International Journal of Soft Computing 11 (2): 45-51, 2016
ISSN: 1816-9503

An Enhanced Routing Protocol of VANET Using Trust Computing Algorithms

Thangakumar Jeyaprakash and Rajeswari Mukesh
Department of CSE, Hindustan Institute of Technology and Science, Chennai, India

Abstract: To avoid a frequent communication link failure and to provide a trusted routing among the vehicles, we are proposing an Optimized Node Selection Routing Protocol of VANET using a trust model. The proposed routing protocol is designed to find the optimized node for the transmission of data from the source node to the destination to achieve a trusted communication and high packet delivery ratio. To prove the performance of proposed routing protocol, performance metrics such as packet delivery ratio and end to end delay are evaluated and compared with existing routing protocols using ns2.

Key words: Routing protocol, trust, vehicular adhoc networks, delivery ratio, destination

INTRODUCTION

When using a reactive routing protocol, due to mobility of vehicular ad hoc networks, link failure is the major problem when transmitting the messages from the source node to the destination nodes. Due to the link failure of nodes, routing loops occurs. The routing protocol communication overhead increases by sending the frequent route discovery messages again to do the link repair. Route stability will be decreased. To avoid this, we are proposing Optimized Node Selection Routing Protocol approach (ONSRP). By selecting the optimized node in the VANET, the packet delivery ratio can be increased and the communication delay can be reduced. Trust is one of the most important aspect in the communication of VANET. Denial of Service (DOS) attack (Caballero-Gil, 2011) and sending of false warnings will be happening possibly by the attackers. Injecting false, modified and repeated messages will leads to exploit the VANET in different situations. An attacker is an entity who wants to spread the false information to other nodes to make the VANET functioning improperly.

LITERATURE REVIEW

Eiza and Ni (2013) used the evolving graph theory to model the VANET communication graph on a highway. The proposed model capture the evolving characteristics of the vehicular network topology and determines the reliable routes pre-emptively. Due to the evolving Graph algorithm, the communication overhead and delay may be increased.

Gupta and Sharma (2014) introduces different categories of ad-hoc routing protocols and reviewed several locations based routing protocols. In this survey study, researchers concentrated in reducing control packet overhead, maximize throughput and minimize the power consumption and end to end delay for the location based routing protocols only in MANET.

Bhalodi (2014) states when route break will generate at that time intermediate node send route error packet to source and source has another route in its routing table. This secondary route will work as an active route in data transfer. Due to the secondary route in data transfer, network delay will be increased due to the frequent route discovery process.

Jaballah *et al.* (2014) described a fast and secure multihop broadcast algorithm for vehicular communication which is proved to be resilient to the various attacks of vehicular ad hoc networks. The study is restricted to provide the multihop broadcast algorithm for the secure communication but not for other parameters like packet delivery ratio, network delay and routing overhead.

Mershad *et al.* (2012) exploited the infrastructure of Roadside Units (RSUs) to efficiently and reliably route packets in VANETs. Researchers evaluated the performance of the system using the ns2 simulation platform and compare the scheme to existing solution such as TrafRoute protocol.

Song *et al.* (2011) constructed the routing based on the road-to-road pattern than the traditional node-to-node routing pattern in MANETs called Buffer and Switch (BAS). The study is provided the routing based on road to road which will be the additional overhead for the routing considerations when forwarding the packet from the source to the destination.

Corresponding Author: Thangakumar Jeyaprakash, Department of CSE, Hindustan Institute of Technology and Science, Chennai, India

Chandrika and Papanna (2013) concentrated in reducing control packet overhead, maximize throughput and minimize the power consumption and end to end delay for the reactive routing protocols only in MANET. Researchers provides an overview of reactive protocols (e.g.: AODV, DSR, TORA, LAR) (Chandrika and Papanna, 2013).

