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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Secure and Proficient Routing Protocol in Mobile Ad-hoc Networks using Genetic Mechanism

Ritu Sharma

Ph.D. Scholar, Department of CSE, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal, India

ABSTRACT: Routing in Mobile Ad-Hoc Networks (MANETs) is a major issue because of its behaviour of open medium, without infrastructure, dynamicity and no authenticated centralized authority. In MANET, a node can be compromised during the route discovery procedure. Intruders from inside or outside can easily feat the network. Various Proficient routing protocols have been introduced for MANETs. In this research paper, Ad-Hoc On-Demand Distance Vector (AODV) routing protocol is assumed because of the fact that it utilizes the shortest no. of wireless hops towards a destination node as the primary metric for choosing a route with traffic congestion independence. To add security to AODV, Proficient AODV was developed to improve security facilities to the original AODV. Proficient AODV protocol has been planned with cryptographic methods i.e. digital signatures and hash chains, which can have an important effect on the routing performance of AODV routing protocol. To enhance PAODV efficiency, Enhanced PAODV (EPAODV) was introduced based on Genetic Algorithm and alternative route. The genetic algorithm examines the paths in terms of chosen metrics. The performance and influences of utilizing AODV, S-AODV and EPAODV routing protocols were compared employing RIVERBED Modeler. The simulation results established that utilizing the introduced technique could important reduce the routing overhead and the End-to-end delay.

KEYWORDS: Mobile ad-hoc network, PAODV routing protocol, Genetic algorithm

I. INTRODUCTION

Mobile ad-hoc network is a group of nodes that are linked to one another with wireless connections without any infrastructure. The routing protocols in ad-hoc atmosphere can be categorized as reactive routing protocols and proactive routing protocols. Proactive protocols manage entire paths in routing tables and when the source node requires to set up a route to the target node, the path that already available in its routing table is utilized.

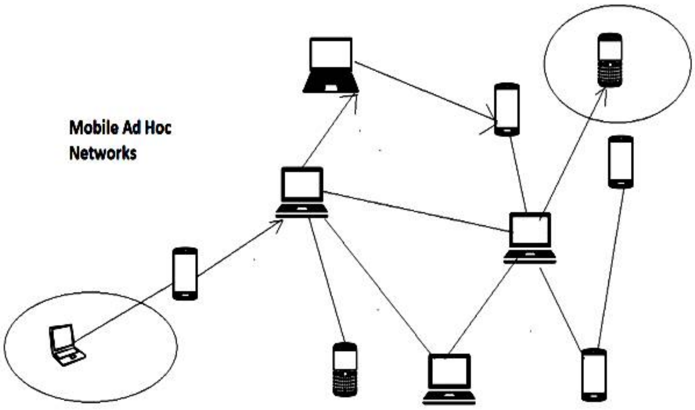


Figure 1: Mobile Ad Hoc Network

DOI: 10.15680/IJIRCCE.2016. 0406093

In reactive protocols, the route is set up only when the source node requires to forward a data packet to the destination node. There are several routing protocols for MANET i.e. AODV, OLSR, DSR, but none of them are protected. As a result, they consider there is no malicious node in the network; since, because of the MANET flexibility, there are a lot of susceptibilities in this type of network and security issue is the most important problem in it. Two different security techniques are shown for routing protocols. The first one ensures routing messages authentication and integrity. The second technique permits node to control another node nature during route discovery mechanism. Both two techniques require some network resources i.e. energy, battery and bandwidth. The main objective is discovering the balance between security and efficiency.

II. PAODV ROUTING PROTOCOL

The first Proficient and extended version of AODV is Proficient AODV (PAODV) that depends on asymmetric cryptography. In PAODV protocol, the routing messages (RREQ, RREP, and RERR) are encrypted by digital signature to ensure the authenticity and integrity. Because of not propagating the RREQ for external nodes, this routing protocol prevents from external active attacks. All nodes are authorized by a unique password. When a source node wishes to forward the RREQ, it first authenticates its neighbours by that password and then floods the message. In PAODV, the forwarder signs the routing messages by its private key and the recipient verifies them by the sender's public key. Due to incrementing the hop-count in every step of routing discovery, the forwarder cannot encrypt it. Thus, for protecting this field (i.e. not permitting malicious node to decrease it), PAODV utilizes hash chain. This structure is hard to utilize when an intermediary node has a route to destination node in routing table however RREP essentially has to have destination signature. For solving this issue, PAODV utilizes double signature. In this process, RREQ has a second signature that is always recorded with the back path route. An intermediate node, which wishes to response RREQ, utilizes second signature and adds it to RREP. Then it is forwarded to the source node. The RREQ and RREP messages fields are: Since, PAODV messages are importantly larger and need heavy computation due to digital signature, particularly for double signature. PAODV solves the routing tables overhead by updating them in specific time. So PAODV prevents the black hole attack. In comparison with AODV, because of an encryption in PAODV, malicious node cannot access the messages content; nevertheless cryptography process increases routing delay and the message length.

