ISSN (Print): 0974-6846
ISSN (Online): 0974-5645
Indian Journal of Science and Technology, *Vol 12(16), DOI: 10.17485/ijst/2019/v12i16/144169, April 2019*

Secure and Intelligent QoS aware Routing Protocol for VANET Environment

S. Gayathri[1], J. Granty Regina Elwin[2]*, Reshma B. Nair[2], K. Ranjeethapriya[2] and R. Ramesh Kumar[2]

[1]Department of Computer Science and Engineering, Amrita School of Engineering,
Amrita University, Coimbatore - 641112, Tamilnadu, India; gayathri24coolgal@gmail.com
[2]Department of Information Technology, Sri Krishna College of Engineering and Technology,
Coimbatore - 641008, Tamilnadu, India; grantyregina@gmail.com, reshmab@skcet.ac.in,
ranjeethapriyak@skcet.ac.in, ramesh4477@gmail.com

Abstract

Objectives: To propose a suitable protocol that is secured and efficient for data transmission in Vehicular Adhoc Networks (VANET) environment. **Methods/Statistical Analysis:** The main challenge in VANET is to protect valuable information from the users. However there are many malicious vehicles that affect the system. To overcome this problem, the Secure and Intelligent routing (SIR) protocol is used that will transmit the data in shortest path through the authenticated vehicles. The proposed method makes use of message transmission, link connectivity and vehicle positioning to forward the data to the destination. Sending the data through the QoS based optimized path will enhance the performance of the system. Hence the proposed Enhanced Secure and intelligent routing (ESIR) protocol is QoS enabled and optimized. The QoS metrics taken into concern are delay, network load and distance with minimum number of hops. Particle Swarm Optimization (PSO) algorithm used for optimization in the proposed work takes one main parameter into concern; it is distance with minimum number of hops. **Findings:** The proposed technique is compared with the existing SIR protocol in terms of throughput, delay, packet delivery ratio, residual energy levels and packet drop. The results obtained show that the proposed technique serves as an efficient routing protocol for VANET environment providing a reliable and robust service.

Keywords: Particle Swarm Optimization, QoS Parameters, Shortest Path, VANET

1. Introduction

VANET (Vehicular Adhoc Networks) is a network with dynamic topology where nodes move at fast speed. It has more processing power, storage and energy than handhelds. In general, VANET uses location based information to detect any accidents that occur in the network. In VANET, the communication in the network is of two types. They are Vehicle-to-Vehicle communication (v2v) and Vehicle-to-Infrastructure communication (v2I). In our environment we use both v2v as well as v2I communications.

According to Figure 1, the vehicles communicate with each other and they communicate with the Infrastructure too. Hence they use both v2v and v2I communications. The main challenge is to reduce the delay constraint during communication in the network, by deploying intelligence. There are many goals in VANET. They are

- VANET can be used to improve traffic safety and provide comfort for the drivers.
- The main goal of VANET is to minimize accidents and traffic intensity.
- VANET must provide up-to-date traffic information.
- VANET can provide weather information as well as vacancies in the parking lots.

All these goals can be achieved by sending data to all the vehicles in the network. Hence we must ensure that the data sent is secured.

In this study we will propose a protocol that is secure and is efficient for data transmission in VANET environment. To begin with, Section II explains some existing works about the routing protocols in VANET environment. Section III is the detailed work plan of the existing work. Section IV is the detailed plan of the

*Author for correspondence

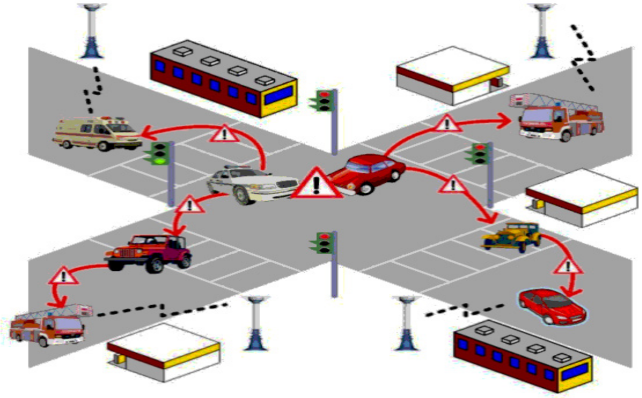


Figure 1. Vehicular networks communication.

proposed work. Section V is the simulation. Section VI presents the result and analysis of the proposed work. Finally, Section VII gives the conclusion.

2. Literature Survey

Many efficient routing protocols (Broadcast, Geocast, Clustering, Position-based and beaconing) are proposed for VANET[1,2].

