Self Organized Routing Scheme for Efficient Traffic Management Systems in Vanet

Mrs. D. Vinodhini,
[1]PG Scholar,
Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode
Tamilnadu, India.

Mr. K. Gopalakrishanan,
[2]Assistant professor,
Department of Computer Science and Engineering,
Vivekanandha College of Technology for Women,
Elayampalayam, Thiruchengode.
Tamilnadu, India.

***Abstract*--- In VANET, the main aim is to implement a privacy preserving route reporting technique that reduces collision and attacks in the network. In Data aggregation clustering concept is used to transmit messages faster and efficient. Also Homomorphic encryption and ECC point addition are used in order to get the network collision free. Even though this technique is trust worthy, intruders will use different ideas in day to day life. Hence to protect completely from the attacks and to make efficient network the Dydog mechanism is used. The concept of Dydog is same as watchdogs. The difference will be like in watchdogs if 5 to 6 nodes are deployed and it will act as police nodes like which will roam around the network and check for the malicious nodes but in Dydog it will make all the normal nodes to act as watchdogs. Hence if all nodes are alert and there won't be any attack in the network. More over watchdogs will use a key in the network and that will be randomly generated each and every time. Hence for random key generation Digital signatures are used which will randomize the key for Dydog nodes that is for normal nodes. By applying this technique end to end delay and energy spent decreases and pdr throughput increases. Obviously the network load and collision will decreases.**

Keywords: Traffic management, Homomorphic encryption, Privacy preservation, Collusion attack route reporting

I. INTRODUCTION

Network security consists of policies that are used to detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them for accessing the information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs. It secures the network as well as protecting and overseeing operations being done.

A. Wireless Sensor Network

A Wireless Sensor Networks (WSNs) are ideal candidates for monitoring environments in a wide variety of applications such as military surveillance and forest fire monitor, animal identification etc,. The field of wireless sensor networks offers a affluent, multi-disciplinary area of research, in which a variety of tools and concepts can be employed to ponder on a diverse set of applications.

Research is going in the fields of wireless sensor networks mainly on routing, energy consumption and security. Here the main focused idea is in intrusion detection systems (IDS) to secure the wireless sensor networks with energy optimization even in high error prone and in crowded situation by using DIDN. Unlike mobile ad-hoc networks or other wireless networks, wireless sensor networks have more number of nodes in dense manner in Fig 1.

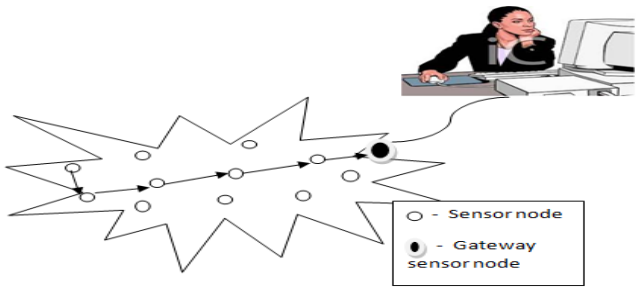


Fig. 1. Wireless Sensor Networks

B. Intrusion Detection System

Intrusion detection system is the system or tool or any intelligent computing algorithm that has been designed to monitor and detect unauthorized activities or malicious activities (attacks) in wired or wireless networks. Wireless sensor networks are distributed in nature, so here the intrusion detection system is called as Distributed intrusion detection system (DIDS). Distributed intrusion detection system works on individual wireless sensor nodes as an intrusion detection agent module to detect the vulnerabilities, attacks and decisions will be taken in distributed manner with the help of local and global agents.

C. Attacks and Compromised nodes

Normally wireless networks are more vulnerable against the attacks like Denial Of Service (DOS) which causes for Blackhole attack, Sybil attack, Wormhole attack, Selective forwarding attacks, Jamming attacks etc. This is the serious problem in wireless sensor networks. Likewise wormhole attack records and uses the secret data in unauthorized manner, Sybil attack causes for faulty identification and Selective forwarding attack causes for hunger and data loss in wireless sensor networks. Against these various types of attacks our proposed model will provide flexible and resilient

solution with the help of Dynamic Intrusion Detection Nodes for High-Data rate Wireless Sensor Networks based on data flow at runtime.