III. GENETIC ALGORITHM

John Holland introduced genetic algorithm in 1970. The route contains sequence of nodes. This algorithm executes on routes, which are obtained from route discovery procedure. In the first step, the route is coded by sequence of integers, which these are the node's IP. The sequence length cannot be more than the no. of nodes. GA operation contains six essential levels: genetic presentation, initial population, fitness function, selection, crossover and mutation. This collection is "standard GA" (SGA).

Discovering the shortest path in mobile ad-hoc networks needs the route evaluation from the source node to the destination node, which has the minimum cost. The old algorithms i.e. Dijkstra and Bellman ford show how the shortest path is discovered. Yet, these algorithms are particularly utilized for wired network and are not appropriate for wireless networks. Genetic algorithm is one of the algorithms that are helpful for ad-hoc networks and it is utilized for designing more efficient protocols.

3.1 Genetic Presentation

The path is coded by integers sequence, which are node's IP.

3.2 Initial Population

Every chromosome represents a powerful solution. Initial population contains no. that shows the chromosomes in AODV protocol. The routes that are obtained from route discovery procedure are targeted for initial chromosomes.

3.3 Fitness Function

The quality of every solution should be measured accurately. In this function, the primary objective is discovering the richest path between source node and destination node. The fitness parameters are defined according to the problem needs. In this paper, the objective of utilizing genetic algorithm is discovering the shorter path from the source node to the target node with decreasing end-to-end delay.

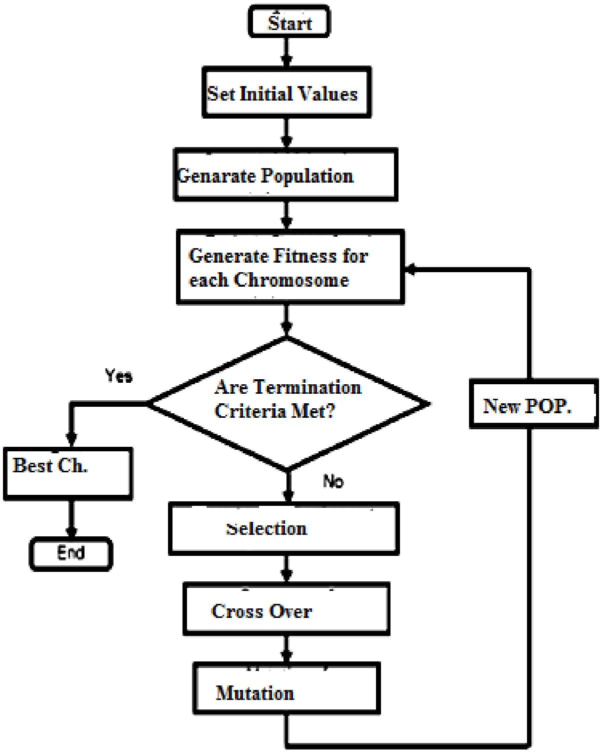


Figure 2: Genetic Algorithm Approach

3.4 Selection

This function plays the important role to encourage the average of population quality by choosing the high qualified chromosome for next generations. Selection is worked on fitness output. Every chromosome that has the best fitness value is chosen. This function plays the important role to encourage the average of population quality by choosing the high-qualified chromosome for next generations. Selection is worked on fitness output. Every chromosome that has the best fitness value is chosen.

3.5 Crossover

Crossover processes the current solutions to discover the better approach. In this mechanism, one or more than a bit of chromosome changes and a new population is generated. Genes are chosen from father’s chromosomes and make the new children.

3.6 Mutation

GA could fast access the required cost level. Mutation arbitrarily changes some bits of sequences and moves them to new location of available solution.

IV. PROPOSED PROTOCOL

In this paper, PAODV is introduced to enhance the AODV efficiency. PAODV removes the same routing messages, utilizes genetic algorithm to discover the better path in route discovery and also stores an alternative path and utilizes it when the connection failure takes place. To preserve this protocol security, same as AODV, digital signature and hash chain are utilized. This technique prevents PAODV from eavesdropping, external attack and black hole attack.

