International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 8, August-2016, Impact Factor: 1.544

A Hybrid Authentication and Encoding Model for reliable VANET Communication

Manju[1], Dhirendra Mohan[2]

Student, M.Tech. (CSE), Royal Institute of Technology and Management
Asstt. Professor, CSE Dept., Royal Institute of Technology and Management

Abstract **- Secure communication in vehicular network is a critical challenge because of hybrid nature and mobility. In this paper, a hybrid cryptography based encoded communication model is provided to achieve the security against internal and external attacks. The work is defined for the infrastructure specific vehicular network in which the RSUs have controlled the region communication. In first phase of the proposed model, the RSA based signature verification is done for new nodes in the region. In second phase, DES adaptive encoded communication is provided. The method also observed the group adaptive analysis to generate the preventive communication path. The work model is implemented in NS2 environment. The simulation results show that the model has improved the network communication and reduced the communication delay.**

Keywords : VANET, Secure, RSA, DES, Encoding, Authentication.

I. INTRODUCTION

Vehicular network is the vast area network with large number of vehicle nodes and infrastructure specification. The geographical location, scenario specification, infrastructure placement, vehicle type and vehicle movement are the features as well as challenges for this network form. The network is defined under the hybridization feature defined at different levels. These levels includes architecture level, communication level and channel level. The vehicle type, speed, direction and the coverage also affects the network performance. These hybrid features and characterization also increases the communication criticality and the network suffers various internal and external attacks. Different attack detection, prevention and authentication methods and measures are defined to provide the safe communication over the network. This work is basically focused on cryptography based vehicular communication model. This encoded communication based model is shown here in figure 1. The figure is showing the vehicular communication with infrastructure specification as well as encryption modeling while performing the communication within network.

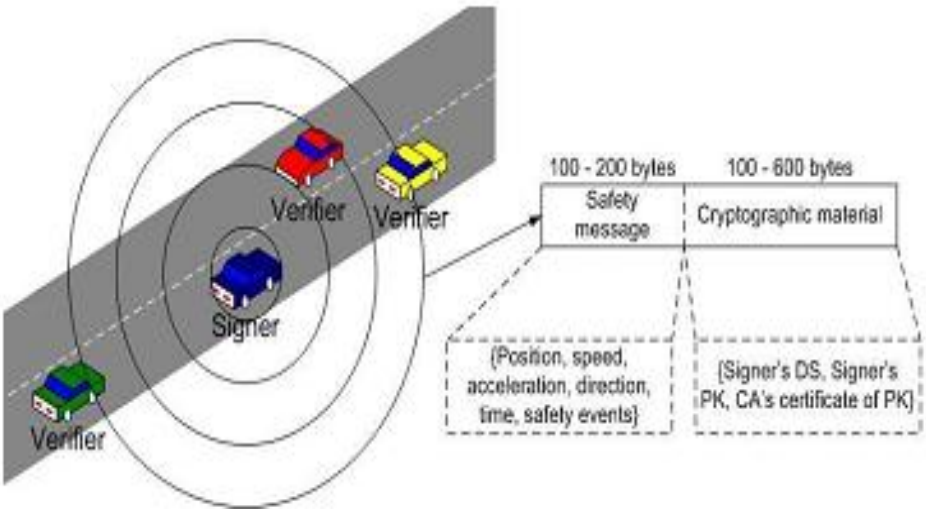

Figure 1 : Secure VANET Architecture

The authentication or the encoded communication in the vehicular network can be defined at different level. The V2V and V2I based encoded communication is defined to provide reliable communication. The cryptography key based mapping can be defined for authentication check as well as the encryption algorithm provides the encoded communication. The secure key exchange based communication is shown in figure 2.