II .OVERVIEW OF VANET

Vehicular Ad Hoc Network (VANET) is a form of Mobile Ad Hoc Networks (MANET). VANETs provide us with the infrastructure for developing new systems to enhance drivers and passenger's safety and comfort. This type of networks is developed as part of the Intelligent Transportation Systems (ITS) to bring significant improvement to the transportation systems performance. One of the main goals of the ITS is to improve safety on the roads and reduce traffic congestion, waiting times and fuel consumptions. The integration of the embedded computers, sensing devices, navigation systems (GPS), digital maps and the wireless communication devices along with intelligent algorithms will help to develop numerous types of applications for the ITS to improve safety on the roads.

Vehicular networks that contains mobile nodes vehicles with (OBU) that is On Board Units and stationary nodes are called Road Side Units (RSU).Wireless/wired communications capabilities are in OBU and RSU. OBUs communicate with RSU in an ad hoc manner. VANET allow the wireless communication between vehicles (V2V) and between vehicles and infrastructure access point (V2I) as shown in Fig 2. Vehicle to vehicle communication (V2V) has two types of communication Single hop communication (direct vehicle to vehicle communication) and Dual hop communication (vehicle relies on other vehicles to retransmit).

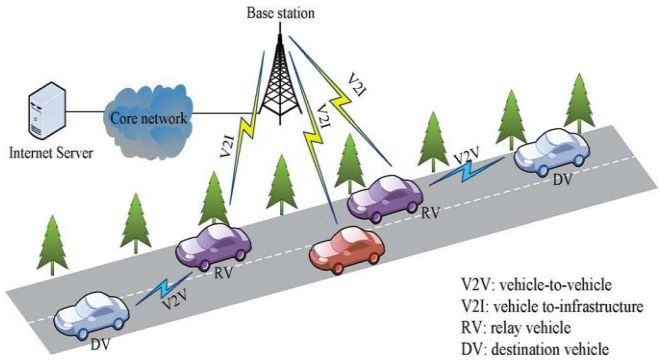


Fig. 2. V2I and V2V links in VANET'S

III. PROPOSED METHOD-DY-DOG

A. Selection of Intrusion Detection Nodes

In this proposed scheme dynamic intrusion detection nodes will be created to detect various attacks like DOS (Blackhole, Wormhole, Sybil and Selective forwarding attacks etc.,), Compromised nodes (CN) in wireless sensor networks. In previous related work only single blackhole can be identified. But here by using more selected Dynamic Intrusion Detection Nodes multiple Blackholes can be identified with the help of any suitable intelligent computing algorithms. Here every node will be monitored by more than one Intrusion Detection/Monitoring Nodes. In this scheme the node acts as both intrusion detection node as well as forwarding node dynamically. Also without cluster head the node itself take an action against these attacks and intimate to other neighbors with limited updates. The nodes in forwarding list acts as forwarding nodes for a moment only and this will be changed their nature to idle dynamically until it is the one hop neighbor for the forwarding node in other forwarding path if the data transmission is going on that path. Only the neighbor nodes which are not in that forwarding path monitor their forwarding nodes for intrusion detection at the time of data transmission and others are stable in functionality. At the time every single node can be monitored by more than one Dynamic Intrusion Detection Nodes (DIDN). If anyone is traced by the adversary other can detect the attack and action will be taken. This will provide better resiliency in intrusion detection and flexibility in DIDN availability with the help of designed algorithm will be discussed later. This method is very critical for intruders to identify or attack the Intrusion detection nodes.

Here we are going to use only idle nodes which are in one hop distance from forwarding node are selected as DIDNs when they are not in their forwarding path. By that the utilization of monitoring nodes will be increased and the data transmission will not be affected in any way. If any node will not satisfied the above condition will go to idle state to reduce power consumption. In worst case scenario, if the forwarding node won't be monitored by at least two Intrusion detection nodes or the data rate over the nodes will increase the overhead due to maximum mobility then the Intrusion detection node in one hop will select its next hop neighbor node as the Dynamic intrusion detection node (DIDN) for actual forwarding node if that monitoring node within the transmission range of forwarding node by the designed algorithm. But this will happen when high level data transmission occurs and the forwarding nodes need not to maintain two hop neighbor information all the time. At the time of critical situation or high data rate condition the one hop monitoring nodes will share their one hop node's information with forwarding node as its two hop monitoring node dynamically with predefined shared session key.