Al-Janabi *et al*. (2012) provides the Bus Ad Hoc On-demand Distance Vector (BAODV) Routing Protocol for the VANET. BAODV is suitable with the minimum number of vehicles (buses) and it minimized end to end packet delay in the network. Cho and Ryu (2012) mentioned that each node forwards packets to other intermediate nodes that are constantly nearer to the packet's destination (greedy forward). In this study, researchers mentioned that it may cause high packet loss and more latency time due to the large number of hops in perimeter forwarding mode.

Gadkari and Sambre (2012) introduces different VANET routing protocols, security issues and simulation tools. In this study, researchers concentrated in reducing control packet overhead, maximize throughput, minimize the power consumption and end to end delay for the VANET routing protocols.

In Fig. 1, researchers have mentioned the tactical information management system between unmanned vehicles in military areas. In this study, Jeyaprakash and Mukesh (2013), researchers doesn't mention any trust based routing protocol for the communication of MANET.

Argyroudis and O'Mahony (2005) formulated the threat model for the ad hoc networks and mentioned specific attacks that can target the operation of Routing protocol. The several specific attacks discussed in this study are location disclosure, black hole attack, replay, warmhole attack, Denial of service, routing table poisoning, etc. He also compared the set of secure ad hoc routing protocol of MANET and each protocol has a different set of operational requirements and provides protection against different attacks by utilizing particular approaches. Raya and Hubaux (2005) provides a detailed threat analysis such as bogus information, cheating with positioning information, ID disclosure of other vehicles, Denial of service, etc. and describes an appropriate security architecture. The reviewed routing protocols are differs in architecture but the goal is to reduce the communication overhead, maximize the throughput and end to end delay.

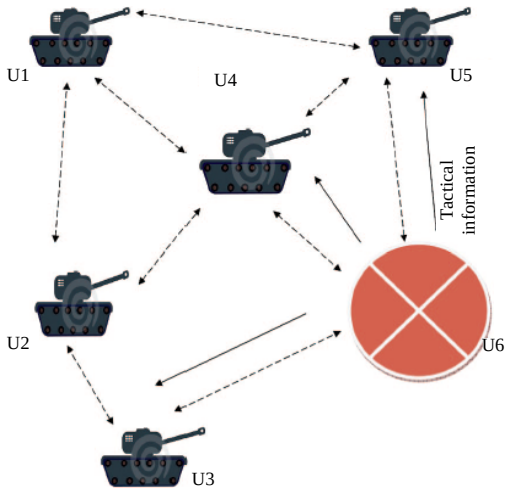

Fig. 1: Sharing of information from damaged UGV (Jeyaprakash and Mukesh, 2013)

EXISTING WORK

Al-Rabayah and Malaney (2012) proposed a new hybrid routing protocol for VANET which combines the features of location and topology based routing protocols. They combine the protocols in such a way that if the location information is degraded, it automatically uses the reactive routing protocol to transmit the packet from the source to the destination. The route discovery starts with the geographic routing and again route discovery will be initiated, if the location routing is degraded.

In Fig. 2, consider a Vehicular Ad Hoc Network. Each node may be a static node or an dynamic node. When a source node S needs a route to a destination node and there is not the valid route in the routing table, the source node broadcasts a Route Request Packet (RREQ) to the destination node D. When each node receives the RREQ, if it does not have a valid route to the destination node in the routing table, it rebroadcasts the RREQ. Once the

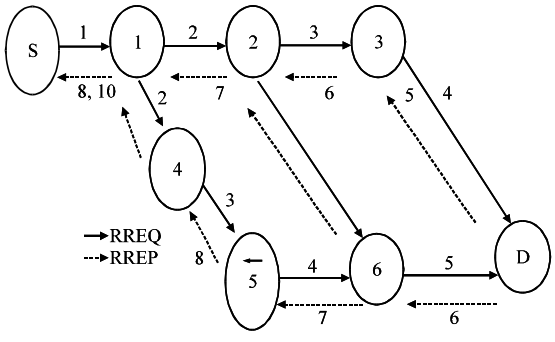

Fig. 2: Route discovery process; Path 1: S→1→2→3→D Hop Count: 4; Path 2: S→1→2→6→D Hop Count: 4