In[1,3] planned a greedy traffic aware routing (GyTAR) protocol to send the information expeditiously. This protocol uses the cell information packet to seek out score of its neighboring junction. However, this suffers from congestion as a result of the cell information packets area unit changed at high rate. Moreover, it's an insecure routing protocol that's full of the attackers within the network.

Anchor-based street and traffic aware routing (A-star)[1,4] could be a routing protocol wherever the information is forwarded in a very pre-defined path. The most disadvantage of this protocol is, it lacks current traffic info.

Securing the optimized link state routing (SOLSR)[1,5] could be a secure OLSR protocol that's accustomed give authentication to the information packets and helps in protective the network from replay attacks. It uses symmetrical key cryptography that helps in reducing computation overhead within the network. However this protocol lacks data regarding the network gaps and conjointly will increase delay within the network.

Time efficient Stream loss-tolerant authentication[1,6] could be a broadcast authentication wherever HMAC is employed for security. This lacks data regarding network gaps and thus will increase path length also as delay within the network.

A QoS-based clustering protocol named as VANET-QoS-OSLR is planned[7,8]. The goal is to create stable clusters and maintain stability and link property within the network. This routing protocol is evaluated with ACO (Ant-colony optimization) algorithmic program. The most disadvantage is it will increase delay within the network.

3. Secure and Intelligent Routing (SIR) Protocol

In SIR model, a Trusted Vehicle (TV)[1] is fixed at every Junction (location where multiple roads intersect). This TV will store beacon messages like vehicle id, speed, location and direction[1]. Hence, this TV will act as an intelligent system by communicating in the network.

Initially, the vehicles in the network exchange beacon messages at specific intervals to know their neighbouring vehicles. Vehicles in the network use Global position system service to know their own location[1]. The functionality of SIR starts by selecting a source vehicle V_s and destination vehicle V_D. The source vehicle V_s will contain data that has to be sent to the destination V_D in short time. To forward the data, V_s first finds the shortest path to destination by using Dijkstra's Algorithm[9] by considering the junctions[1]. Dijkstra's algorithm is used since it has less time complexity than any other shortest path algorithms. V_s forward the encrypted data to the neighbouring vehicles only after the verification of their genuineness. The Central Authority (CA) will provide valid certificate to the authenticated vehicles. Hence, the vehicles in the neighbouring field will verify the vehicle by validating the certificate 'C'. Vehicle with valid C is genuine vehicle while vehicles with invalid C are malicious vehicles[1]. Once again for more security reasons, the data that is being forwarded should not be altered during transmission. Hence the message is secured and protected by using Diffie-Hellman Key agreement protocol[10]. The vehicles will forward the encrypted data to the neighbouring genuine vehicles until it reaches the junction. The vehicle closest to the junction will forward the encrypted data to the TV. (TV is assumed to be trusted with previous history). The TV will calculate a weight W for every neighbouring junction and will forward the data to the junction that has minimum weight W[11].

The calculation of weight W is:

W = Shortest distance from current junction to the destination + total number of genuine vehicles + time of transmission between source and destination + total number of link connectivity between the vehicles.

Link connectivity = It is the link availability time of the vehicle in the network (the total time the vehicle is available in the network).

Hence, by calculating the weight W for each path, the TV will forward the data to the path that has minimum W^1. This process will continue until the encrypted data reaches the destination vehicle V_D. The destination vehicle will decrypt the data and will take proper decision.

4. Methodology - Sir with QoS and Pso

From the existing SIR protocol (including Intelligent system (TV), beacon message for neighbour discovery, 'C' certificate), the proposed Enhanced Secure and Intelligent routing (ESIR) protocol adds up QoS metrics and Optimization concept.

In the existing SIR protocol for encryption and decryption of messages, Diffie-Hellman key exchange protocol was considered. The main drawback of Diffie-Hellman Key exchange protocol is the private key is smaller which can be easily decoded. Hence the proposed (ESIR) protocol uses RC4 (Ron's Code 4) algorithm for encryption and decryption of messages. Encryption works by running data through a Key. Both the sender and receiver should know this key for encrypting and decrypting the data.

The steps for RC4 algorithmic program is:

- Obtain the info to be encrypted and therefore the secret key.
- Generate 2 string arrays.
- Fill one array with numbers from zero to 255.
- Fill the opposite array with the key.
- Randomize the primary array betting on the array (second array) of the key.
- Randomize the primary array at intervals itself to come up with the ultimate key stream of Knowledge.
- XOR the ultimate key stream of knowledge with the info to be encrypted to offer cipher text.

