node is present and its trust value is 0, the node discards that packet. If the sending node is present and its trust value is not 0, the node accepts the packet and updates its

Reqseentable. If on updating the Reqseentable the sending node is found guilty of data aggregation then its trust value is set to 0 and a malicious-intent message is broadcasted to all the nodes. If however the node is not present in the Trust Table it is inserted in the Trust Table with a trust rating of 2 and the node also inserts the request into the Reqseentable. The request packet is accepted only if the node is either not in the Trust Table or is present with a trust value not equal to zero. When the initiator of the request receives Neighborrep it scans its Neighbor Table and Trust Table to check if the entry already exists for that node. If the entry does not already exist in the Neighbor Table then the initiator inserts it in the Neighbor Table and if it does not exist in the Trust Table then it is inserted in it with a trust value of 2 and counter value of 0.

Once a node has identified its neighbors it broadcasts the data packet and inserts this event in its event table to keep record of the fact that this event had been dispatched. When a node receives a data packet it performs the following checks on it. If the packet is received from outside the threshold range that means it is pertaining to an event that is far away then the packet is dropped. If the action has already been taken on that event then also the packet is dropped. If the above two criteria are not met then the node checks whether the event is in its detection range or not where detection range is the range of the node within which the node can detect an event. If the node is itself in the detection range and it has no information about the event then the event is possibly false and it decreases the trust value of the sending node and broadcasts a malicious intent control packet. If the node is itself in the detection range and it has information about the event then the event is genuine and it increases the trust value of the sending node. If the receiving node however is not in the detection range then it starts a timer and collects the responses from the other nodes in the temptable. If after the expiry of the timer the number of responses collected exceeds the threshold value, the event is considered to be genuine and the trust values of all the sending nodes are incremented.

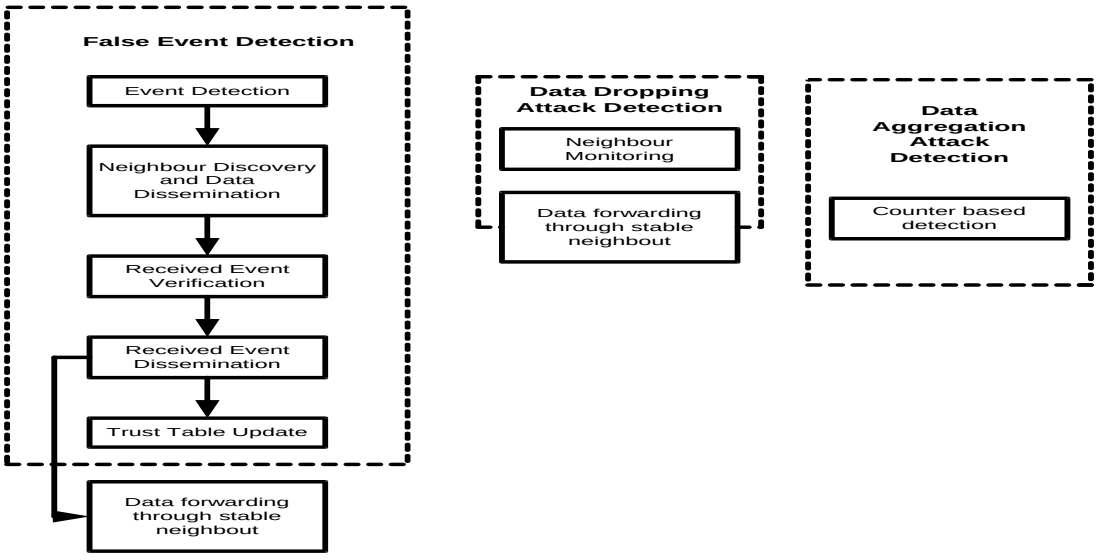

Fig. 2 Block diagram of proposed system

False Event Generation
False event generation is a type of attack in which a vehicle generates information about an event that actually does not exists.

Data Modification
Data modification is a type of attack in which a vehicle purposely modifies the type of event that is a traffic jam to an accident or vice versa. For this a vehicle changes the type of event field in the data packet.

Data Dropping
Data dropping is a type of attack in which a vehicle does not forward the information it is supposed to forward is shown in Fig. 2.

Data Aggregation
Data aggregation is a type of attack in which a vehicle continuously sends or rather floods packets in the network.