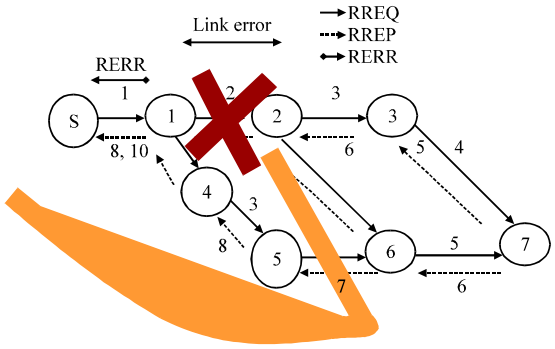

Fig. 3: Route link failure

RREQ broadcasts towards the destination node, the destination node forwarded the RREP to the source node and creates the reverse route with the sequence number. When the RREP reaches the source node with the sequence number incremented, the source node starts communicating with the destination node. If the intermediate node has the updates about the destination node, it will stop broadcasting the RREQ and creates the reverse route to the source node.

In Fig. 3, due to the link error between node 1 and 2, the multicasting packet will be move towards 2 with the hop count 4 for the dissemination of messages now the source has to do the route discovery by sending the RREQ for the communication after it received the RERR (Route Error) message. The communication overhead has been increased due to link error using SHR-AODV protocol. This problem can be recovered using optimizing node Selection Routing protocol.

PROPOSED WORK

Optimised Node Selection Routing Protocol (ONSRP): To avoid the link failure and routing loops, we have proposed a new enhanced trusted routing protocol algorithm for high mobility; each node maintains a Flag Trust database routing table that stores the signal strength based on distance, direction and velocity of the nodes and trust information of neighbour nodes. It can therefore be classified as Optimized Node Selection Routing Protocol approach (ONSRP).

In Fig. 4, the node N2 detects the weak link with N3 and notifies about the weak link to the node N1. Now the node N1 creates and updates the routing table flag as 0 for the destination IP address N3 with the next node as N2. Due to the weak link, the node N2 creates and updates the routing table flag as 0 for the destination IP address N3 with the next node as N3. Now, with the knowledge of

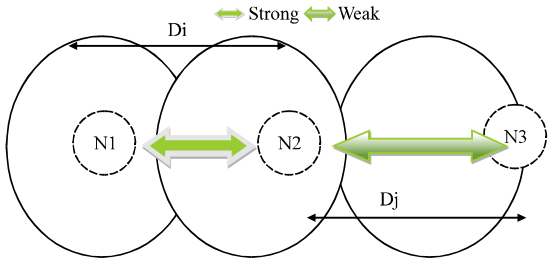

Fig. 4: Signal strength between two nodes

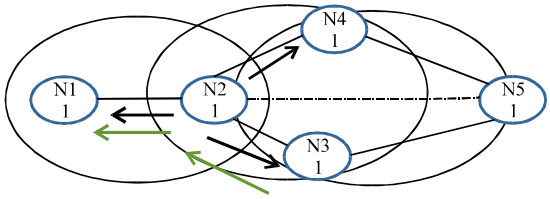

Fig. 5: Instance formation of VANET

weak link between node N2 and N3, N1 will broadcast a RREQ to find the destination as N2 knows about the situation and it will discard the RREQ from N1 and it will never forward the RREQ again. The RREQ broadcasted towards the destination will reach the other node nearer to N3 will send a RREP to the intermediate nodes. Once the intermediate nodes has been received the RREP, the reverse route has been formed up to N1 and now the node N1 will creates and updates the new route in the routing table. Apart from this, if a link error is happened, this will be stored immediately in the neighbour hop to avoid the RREQ broadcast.