The enhanced SIR (ESIR) considers three QoS metrics. They are delay, network load and distance with minimum number of hops. By considering these metrics, all possible paths from source to destination are obtained. From the above paths, we perform Particle Swarm Optimization (PSO) with distance between source and destination as parameter to get the best shortest path.

From all possible paths from source to destination, the ESIR protocol chooses path that has minimum delay with threshold less than 40%. From the chosen paths, the ESIR protocol again chooses path that have minimum network load with threshold less than 70%.

Particle Swarm Optimization (PSO) algorithm is used to identify feasible routes between source and destination. From the above selected paths, the algorithm finds the path that has minimum distance with less number of hops. Hence, the path having minimum distance with less number of hops is taken as the final path that can be used to traverse from source to destination. The basic concept of PSO is to iterate between the paths and find the best feasible path from source and destination.

The proposed work is:

- Initializing the system
- Computing all paths from source to destination
- Selecting paths that have minimum delay with threshold less than 40%
- From the above selected paths, choose paths with network load less than 70%
- Initialize the selected paths to a new array A[ ]
- For I = 1 to ITER
- Generating particles from A[ ]
- checking path that has minimum distance with less number of hops
- Updating the best path with less distance
- End for

By doing this we achieve a secure feasible path in the network.

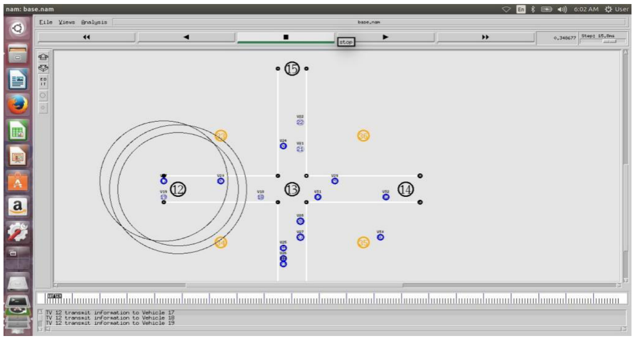
5. Simulation Results

The simulation is implemented in NS2 (Network Simulator). Simulation Results for the various parameters employed for performance evaluation is listed in Table 1.

The simulation environment consists of 5 junctions (12, 13, 14, 15, and 16) as shown in Figure 2. Source and destination points are received from the terminal. Once the source and destination is known we generate keys for individual vehicles as well as for the TV's. The keys generated are taken as session keys for communication between the vehicles in the network.

Table 1. Simulation for Performance evaluation

PARAMETERS	PARAMETER VALUES
Number of junctions	5
Vehicle speed	40–80 km/hr
Vehicle range	250 m
TV range	250 m
Number of RSU	4
Number of vehicles	30
Packet size	512 bytes

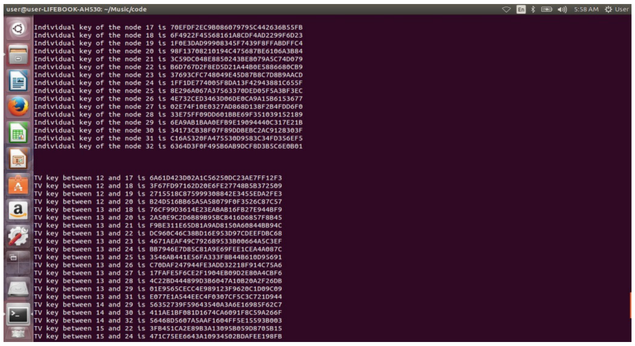


```
TV 12 transmit information to Vehicle 17
TV 12 transmit information to Vehicle 18
TV 12 transmit information to Vehicle 19
```

Figure 2. Simulation Environment.

Figure 3 shows the keys for individual vehicles and for TV's. The keys are generated randomly and are assigned for each vehicle and TV. With the help of these session keys, the vehicle will encrypt and decrypt data in the network. TV just transmits the data without decrypting. We use RC4 algorithm for encryption. Overhead of key generation between vehicle and TV are lesser as only one key is generated for one session from source to destination. Encryption and decryption is done end-to-end.