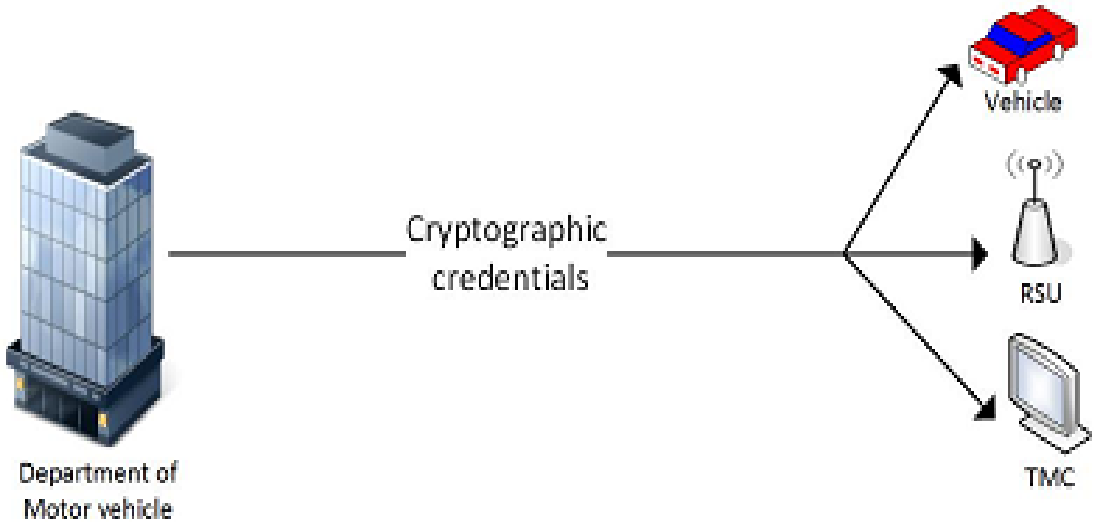

Figure 2 : Encoded Communication in VANET

Here figure 2 is showing the encoded communication model defined in the network. The figure shows that the encoding is managed by the Motor vehicle management that captures the vehicle and the node form. The inclusive cryptography elements include the vehicle nodes, RSU and the base station devices. Relatively, the secure V2V and V2I communication can be performed. In this paper, a dual cryptography based communication model is provided for vehicular network.

II. RELATED WORK

Security is the primary requirement for any network. For VANET, in which new nodes are introduced very quickly, the criticality of the network increases. Some authentication methods can be applied to improve the communication quality of the network. In this section, the work defined by earlier researchers to improve the communication security in VANET. Author[1] has used the RSA integrated encryption with effective WiFi integrated traffic system for VANET. Author applied the encryption method on MAC protocol and controlled the cryptography behavior via RSUs. Author[2] has defined reencryption method to improve the reliability of V2V communication. The proxy based cipher conversion and the capacity specific transition shows that the method has improved the communication reliability. Author[3] has defined a work on vehicle specific authentication by using the concept of random permutation. The weak encryption method is defined to provide the efficient encoding. A symmetric key based block cipher was used by the author with random permutation to improve the communication reliability. Author[4] also used the concept of Re-key based encoding to apply the authorization in Vehicular network. Author defined the intermediate re-encryption concept under the time slot analysis. The method not also provided the data security but also improved the communication throughput. Author[5] has defined a work on vehicular network modeling with topological change observation. The cryptography inclusion was provided to perform the V2V and V2I communication. The encoding and authentication was ensured using public key and private key concept. The privacy adaptive communication was provided by the author. Author[6] has defined a work on route reporting scheme with inclusion of privacy at vehicle level. The RSU ensured the key distribution and data encoding at vehicle level. Secure message communication and the information transition also controlled by the RSU. The traffic condition analysis based potential congestion control at traffic level was provided by the author.

Author [7] has defined a group key concept for improving the VANET communication using Diffie Hellman cryptography method. The pre-shared key based man-in-middle attack detection and secure communication was provided by the author. A privacy scheme based attack detection and prevention was provided by the author. The group

generation, group key generation and sharing was controlled at vehicle level. The aspired communication and authentication model was provided by considering the neighbor group nodes. Author[8] has defined an anonymous authentication key agreement to improve the vehicular message security. Author used the Elliptic key cryptography method to verify the communication using signature driven scheme. The service announcement and the protocol integration with security measure were provided by the author. The attack preserved communication was censured by the author. Author[9] has provided the location driven authenticity for improving the services of Road Network. Author defined analysis at node level against inference attack, correlation attack and the transition attack.