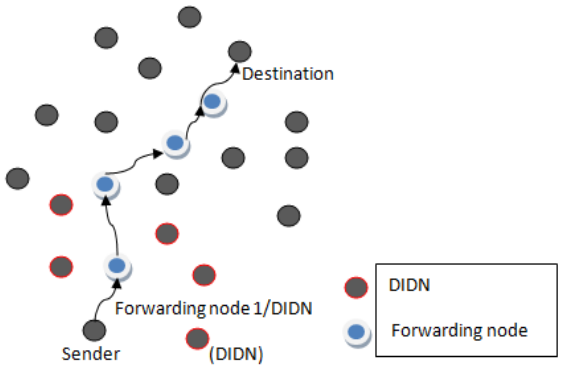


Fig . 3. DIDNs and Forwarding Nodes

From the Fig. 3 the nodes are separated as three types like Sender/Destination, Forwarding node only for the time of data forwarding and it will be changed as DIDN or idle node. And the Dynamic Intrusion Detection Nodes for forwarding

node 1 (One hop neighbors for forwarding node 1 which are not in the forwarding path). For this mechanism we propose a framework of efficient dynamic intrusion detection protocol to detect multiple attacks in wireless sensor networks and this will be used to send any type of data (multimedia) in secured manner. The proposed scheme has been planned to enhance the security against various attacks like DOS (Blackhole, Wormhole, Sybil and Selective forwarding attacks etc.,), Compromised nodes (CN) with secured dynamic Intrusion detection nodes even in dynamic condition of wireless sensor networks. This will suitable for both fixed wireless sensor networks as well as adhoc wireless sensors. By this flexible DIDNs deployment we can significantly reduce the overhead and power consumption of the individual nodes and increase the security against the attacks.

B. Secured Key Management for DY-DOG

To select DIDN here we need to make secure way which is used to identify the malicious nodes from DIDNs. The Intrusion detection node should maintain two secret shared session keys here to ensure the identity of that node from other malicious nodes. Secret shared session key for unique intrusion detection node. This key will be generated from forwarding node's partial data bits, sender's ID and monitoring node's ID (node to be DIDN). The entities are concatenated in forwarding node and EX-ORed in intrusion detection node and send that key to forwarding node. From this key the monitoring node's identity will be checked with reverse EX-OR operation. This will increase the security against intruder nodes. Within the particular session these keys are hard to be identified. This authentication scheme is used to avoid the malicious nodes monitor the sensor nodes as like DIDNs during data transmission.Decision making key for unique intrusion detection node. This will be generated after attacks are identified by the intrusion detection nodes.

C. Decision Key for Decision Making Dynamic Intrusion Detection Node Selection (DMDIDN)

The decision will be taken at the time of attacks identified. At the time of intruder attack based on this proposed system more than one intrusion detection nodes will monitor the forwarding nodes which are in one hop distance from that monitoring nodes. Every monitoring node could identify the attacks as much as possible, but when the action taken against these attacks the data need to be rerouted through other forwarding path after heal the infected node or infected packets. These alternative paths will be dynamically selected by intrusion detection node itself. But there are multiple monitoring nodes are available here to monitor the forwarding nodes.

Although there is more than one intrusion detection nodes are here only one will take a decision on route change during intrusion time. Here the forwarding node will send another key which is called as decision making key to their monitoring nodes and waiting for reply from those nodes. The nodes will reply the decision making key which had been got and TTL field to forwarding node. The lowest TTL valued node will be selected as decision making intrusion detection node. In the next step the forwarding node send only initial portion of data to the selected intrusion detection node and wait for acknowledgement for ensuring authentication. After that the remaining data will be forwarded to the correspondent node to make secured route selection. This Decision making node selection changes depends on nodes mobility.

D. Proposed Algorithms for DY-DOG, Dynamic Energy Efficient Intrusion Detection Protocol Model

The algorithm used to design DY-DOG protocol for dynamic intrusion detection based on data flow with maximum network data rate.