4.1 Propagation RREQ and RREP

When the source node requires a route to the destination node, it generates RREQ and floods it to all neighbours. Intermediary node obtains the RREQ packet and then examines the routing table. If there is a path to the destination node with higher sequence no., this intermediate node forwards the RREP to the source node by reverse path. Else, every intermediary node maintains its routing table and then forwards the RREQ to all neighbours until the destination obtains the message. During this process execution, some nodes may provide the same RREQ many times and flood it more than once, which decreases the nodes energy and increments the delay. The new technique has been designed in PAODV to prevent from replying the same routing message. When the node obtains the RREQ for the first time, it records its broadcast IP in the routing table. After that, whenever it obtains the RREQ with the same IP, it does not broadcast this message because it is reiterative. This solution causes decrement of routing delay and saves the nodes energy. As presented in fig 3, A is a source node and 1, 2, 3, 4 and 5 are intermediary nodes. A Broadcasts RREQ to all neighbouring nodes and it continues by others. Node 3 is a neighbour of 1 and 2. So it obtains RREQ from both 1 and 2 and broadcasts the same RREQ twice.

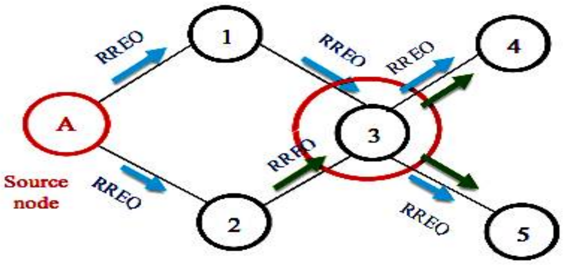


Fig. 3 Broadcasting RREQ in PAODV

In PAODV, when node 3 obtains the RREQ for the first time, it stores its broadcast IP. After that, whenever it obtains the RREQ, firstly it examines the routing table. If the current IP is same as the IP that available in routing table, the node removes the same RREQ and does not broadcast it. Else, the message is broadcast to its neighbouring nodes.

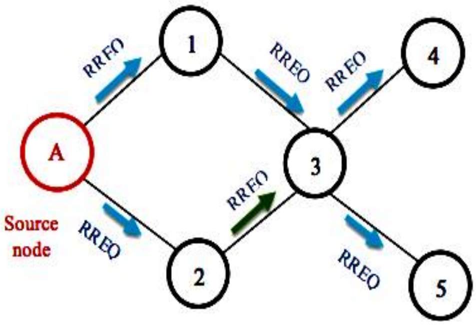


Fig. 4 Broadcasting RREQ in EPAODV

In the introduced protocol, this structure has also been implemented for RREP broadcasting. B is the target node and 4, 5, 6, 7 and 8 are the intermediary nodes.

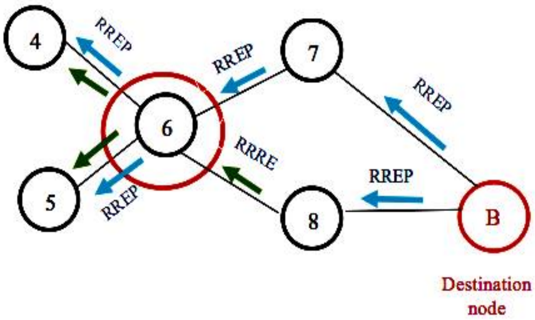


Fig. 5 Broadcasting RREP in PAODV

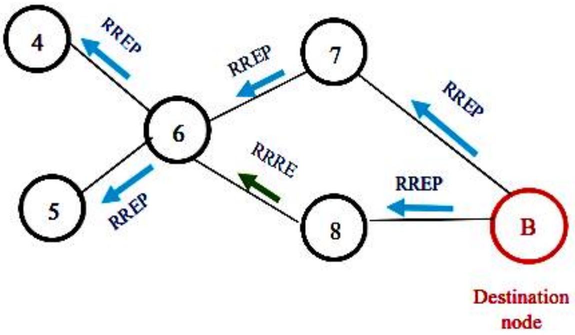


Fig. 6 Broadcasting RREP in EPAODV

4.2 Implementing the Genetic Algorithm

In the routing procedure, discovering a route, which has less delay, is a significant challenge. Smart algorithm is a type of algorithm that is utilized in optimization issues to determine the better solution. Genetic is one of the smart algorithms that measure the chromosome according to the objective. In PAODV, genetic algorithm is executed after the route discovery mechanism. The paths that are discovered from this process generate initial population. Fitness of this algorithm is computed depending on the delay. Every RREQ message has timestamp, which represents the message creation time. Route delay is the difference between routing current time (the time that message is obtained by the destination node) and RREQ timestamp.

rdelay = (CURRENT_TIME - rq_timestamp) (1)

rdelay is a variable that represents the delay. Current_time is a time that the message is obtained by the destination node. rq_timestamp is a time that the RREQ has been generated. According to the computed delay for every path, the path that has the minimum delay is chosen. So not only is the route selected depending on the hop-count, but also delay influences choosing it. Genetic algorithm both speeds the routing procedures and discovers the better route to forward the data. Because of the delay reduction, the lifetime of network is increased.