The location preserved communication architecture was provided by the author along with zone modeling. Author[10] has improved the security feature for WAVE protocol using distributed key concept. The key generation and management were provided by author using priority specific packet generation. The symmetric key cryptography method was provided to improve the security goals and to improve the communication throughput. The short term and long term keys were used to achieve the security based on the communication type. Author[11] has provided the comprehensive message authentication while performing the intra-RSU and inter-RSU based communication. The handoff management and the attack preserved communication control were also provided by the author. The signature generation, sharing and the source driven negotiations were defined by the author. Based on this negotiation, the secure route formation is done at vehicle and RSU level.

Author [12] has defined a security driven framework for improving the geographic adaptive communication for vehicular network. The physical location analysis and the physical characteristic determination were provided by the author to provide message encoding and decoding. The secure and reliable communication modeling was provided by the author. The region specific secure message exchange was provided by the author to improve the communication reliability at node level. The scenario specific Geo locking was provided by the author. Author[13] has provided a secure communication modeling using trust based message communication in vehicle network. The fuzzy logic based trust value observation and the secure communication primitive generation was provided by the author. The link state analysis was provided by the author to improve the trust level so that the routing decision will be improved. The fuzzy rule integration was provided to achieve the preventive communication against the malicious behavior nodes. Author[14] has provided a work on attribute based access control to provide emergency message communication for vehicular network. The confidentiality based communication with fine grained message control was provided by the author. The key specific communication has reduced the computational delay and provided the preventive communication against the collusion attack.

The rescue query based message communication and transmission was provided by the author. Author[15] has provided the security solution to achieve the intelligent transportation for vehicular network. Secure V2V and V2I communication was provided by the author using Elliptic Curve Cryptography model. The collision avoidance and the pre-crash system were provided by the author to achieve the phase driven communication. The risk evaluation and the intervention control were provided by author to improve the communication integrity. The infrastructure specific communication control for vehicular network was provided by the author. Author[16] has defined a work on dynamic key based communication in vehicular network. The tamper free communication was provided by the author with specification of certification verification. The certificate authority based message revocation was provided to achieve the secure communication. The dynamic secure communication also reduced the communication cost. Author[17] has defined a work on RSA based encoded communication in vehicular network. The self organized key generation and distribution model was provided to reduce the weakness of vehicular network. The signature specific encoding using RSA method was provided to improve the communication trust.

III. RESEARCH METHODOLOGY

The security is the primary requirement for any global network. Different internal and external attacks affect the network integrity and reliability. In case of open area network such as Vehicular network, the communication criticality also increases. To provide the secure and authenticated communication, some cryptographic methods can be applied. In this work, a dual cryptography method in applied to ensure the authentication in vehicular network. This hybrid authentication model is based on the group formulation. The session specific communication and reliability was provided by the author. The security was provided by the RSU by using the static and dynamic parameters and provided the two cryptography at node level.

These dual cryptography methods were provided using RSU and DES method. The work in here divided in two phases. In first phase, the node analysis will be applied based on static and dynamic parameters to identify the node reliability. The reliability of node is under the session level observation and its commitment to a RSU. Once the node reliability will be identified, the cryptographic methods will be applied. For the dedicated reliable nodes, one time authentication check will be applied using RSA method. For unreliable nodes, a session based authentication check will be performed using DES method. The work is about to improve the communication throughput and reduce the communication delay. The proposed work model is shown here in figure 3.