4. PERFORMANCE EVALUATION

Packet Delivery Ratio
PDR is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

$$\text{PDR}(\%) = \frac{\text{Number of packets successfully delivered to destination}}{\text{Number of packets generated by source node}}$$

Detection Delay
It is the average delay to detect the attacker making the attack in the network

Throughput
The amount of data successfully received at the destination.

$$Throughput\left(\frac{bits}{s}\right) = \frac{Total\ data}{Data\ transmission\ duration}$$

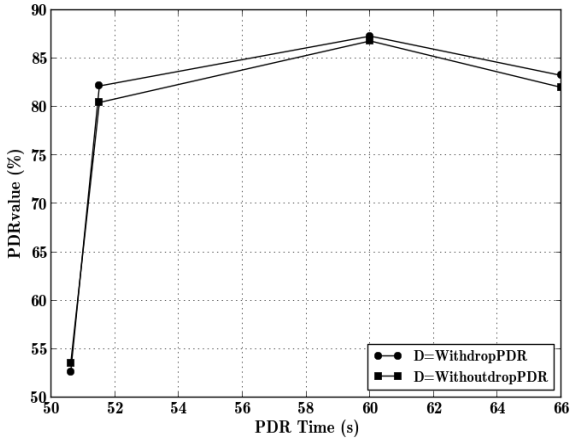

Fig. 3 Dropping attack in Packet Delivery Ratio

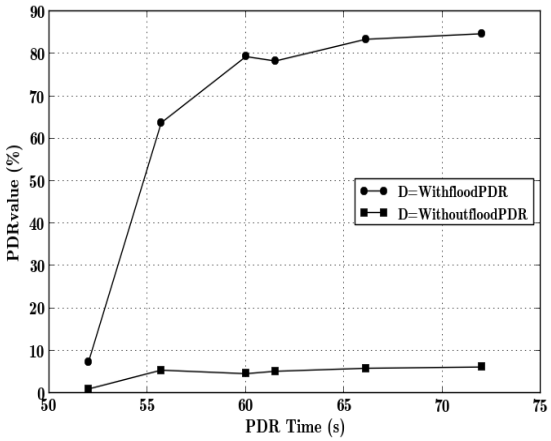

Fig. 4 Flooding attack in Packet Delivery Ratio

In Fig. 3 x- axis represents the PDR time and y- axis represents the PDR value. PDR compare with dropping attack and without dropping attack. Withoutdropping attack is better than the dropping attack. In Fig. 4 x- axis represents the PDR time and y- axis represents the PDR value. The withoutflooding PDR is better than the withflooding PDR.

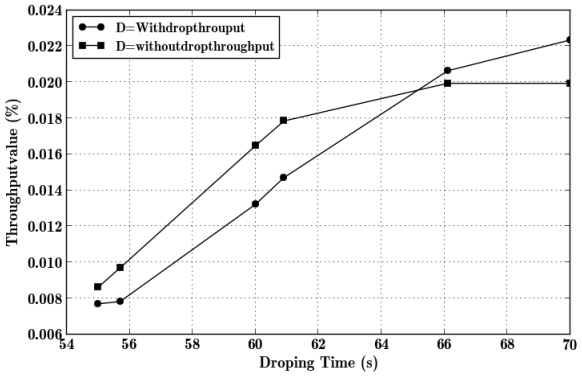

Fig. 5 Dropping attack in Throughput

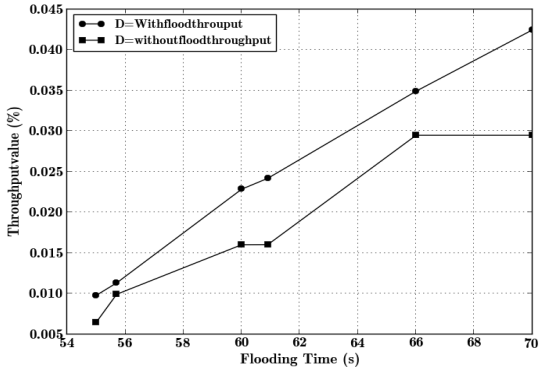

Fig. 6 Flooding attack in Throughput

In Fig. 5 x- axis represents the dropping time and y- axis represents the throughput value. The withdropthroughput is higher than the withoutdropthroughput. In Fig. 6 x- axis represents the flooding time and y- axis represents the throughput value. The withoutflood throughput is better than the withflood throughput.