Distance: In Fig. 5, assume that in this example node N1-N5 are moving in the same direction at the same speed. When node N1 wants to establish a route to node N5, N1 computes a distance value in kmps for transmits the packet to the destination based on available position information. If distance information is available (e.g., from a route that was established), a distance threshold value is defined to compare as the set of distance values available to transmits the packet. In this case, nodes will forward the route discovery packet only if they are within the threshold distance value. This type of RREQ is shown in Fig. 2. A node is allowed to forward the packet again only if it is at most some flag trust value is 1. In order to determine this direction, a node calculates the direction of the neighbor node as follows. At time T1:

$$\text{Distance (Do)} = \prod \text{Minimum (D1||D2||D3...Dn)} \quad (1)$$

Where:

$$Dn = \sqrt{(x1-x2)^2+(y1-y2)^2} \quad (2)$$

Where:

D1 = Distance between the last node of path 1 routing table and the destination node

D2 = Distance between the last node of path 2 routing table and the destination node

DN = Distance between the last node of path N routing table and the destination node

Direction of nodes: In Fig. 5, N1 be the source and N5 be the destination. In ONSRP, the sender N1 of a packet with destination N5 will forward the packet to all one-hop neighbours that lie in the in the same direction. In order to determine this direction, a node calculates the direction of the neighbour node as follows. At time T1, angle in degrees:

$$(Ao) = \prod D\,(RWP(i, j)) \,\&\, Min(D1||D2...Dn)(i, j) \quad (3)$$

Where:

$$Dn = \sqrt{(x1-x2)^2+(y1-y2)^2}$$

Where:

D1 = Distance between the last node of path 1 routing table and the destination node

D2 = Distance between the last node of path 2 routing table and the destination node

DN = Distance between the last node of path N routing table and the destination node

D = Destination

RWP = Random Way Points in the network

i, j = Two successive random way points

Velocity: In the following, we utilize the velocity of nodes parameter from viewpoint to develop our Flag Trust Model. We consider the velocity distribution over simulation of network to determine the network connectivity status. The velocity of nodes is the main parameter that determines the network topology dynamics. It also plays a significant role in determining the estimated communication time between two vehicles. At time T:

$$Velocity(Vo) = \prod V(Dn)||V(N1||N2||N3...Nn) \quad (4)$$

Where:

Dn = Destination node

N1 = Velocity of neighbour node 1 of Dn

N2 = Velocity of neighbour node 2 of Dn

Nn = Velocity of neighbour node n of Dn

Vo = Optimized velocity

Trust Computing algorithm to calculate O(n):

```
//Implements the Trust Computing for the Optimised Node  O(n)
//Input: An Array of nodes (A[0….n-1]] nearer to the destination
//Output: Calculates the trust value to set the flag value of the node 0 or 1
to find the Optimized nodes O(n).

i←0; j←0; k←0
t_count←α; d_threshold←β;
No of times data forwarded←•
count←0; trust←0;
for i←0 to n-1 && Do≥β do
        Do = Minimum_Distance_of_Node (i, j);
        Swap A[j] = A[i];
        return A[j];
for j←i+1 to (n-1-i) && O' ↑ A[n-1] do
        O' = ((Xi, Yi) (A[j], (A[n-1])));
        swap A[k] = A[j];
        return A[k];
for k←i+j+1 to (n-1-i-j) && V≤A[n-1] do
        if V(A[k])≥ V (A[n-1])
        return V(A[k]);
        swap O(n) = V(A[k]);
        α(O(n)) = count++;
        else return-1
if (α(O(n)≥ • ))
        SET flag (O(n)) = "1"
        else SET 0;
```