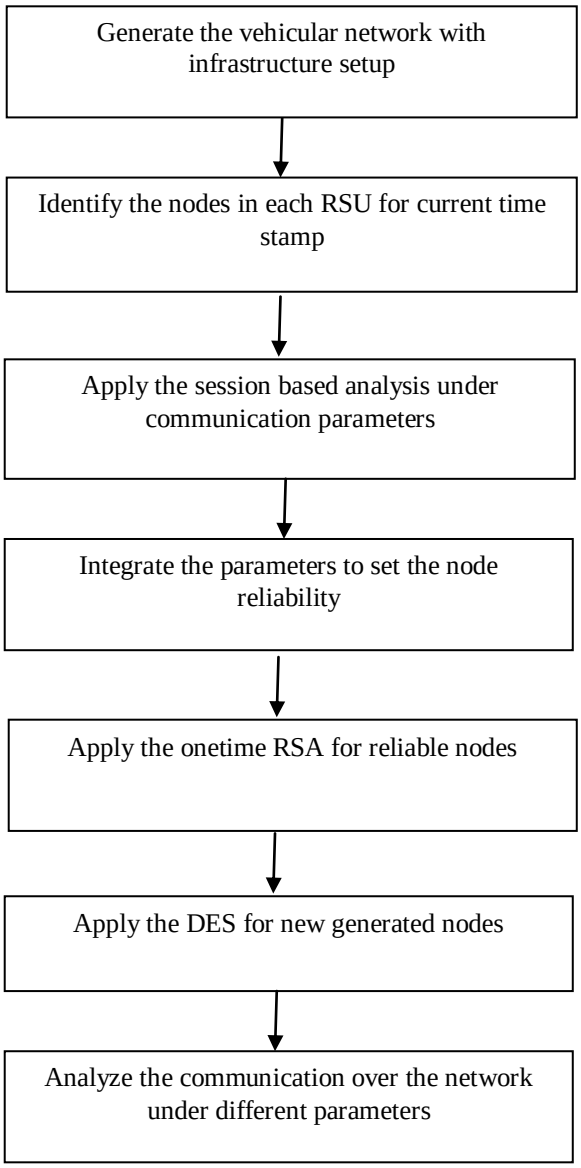

Figure 3 : Work Model

Here figure 3 is showing the secure encoded communication in vehicular network. At first, the scenario specific network is defined with specification of base station and road side units. Once the network is generated, and the vehicles are defined with mobility. The message communication between the vehicles and the Rode side units is done. The session specific analysis is here done to identify the reliability based on different parameters. The RSA and DES based authentication is performed for different node types. The first time authentication is performed as the signature map using RSA approach and later on DES is applied to provide the encoded communication. The parameters specific secure communication is provided in this work.

A) DES

DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. 56-bit key is used in DES and 16 cycle of each 48-bit sub keys are formed by permuting 56-bit key. Order of sub keys is reversed when decrypting and the identical algorithm is used. Block size of 64-bit is made from L and R blocks of 32-bit. The basic process of RSA is shown in figure 4.

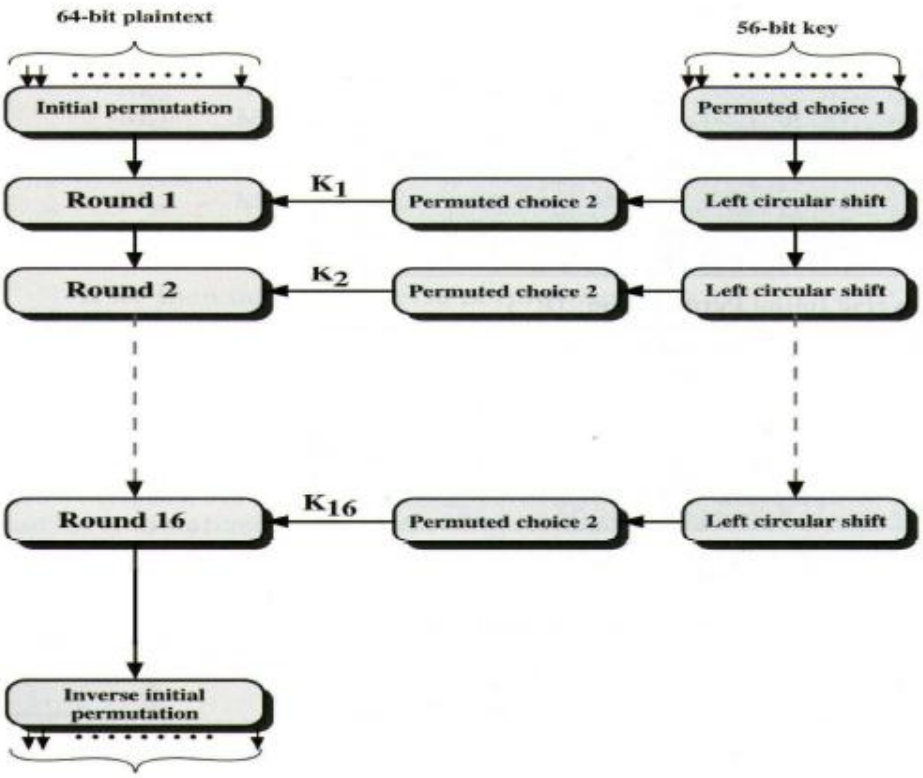

Figure 4: DES Process

B) RSA

RSA is the cryptographic algorithm that provides higher degree of security. It uses the modular exponentiation of long integer in the mathematical operational form. It is responsible to perform encryption and decryption. RSA is the cryptographic algorithm based on the factorization problem of long integers.