4.3 Alternative Path

After executing route discovery and genetic algorithm, the output of algorithm is chosen as a current route to forward the information. If connection failure takes place, route discovery mechanism in PAODV starts again. This mechanism increases the packet routing overhead.

EPAODV utilizes an optional path. In this technique, the second path is stored in nodes routing table. When the genetic algorithm is performed and the better path is chosen for forwarding the data, the second better path (which has the minimum delay except the first route) is chosen as an optional path. So when the connection failure takes place, the second path alternates the current route and forwards the information continues. To implement this technique, every node has rtcount function. This function represents the no. of the path to the target node. If this no. is lower than one, the second path is stored as an optional path. During the protocol execution, if the route with less delay is discovered, this route is changed with the optional path and the routing tables are updated. This technique importantly decreases the overhead of packet routing.

V. SIMULATION METHODOLOGY

A simulation tool ‘Riverbed is used for simulating AODV routing protocol and improving its performance on 150 and 200 nodes. OPNET is a network simulator that provides multiple solutions for managing networks and applications e.g. planning, network operation, research and development (R&D), network engineering and performance management. It allows the user to design and study the network communication devices, protocols, individual applications and also simulate the performance of routing protocol. It supports many wireless technologies and standards such as, IEEE 802.11, IEEE 802.15.1, IEEE 802.16, IEEE 802.20 and satellite networks.

Table 1: Simulation parameters

Simulation Parameters	
Examined Protocols	AODV
Number of Nodes	150, 200
Types of Nodes	Mobile
Simulation Area	50 x 50 km
Simulation Time	1200 seconds
Mobility	50 m/s
Pause Time	300 seconds
Performance Parameters	Throughput, Delay
Traffic type	FTP
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Wireless LAN MAC Address	Auto Assigned
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	256
Packet-Reception Threshold	95
Long Retry Limit	4
Max Receive Lifetime(seconds)	0.5
Buffer Size(bits)	256000

VI. RESULT AND ANALYSIS

The simulation studies involve network topology with 150 and 200 nodes. The proposed multipath algorithm s implemented in Riverbed. Results show that the proposed multipath algorithm improved the throughput value and decreases the delay. Fig 7 and fig 8 shows throughput comparison between normal and PAODV.

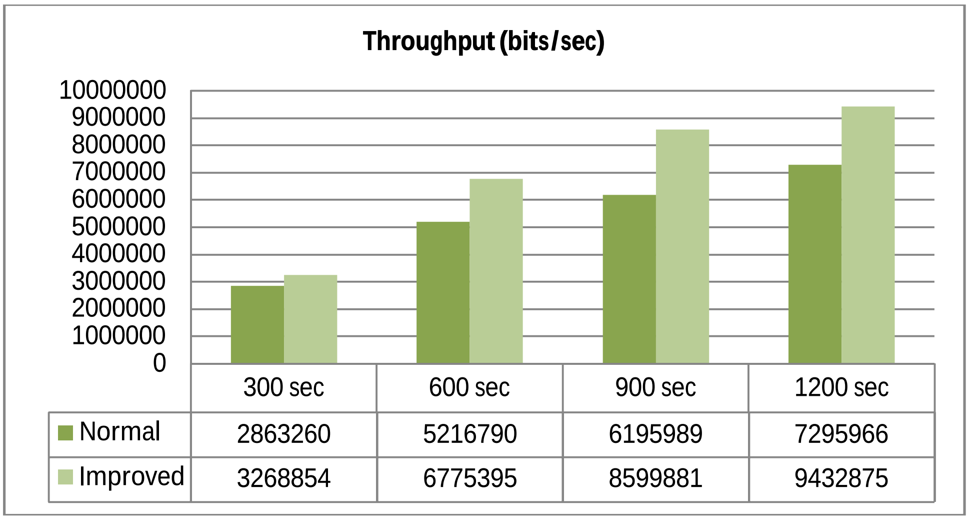
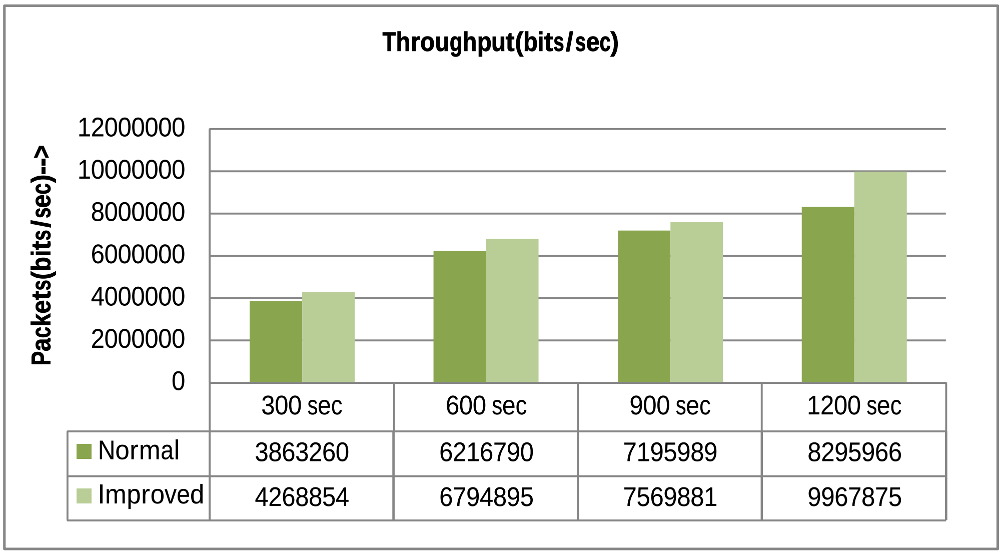