Computation of distance (i, j):

```
//Implements the Minimum_Distance_of_Node (i, j)
//Input: An Array of nodes (A[0...n-1]] nearer to the destination
//Output: Calculates the distance value from node 0-n-1
i←0; j←0; vertex←0;
distance←0;
for i←0 to n−1 do{
    for j←1 to n−2 do{
            if (j! = i){
            set x_pos1 [n(i) set X];
                    set x_pos2 [n(j) set X];
                    set y_pos1 [n(i) set Y];
                    set y_pos2 [n(j) set Y];
    vertex = x_pos1*x_pos2+y_pos1*$y_pos2;
                    distance (i, j) = sqrt(vertex);
                    print dist "Node i to j: ds(i, j)
            }
    }
}
```

From Eq. 1, 2 and 4, trust value has been calculated:

$$Flag\ Trust = \sum Do.Ao.Vo.FlagTrustCount \quad (5)$$

Where, i = 1 to n; at time T1, from Eq. 1 and 2:

$$Distance\ (Do) = \prod Minimum\ (D1||D2||D3...Dn)$$

Where:

$$Dn = \sqrt{(x1-x2)^2+(y1-y2)^2}$$

At time T1, from Eq. 3 and 4:

$$Velocity\ (Vo) = \prod V\ (Dn)||V(N1||N2||N3...Nn)$$

At time T3:

$$\text{Angle in degrees (Ao)} = \prod D\ (RWP\ (i, j)) \ \&\ Min\ (D1||D2||D3...Dn)\ (i, j))$$

Where:

D1 = Distance between the last node of path 1 routing table and the destination node

D2 = Distance between the last node of path 2 routing table and the destination node

DN = Distance between the last node of path N routing table and the destination node

x1, y1, x2, y2 = Location coordinates

After the FlagTrust value has been calculated, it will be compared with the threshold value to update the value of flagTrust in the routing table. The FlagTrust value has been updated as 0 and 1.

RESULTS AND COMPARISONS

We have tested the simulation to evaluate the performance of enhanced Trust-Based hybrid routing protocol for the communication of unmanned ground vehicles using optimized node selection routing protocol in three phases using ns2. The proposed protocol has been compared with Scalable Hybrid Routing protocol-Ad hoc on Demand Vector (SHR-AODV).

Phase 1 (DRS-ONSRP): The first phase has been simulated with the parameters of Distance (Do) and RSSI (Received Signal Strength Index):

$$RSSI\ (Pr\ (do)) = Ct \times Pt/d^4 \times Pl \quad (6)$$

Where:

Pt = Transmitted power (Sebastian and Jeyaprakash, 2014)

Ct = Tranceiver constant

Pl = Packet loss

Phase 2 (AVT-ONSRP): The second phase has been simulated with the parameters of Angle(Ao), Velocity(Vo) and FlagTrust count). From Eq. 2:

$$\text{Angle in degrees (Ao)} = \prod D\ (RWP\ (i, j)) \ \&\ Min(D1||D2||D3...Dn)\ (i, j))$$

From Eq. 3:

$$\text{Velocity (Vo)} = \prod V(Dn)||V(N1||N2||N3...Nn)$$

Phase 3 (DAVT-ONSRP): The combination of first and second phase has been integrated in the third phase to find trust node. At time T1 from Eq. 1, 2 and 4:

$$\text{Distance (Do)} = \prod \text{Minimum}\ (D1||D2||D3...Dn)$$

$$\text{Angle in degrees (Ao)} = \prod D\ (RWP\ (i, j)) \ \&\ Min\ (D1||D2||D3...Dn)\ (i, j))$$

$$\text{Velocity (Vo)} = \prod V\ (Dn)||V\ (N1||N2||N3...Nn)$$

$$\text{FlagTrust} = \sum \text{Do. Ao. Vo. Maximum Trust Count}$$

Simulation parameters: Simulation has been done by executing trust computing algorithms simulations compared with the existing Scalable Hybrid Routing Protocol (SHR-AODV). In Table 1, the simulation transmission of data packet transfer rate is considered as 8 packets/sec. For each set of simulation parameters, each protocol is subjected to an identical sequence of random events. To prove the performance of proposed routing protocol.