I) Algorithm- Secured DIDN Selection

If $D_R > D_{TH}$ || $DIDN_1 \leq 1$
{
Conditions on selection:-
$N \notin N_{F1L}$ of $N_{F1}(S)$:
$N \notin N_{FL}$ of $N_F(S)$;
$N \notin N_{FO}$ of $N_{FO}(S)$ || $DIDN_O$;
Let N (Node taken for selection process) $= N_{F2}$ here;
$N \in N_{11L}$ of $N_{F1}(S) \equiv N_{F2L}$ of $N_{F2}(S)$;
Then,
N_F $ID_{XF}||S_{DSF}$ N_{F1} ID_{NF1} ***XOR*** $(ID_{XF}||SD_{SF})$ N_{F2};
N_{F1} ID_{NF2} N_F ;
N_{F2} $ID_{XF}||S_{DSF}$ ***XOR*** ID_{NE1} ***XOR*** ID_{NE2} *via* N_{F1} N_F
Here, Key1=$ID_{XF}||SD_{SF}$ ***XOR*** ID_{NF1};
Key2=$ID_{XF}||SD_{SF}$ ***XOR*** ID_{NF1} ***XOR***ID_{NF2};
In Key1 ⟶ N_F checks If (ID_{XFR}= =ID_{XF} &&S_{DSFR}= =SD_{SF} &&ID_{NF1R}= =ID_{NF1})
{
And have the ID_{NF1}
Then in Key2 ⟶ N_F checks If (ID_{NF1R}= ID_{NF1}&& ID_{NF2R}= =ID_{NF2})
{
And have the ID_{NF2}
N ⟶ DIDN =N_{F2} ⟶ DIDN and this node ready to monitor;
}
Else
{
N ⟶ Malicious Node (N_{F2} ⟶ Malicious Node)}
It is valid If and only if ($N=N_{F2} \in A_{NF}$)
{
Else
Do the process from initial stage;
}}

Here, N_F - Forwarding node in current forwarding path; N_{F1L} & N_{F2L} -Forwarding List of one-hop and two-hop neighbor node respectively for N; N_{FL}- Current Forwarding path node list; N_{FO}- Forwarding node for other path; $DIDN_O$- DIDN for Forwarding node in other path; ID_{XF} & ID_{XFR} - ID of the sender for Forwarding node and received ID_{XF} in N_F respectively; S_{DSF} & S_{DSFR} - Sample data bit from Forwarding node and received S_{DSF} in N_F; ID_{NF1} & ID_{NF2}-ID of the Node taken for selection process from one-hop and two-hop respectively; N_{F1} & N_{F2}- Node taken for selection process from one-hop and two-hop respectively; ID_{NF1R} & ID_{NF2R}-received ID_{NF1} & ID_{NF2} in N_F; AN_F - Coverage area of N_F. This is the common one for other nodes also which have satisfied the above initial conditions in high error rate wireless sensor network.

IV.ANALYSIS OF SIMULATION RESULTS:

In simple topology seven nodes are send for the packet transmission. In this the packets are sent without any jammer. So the performance rate will be very high. The energy spent for the transmission of packet is very less. The average throughput and the packet delivery ratio gradually increases. There will be no average delay in packet transmission because only minimum modes are used without any traffic in the network. The values of network overhead, average throughput, average delay, energy spent, packet delivery ratio are measured.

In Normal topology instead of using seven nodes fifty nodes are sent for the packet transmission. As like simple here also the packets are sent without using jammer. But the performance rate will decreases compare to simple topology. This is one of the complex topology where the average throughput decreases. The values of network overhead, average throughput, average delay, energy spent, packet delivery ratio are noted to compare with the simple topology.

In this module instead of sending nodes to the network, the traffic so called Jammer is introduced in the network. After the introduction of jammer the performance rate decreases. The average throughput and the network overhead increases. Comparison is made to check the performance level of the packet transmission. The values of network overhead, average throughput, average delay, energy spent, and packet delivery ratio are noted to compare with simple and normal topology.

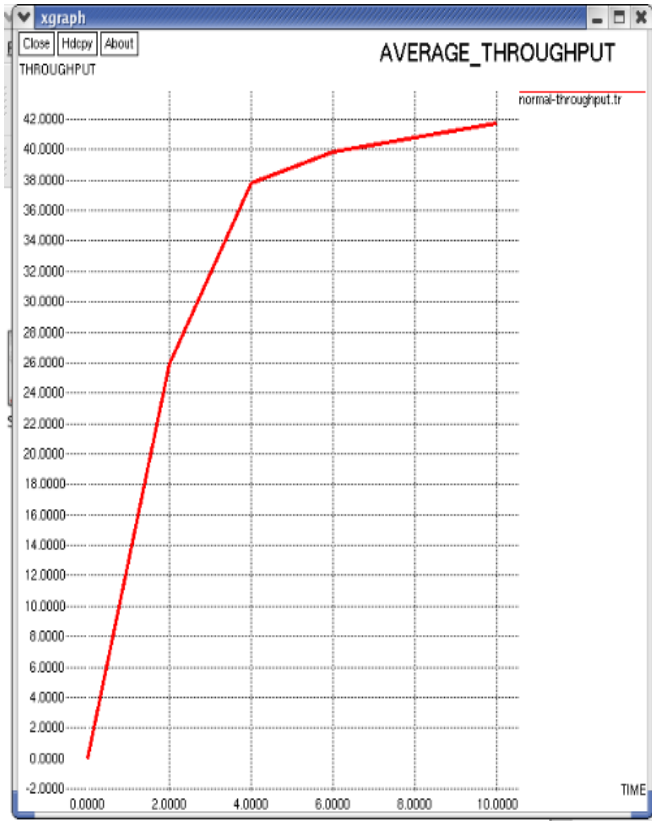


Fig. 4. Throughput in different traffic conditions.