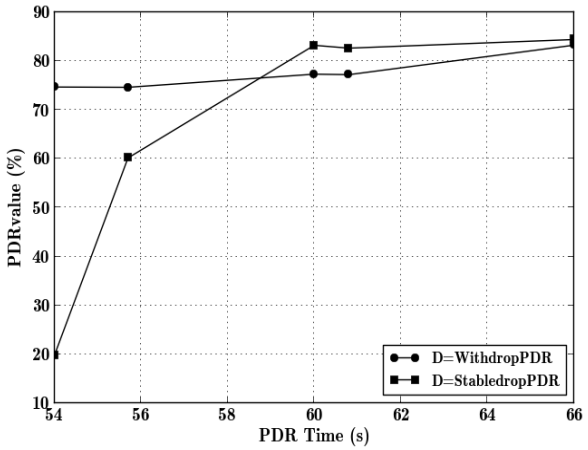

Fig. 7 Stability in Packet Delivery Ratio

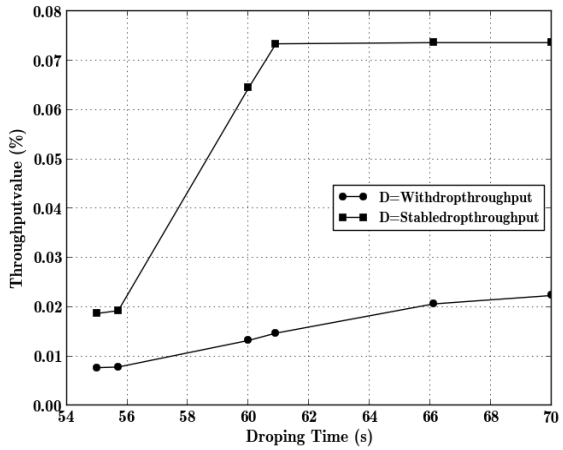

Fig. 8 Stability in Throughput

In Fig.7 x- axis represents the PDR time and y- axis represents the PDR value. The stabledrop packet delivery ratio is better than the withdrop detection attack. In Fig. 8 x- axis represents the dropping time and y- axis represents the throughput value. The stabilitydrop throughput is better than the withdrop detection attack.

5. CONCLUSION

VANET support infrastructure based commercial services which lead to security threat in different ways. The performance of service oriented VANET depends on their ability to protect against various types of security attacks. While most of the algorithms just detect the malicious nodes, VSRP not only detects malicious activity but also eliminates the malicious nodes. VSRP is also the ideal solution to the vehicular problems of developing countries as it is infrastructure less. Since it is infrastructure less, it is more cost efficient and also does not pose the problems associated with RSUs such as the RSU becoming a bottleneck. The control overheads in VSRP are also reduced as each node forwards the data intelligently and does not work in a brute force manner by forwarding the same information from different neighbor nodes a number of times. The simulation results show that VSRP provides an efficient and robust method to secure vehicular networks without using any infrastructure.

6. REFERENCES

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

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

[3] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for VANETs," in Proc. Veh. Technol. Conf., 2007, pp. 26–30.

[4] F. Dotzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., Jun. 2005, pp. 454–456.

[5] Rafael Marin-Perez, Pedro M. Ruiz, "SBGR: A Simple Self-Protected Beaconless Geographic Routing for Wireless Sensor Networks"

[6] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "VANET security framework for trusted grouping using TPM hardware," in *Proc. 2nd Int. Conf. Commun. Softw. Netw.*, Feb. 2010, pp. 309–312.

[7] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in Proc. ACM Mobicom, Montreal, QC, Canada, Sep. 2007, pp. 19–28

[8] TeerawatIssariyakul, EkramHossain, "Introduction to Network Simulator NS2" Springer,2009.

[9] G. Philippe, G. Dan, and S. Jessica, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.

[10] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP : Efficient condition privacy preservation protocol for secure vehicular communication," in *Proc. IEEE 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1229–1237.

[11] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular Ad Hoc networks (VANET)," in *Proc. 4th Int. Conf. New Trends Inf. Sci. Service Sci.*, May 2010, pp. 393–398.

[12] Y. Gongjun, B. B. Bista, D. B. Rawat, and E. F. Shaner, "General active position detectors protect VANET security," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, Oct. 26–28, 2011, pp. 11–17.

[13] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. 3rd Eur. Workshop. Security Privacy Ad Hoc Sens. Netw.*, vol. 4572. Jul. 2007, pp. 129–141.

[14] A. Wasef, L. Rongxing, L. Xiaodong, and S. Xuemin, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.