In Table 2, the performance metrics such as delay and packet delivery ratio for the node density up to 100 of ONSRP and SHR has been compared and the result analysis shows the is optimal in the presence of link failures with efficient packet delivery ratio. More specifically, we can confirm that the ONSRP is optimal by comparing to the Scalable Hybrid Routing (SHR) communication overhead and packet delivery ratio of the network from both analysis and simulation in the presence of link failures. In Fig. 6-8, we show the performance of ONSRP and Scalable hybrid routing using the performance metrics of the packet delivery ratio and the end to end delay for the highway scenario with 20-30 random source-destinations. The graph shows clearly there is an increase in the packet delivery ratio of ONSRP

Table 1: Simulation parameters

Parameters	Values
Simulation time	1500 sec
Simulation area	1000×1000 m
Data pay load	512 bytes/packet
Bandwidth	2 Mbp
Routing protocols	SHR-AODV, ONSRP
Packet rate	8 packets/sec
No. of nodes	25,50,75,100
Node pause time	60
Channel type	Wireless channel
Antenna type	Omni directional

Table 2: Performance measures comparison

Performance metrics	Node density	SHR-AODV	ONSRP
Delay (sec)	25	1.13	0.18
Packet delivery ratio	25	0.63	0.84
Delay (sec)	50	2.56	1.59
Packet delivery ratio	50	0.61	0.82
Delay (sec)	100	2.78	1.63
Packet delivery ratio	100	0.60	0.83

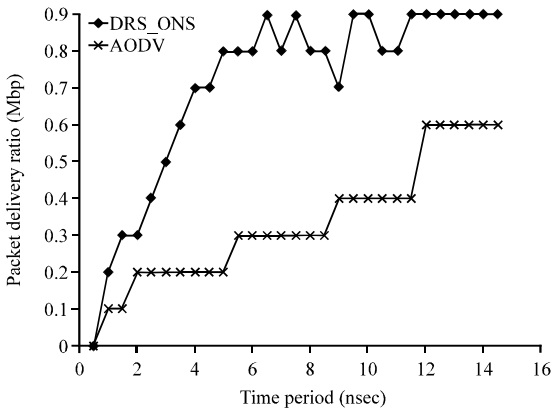

Fig. 6: Packet delivery ratio plot

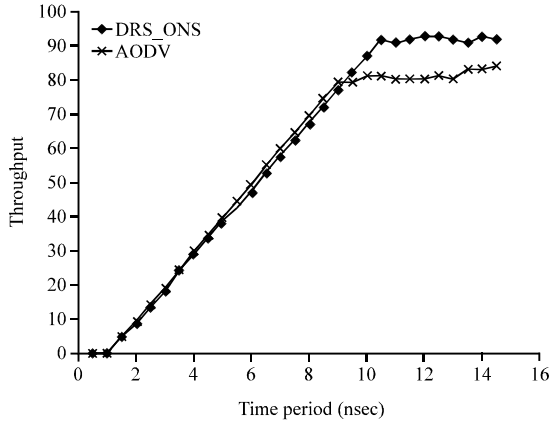

Fig. 7: Throughput plot

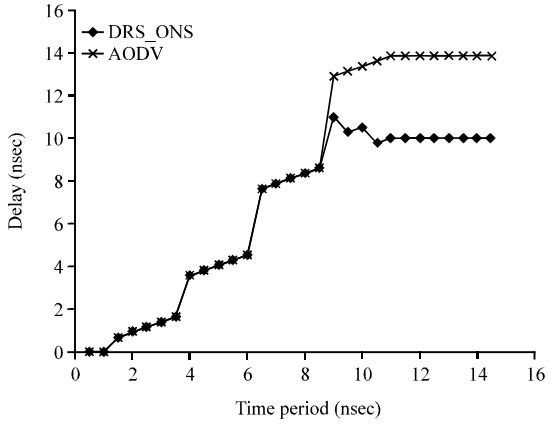

Fig. 8: End to end delay plot

compared to SHR. On the other scenario, for ONSRP, the increasing density is reducing the communication overhead also by avoiding the frequent route discovery process.