Fig 7: Throughput Comparison of at 150 nodes

DOI: 10.15680/IJIRCCE.2016. 0406093



	300 sec	600 sec	900 sec	1200 sec
🟩 Normal	3863260	6216790	7195989	8295966
🟩 Improved	4268854	6794895	7569881	9967875

Fig 8: Throughput Comparison of at 200 nodes

VII. CONCLUSION

In this research paper, PAODV routing protocol with changing no. of vehicles and a static speed of 50 meter per second with 300s pause time has been measured and enhanced. AODV protocol is measured and enhances with respect to throughput. The simulation model of VANET network is modeled utilizing Riverbed simulator and examined and enhances for AODV routing protocol. We used some methodology to enhance the AODV protocol performance by genetic approach and build PAODV routing protocol. We used this enhanced AODV (PAODV) to different no. of nodes i.e. 150 and 200 and concluded that this is efficient in all the situations. It is concluded that PAODV has better QOS i.e. end to end delay and throughput in comparison of AODV protocol.

REFERENCES

[1] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013

[1] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[3] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[4] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[5] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[6] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[7] Sherali Zeadally, Ray hunt and Yuh Shayan Chan, “Vehicular Ad hoc Networks (VANETs): Status, Results and Challenges” In Proceeding of Springer Science, Dec. 2011, pp. 217-241.

[8] Sun Xi and Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," In proceeding of Wireless Communications, Networking and Mobile Computing, 2008. 4th International Conference on Vehicular Ad hoc Networks, 2008, pp.1-4.

[9] ThodetiSrikant, Dr.V.B.Narsimha, “Simulation-based approach to performance study of routing protocols in MANETs and ad-hoc Networks”, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.9, pp. 111-115, September 2011.

[10] OmidAbedi, Reza Barangi, M. AbdollahiAzgomi, “Improving route stability and overhead of the AODV routing protocol and makeing it usable for VANETs”, 29th IEEE International Conference on Distributed Computing Systems Workshops , pp. 464-467, 2009.

[11] Rahul Kumar, Monika Sachdeva, “Performance Evaluation of AODV Protocol in MANET Using OPNET”, pp. 228-232.

[12] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011

[13] Bhoi, S.K.; Khilar, P.M., "A Proficient routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal Processing (ICCSP), 2013 International Conference on* , vol., no., pp.1170,1174, 3-5 April 2013

[14] Prabha R.,Ramaraj N., “An improved multipath MANET routing using link estimation and swarm intelligence”, EURASIP Journal on Wireless Communications and Networking , 2015.

[15] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[16] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," *Communications Surveys & Tutorials, IEEE* , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[17] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Proficient and Privacy-Preserving Navigation," *Computers, IEEE* Transactions *on* , vol.63, no.2, pp.510,524, Feb. 2014

[18] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[19] Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," *Systems and Informatics (ICSAI), 2014 2nd International Conference on* , vol., no., pp.536,541, 15-17 Nov. 2014

[20] Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on* , vol., no., pp.301,305, 4-6 July 2012.