IV. RESULTS

In this present work, a dual cryptography based on security system is applied in vehicular network. The proposed secure communication model for vehicular network is simulated in vehicular network. The city scenario based two-lane network is defined with fixed infrastructure specification. The network is defined with 40 vehicle nodes moving in different directions and speed. The comparative analysis is here provided in terms of network communication and communication delay parameters. The packet communication based analysis is shown here in figure 5.

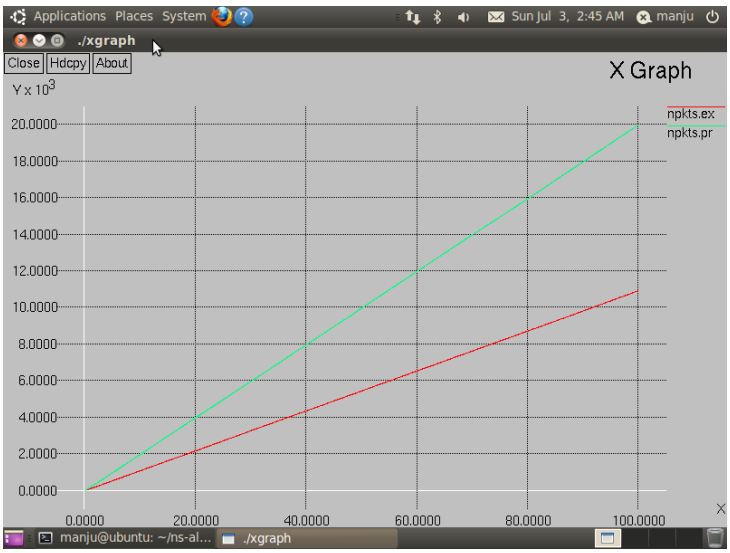

Figure 5: Packet Communication (Existing Vs. Proposed)

Here figure 5 is showing the packet communication analysis for existing and proposed approach. In the proposed approach dual cryptography method is provided based on the RSA and DES approach. Here x axis shows the simulation time and y axis showing the packet communication. The figure shows that the proposed model has improved the packet communication.

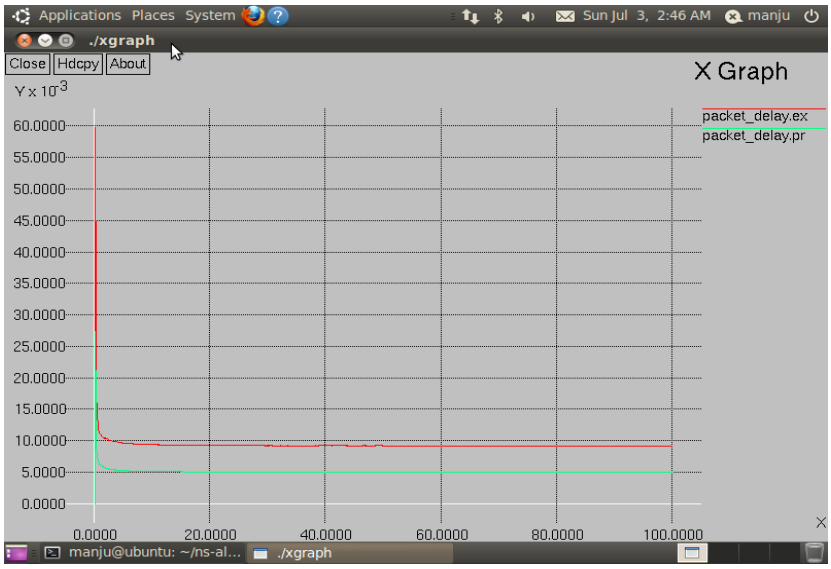

Figure 6: Packet Delay (Existing Vs. Proposed)

Here figure 6 is showing the packet delay analysis for existing and proposed approach. In the proposed approach dual cryptography method is provided based on the RSA and DES approach. Here x axis shows the simulation time and y axis showing the packet delay. The figure shows that the proposed model has reduced the packet delay and over all communication reliability is improved.