CONCLUSION

In this study, we have evaluated an Optimized Node Selection Routing Protocol approach (ONSRP) using Trust Computing algorithms. Here we proposed an extended light weight routing technique and the routing messages with trust information which can be updated directly through optimized node selection Routing Protocol algorithm. When performing trusted routing discovery, communication overhead can be reduced and the packet delivery ratio can be increased by avoiding frequent route discovery process.

REFERENCES

Al-Janabi, S.T.F., Y.S. Yaseen and B. Askwith, 2012. The Bus Ad hoc On-demand Distance Vector (BAODV) routing protocol. Proceedings of the 13th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting, June 25-26, 2012, Liverpool, UK.

Al-Rabayah, M. and R. Malaney, 2012. A new scalable hybrid routing protocol for VANETs. IEEE Trans. Veh. Technol., 61: 2625-2635.

Argyroudis, P.G. and D. O'Mahony, 2005. Secure routing for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 7: 2-21.

Bhalodi, C., 2014. Modified route maintenance in AODV routing protocol. Int. J. Adv. Eng. Res. Dev., 1: 1-9.

Caballero-Gil , P., 2011. Security issues in vehicular Ad Hoc networks. Ph.D, Thesis, University of La Laguna, Spain.

Chandrika, M. and N. Papanna, 2013. A survey on reactive protocols in mobile Ad hoc networks. Int. J. Adv. Res. Comput. Sci. Software Eng., 3: 387-391.

Cho, K.H. and M.W. Ryu, 2012. A survey of greedy routing protocols for vehicular Ad Hoc networks. Smart Comput. Rev., 2: 125-137.

Eiza, M.H. and Q. Ni, 2013. An evolving graph-based reliable routing scheme for VANETs. IEEE Trans. Vehicular Technol., 62: 1493-1504.

Gadkari, M.Y. and N.B. Sambre, 2012. VANET: Routing protocols, security issues and simulation tools. IOSR J. Comput. Eng., 3: 28-38.

Gupta, A. and S.D. Sharma, 2014. A survey on location based routing protocols in mobile Ad-hoc networks. Int. J. Comput. Sci. Inform. Technol., 5: 994-997.

Jaballah, W.B., M. Conti, M. Mosbah and C.E. Palazzi, 2014. Fast and secure multihop broadcast solutions for intervehicular communication. IEEE Trans. Intell. Transp. Syst., 15: 433-450.

Jeyaprakash, T. and R. Mukesh, 2013. A tactical information management system for unmanned vehicles using vehicular ad hoc networks. Proceedings of the IEEE 4th International Conference on Intelligent Systems, Modelling and Simulation, January 29-31, 2013, Bangkok, Thailand, pp: 472-474.

Mershad, K., H. Artail and M. Gerla, 2012. We can deliver messages to far vehicles. IEEE Trans. Intell. Transp. Syst., 13: 1099-1115.

Raya, M. and J.P. Hubaux, 2005. The security of vehicular ad hoc networks. Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, November 7, 2005, ACM Press, Alexandria, VA., USA., pp: 11-21.

Sebastian, N.V. and T. Jeyaprakash, 2014. Appraising vehicular Adhoc networks routing protocols using ns2. Int. J. Inform. Comput. Technol., 4: 491-498.

Song, C., M. Liu, Y. Wen, J. Cao and G. Chen, 2011. Buffer and switch: An efficient road-to-road routing scheme for VANETs. Proceedings of the 7th International Conference on Mobile Ad hoc and Sensor Networks, December 16-18, 2011, Beijing, pp: 310-317.