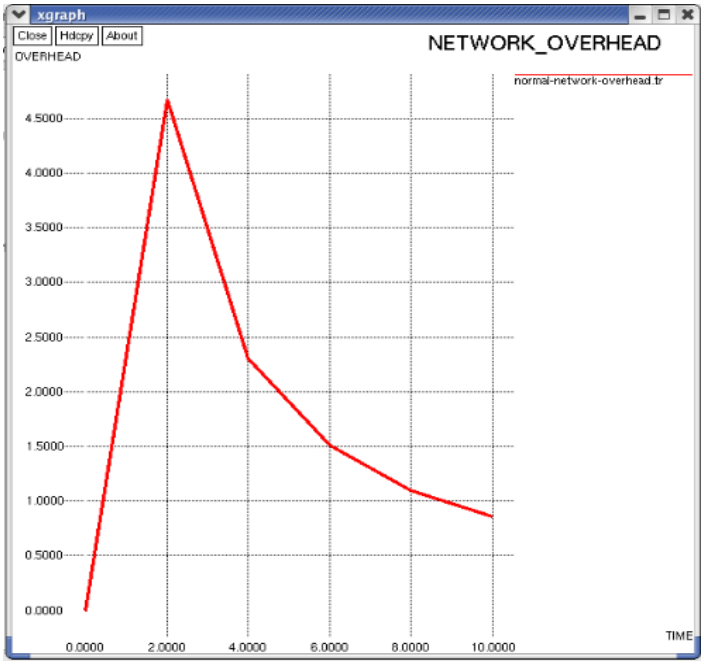
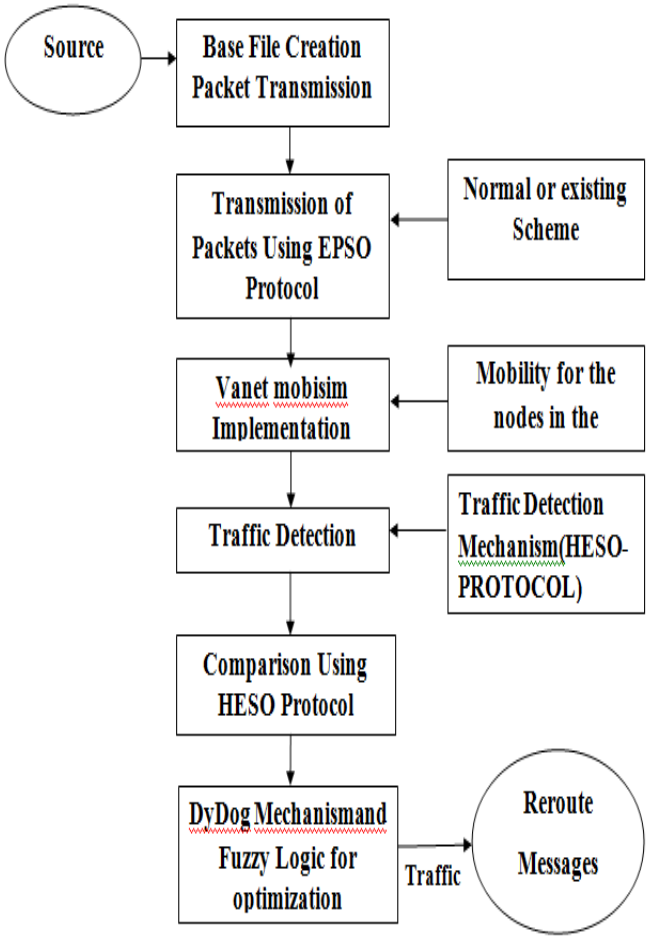


Fig. 5. Network overhead in different traffic conditions.

V.SYSTEM ARCHITECTURE



VI. PERFORMANCE METRICS FOR PROPOSED SYSTEM

The following performance metrics are considered to assess the network performance.