CONCLUSION

In this paper, a dual cryptography based secure communication model is provided for improving the reliability in vehicular network. At the earlier stage, the RSA encryption method is used as the signature map for a new vehicle in the region. Later on, DES cryptography is applied to provide the secure communication in the region. The simulation results show that the method has improved the communication and reduced the communication delay.

REFERENCES

[1] M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," Computer, Communication and Control (IC4), 2015 International Conference on, Indore, 2015, pp. 1-5.
[2] M. Kaur, Rajni and P. Singh, "New proxy re-encryption method to evaluate performance of V2V communication in a straight road scenario," Communication and Computing (ARTCom 2013), Fifth International Conference on Advances in Recent Technologies in, Bangalore, 2013, pp. 84-90
[3] N. V. Vighnesh, N. Kavita, S. R. Urs and S. Sampalli, "Vehicle authentication scheme based on random permutation for VANET," Information and Communication Technologies (WICT), 2011 World Congress on, Mumbai, 2011, pp. 722-726.
[4] A. Malik and B. Panday, "Performance analysis of enhanced authentication scheme using re-key in VANET," 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Noida, 2016, pp. 591-596.
[5] V. K. Tripathi and S. Venkaeswari, "Secure communication with privacy preservation in VANET- using multilingual translation," Communication Technologies (GCCT), 2015 Global Conference on, Thuckalay, 2015, pp. 125-127.
[6] K. Rabieh, M. M. E. A. Mahmoud and M. Younis, "Privacy-preserving route reporting scheme for traffic management in VANETs," 2015 IEEE International Conference on Communications (ICC), London, 2015, pp. 7286-7291.
[7] M. N. Mejri, N. Achir and M. Hamdi, "A new group Diffie-Hellman key generation proposal for secure VANET communications," 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2016, pp. 992-995.
[8] C. Büttner and S. A. Huss, "A novel anonymous authenticated key agreement protocol for vehicular ad hoc networks," 2015 International Conference on Information Systems Security and Privacy (ICISSP), Angers, France, 2015, pp. 259-269.
[9] A. K. Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," Communications and Signal Processing (ICCSP), 2015 International Conference on, Melmaruvathur, 2015, pp. 1319-1326
[10] K. J. Ahmed, M. J. Lee and J. Li, "Layered scalable WAVE security for VANET," Military Communications Conference, MILCOM 2015 - 2015 IEEE, Tampa, FL, 2015, pp. 1566-1571.
[11] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular adhoc networks," 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, 2009, pp. 804-809.

[12] S. Tan; X. Li; Q. Dong, "A Trust Management System for Securing Data Plane of Ad Hoc Networks," in IEEE Transactions on Vehicular Technology , vol.PP, no.99, pp.1-1
[13] W. Hsin-Te, W. S. Li, S. Tung-Shih and W. S. Hsiehz, "A Novel RSU-Based Message Authentication Scheme for VANET," 2010 Fifth International Conference on Systems and Networks Communications, Nice, 2010, pp. 111-116.
[14] L. Y. Yeh, Y. C. Chen and J. L. Huang, "ABACS: An Attribute-Based Access Control System for Emergency Services over Vehicular Ad Hoc Networks," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 630-643, March 2011.
[15] E. Bubenikova, J. Durech and M. Franekova, "Security solutions of intelligent transportation system's applications with using VANET networks," Control Conference (ICCC), 2014 15th International Carpathian, Velke Karlovice, 2014, pp. 63-68.
[16] A. Hesham, A. Abdel-Hamid and M. A. El-Nasr, "A dynamic key distribution protocol for PKI-based VANETs," Wireless Days (WD), 2011 IFIP, Niagara Falls, ON, 2011, pp. 1-3.
[17] J. Choi and S. Jung, "A Security Framework with Strong Non-Repudiation and Privacy in VANETs," 2009 6th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, 2009, pp. 1-5.