• Average end-to-end packet delay: after the packet is sent the average time takes by it to reach its destination.

• Throughput: Fig 4 shows the vehicles receives the average amount of data per second.

• Participation ratio: This is the percentage of vehicles that joined a group and could stay connected to the group till receiving the final traffic report. It is possible that some vehicles do not meet leaders to join platoons.

*Average packet delay:*The average packet delivery delay at different traffic conditions. It can be seen that the packet delay increases when the number of vehicles increases in EPSO and HESO schemes. This increase is mainly due to channel contention. It can also be seen that EPSO experiences less delay than HESO. This is because the vehicles perform ECC point addition to encrypt the route information in EPSO, which takes less computation time than the exponential operations needed in HESO.

Throughput: The average throughput at different traffic conditions. It can be seen that the throughput increases with the increase in the number of vehicles in EPSO and HESO. This is very much expected because the number of transmissions increases as the vehicle population grows. It can also be seen that the throughput in the case of EPSO is less than that of HESO. This is due to two main reasons: 1) Unlike EPSO that requires reporting the route only once, vehicles should report routes at least twice to the leader and subleaders in HESO; and 2) the packet size to report routes in HESO is larger than that of the EPSO because HESO uses homomorphic encryption that needs more space than the ECC used in EPSO.

Fig 5 shows the packet size in EPSO is about 180 B, whereas the packet size in HESO is 636 B.

Participation ratio: The vehicles' participation ratio at different traffic conditions. It can be seen that the participation ratio is the same at different traffic conditions. This is because the number of leaders is 5% of the total number of vehicles; therefore the number of leaders increases with the increase in the number of vehicles. This is because the execution of HESO takes more time than EPSO, and thus more vehicles may leave a platoon without receiving the traffic report.

VII.CONCLUSION

Reporting current and future routes of vehicles helps traffic management systems to alleviate and prevent congestion, yet it degrades driver's privacy. This paper have proposed Self organized routing scheme for an efficient traffic management systems in VANETs.In the case of self-organizing VANETs, our proposed schemes not only preserve the driver's privacy but protect against the notorious collusion attack as well. Hence to protect completely from the attacks and to make efficient network the Dydog mechanism is used. By applying this technique end to end delay and energy spent decreases and pdr throughput increases. Obviously the network load and collision will decreases.

VIII.REFERENCES

[1] Khaled Rabieh, Mohamed M. E. A. Mahmoud, 'Privacy-Preserving Route Reporting Schemes for Traffic Management Systems', IEEE transactions on vehicular technology, vol. 66, no. 3, march (2017).

[2] Boneh.D and Franklin.M.(2016), "Identity based encryption from the weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615.

[3] Calabrese.F, Colonna.M, Lovisolo.P, Parata.D, and Ratt.Ci.(Mar. 2016),"Real-time urban monitoring using cell phones: A case study in Rome," IEEE Transp. Syst., vol. 12, no. 1, pp. 141–151.

[4] Freudiger.J, Raya.M, Felegyhazi.M, Papadimitratos.P, and Hubaux.J.P. (Aug 2015), "Mix-zones for location privacy in vehicular networks," in Proc. ACM WiN-ITS, pp. 1–7.

[5] GHz DRC. (Dec. 2011) , [Online] Available: http:// grouper. ieee. org/ scc32/dsrc/SGupte and M. Younis, "Vehicular networking for intelligent and autonomous traffic management," in Proc. IEEE ICC, pp. 5306–5310.

[6] Jia.D,Lu.K, Wang.J, Zhang X, and Shen.X.(2007), "A survey on platoonbased vehicular cyber-physical systems," IEEE Commun. Surveys Tut., vol. 18, no. 1, pp. 263–284, 1st Quart.

[7] Li.H, Yang.Y, Luan.T.H, Liang.X, Zhou.X, and Shen.X.S.(May/Jun. 2003),"Enabling fine-grained multi-keyword search supporting classified subdictionaries over encrypted cloud data," IEEE Trans. Depend. Sec. Comput., vol. 13, no. 3, pp. 312–325.

[8] Lenstra.A and Verheul.E.(Aug 2002), "Selecting cryptographic key sizes," Public Key Cryptography, vol. 1751, pp. 446–465.

[9] Li.H, Liu.D, Dai.Y, and Luan.T.H.(May. 2000), "Engineering searchable encryption of mobile cloud networks: When QoE meets QoP," IEEE Wireless Commun., vol. 22, no. 4, pp. 74–80