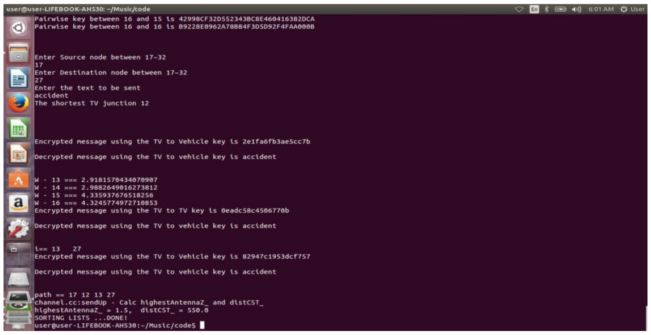
When the user enters the source and destination, the vehicles in the network will exchange beacon messages to know their neighbouring vehicles in the network. With this information, the TV at the junction will calculate the weight W for all the neighbouring TV's and will choose the path that has minimum W.



```
user@user-LIFEBOOK-AH530: ~/Music/code

Individual key of the node 17 is 70EFDF2EC9B086079795C442636B55FB
Individual key of the node 18 is 6F4922F45568161A8CDF4AD2299F6D23
Individual key of the node 19 is 1F0E3DAD99908345F7439F8FFABDFFC4
Individual key of the node 20 is 98F13708210194C475687BE6106A3B84
Individual key of the node 21 is 3C59DC048E8850243BE8079A5C74D079
Individual key of the node 22 is B6D767D2F8ED5D21A44B0E5886680CB9
Individual key of the node 23 is 37693CFC748049E45D87B8C7D8B9AACD
Individual key of the node 24 is 1FF1DE774005F8DA13F42943881C655F
Individual key of the node 25 is 8E296A067A37563370DED05F5A3BF3EC
Individual key of the node 26 is 4E732CED3463D06DE0CA9A15B6153677
Individual key of the node 27 is 02E74F10E0327AD868D138F2B4FDD6F0
Individual key of the node 28 is 33E75FF09DD601BBE69F351039152189
Individual key of the node 29 is 6EA9AB1BAA0EFB9E19094440C317E21B
Individual key of the node 30 is 34173CB38F07F89DDBEBC2AC9128303F
Individual key of the node 31 is C16A5320FA475530D9583C34FD356EF5
Individual key of the node 32 is 6364D3F0F495B6AB9DCF8D3B5C6E0B01



TV key between 12 and 17 is 6A61D423D02A1C56250DC23AE7FF12F3
TV key between 12 and 18 is 3F67FD97162D20E6FE27748B5B372509
TV key between 12 and 19 is 2715518C875999308842E3455EDA2FE3
TV key between 12 and 20 is B24D516BB65A5A58079F0F3526C87C57
TV key between 13 and 18 is 76CF99D3614E23EABAB16FB27E944BF9
TV key between 13 and 20 is 2A50E9C2D6B89B95BCB416D6857F8B45
TV key between 13 and 21 is F9BE311E65D81A9AD8150A60844BB94C
TV key between 13 and 22 is DC960C46C38BD16E953D97CDEEFDBC68
TV key between 13 and 23 is 4671AEAF49C792689533B00664A5C3EF
TV key between 13 and 24 is BB7946E7D85C81A9E69FEE1CEA4A087C
TV key between 13 and 25 is 3546AB441E56FA333F8B44B610D95691
TV key between 13 and 26 is C70DAF247944FE3ADD32218F914C75A6
TV key between 13 and 27 is 17FAFE5F6CE2F1904EB09D2E80A4CBF6
TV key between 13 and 28 is 4C22BD444899D3B6047A10B20A2F26DB
TV key between 13 and 29 is 01E9565CECC4E989123F9620C1D09C09
TV key between 13 and 31 is E077E1A544EEC4F0307CF5C3C721D944
TV key between 14 and 29 is 56352739F59643540A3A6E16985F62C7
TV key between 14 and 30 is 411AE1BF081D1674CA6091F8C59A266F
TV key between 14 and 32 is 56468D5607A5AAF1604FF5E15593B003
TV key between 15 and 22 is 3FB451CA2E89B3A13095B059D8705B15
TV key between 15 and 24 is 471C75EE6643A10934502BDAFEE198FB
```

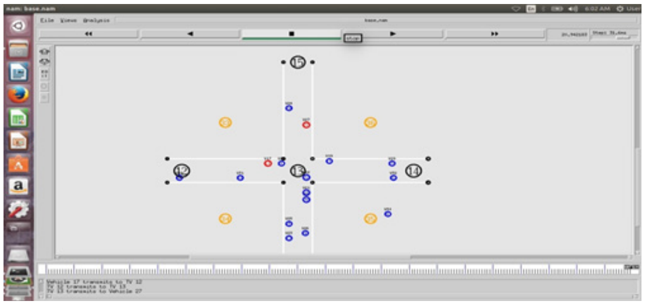
Figure 3. Keys for vehicles and TV.

In this simulation, the user entered 17 as source vehicle with message "accident" and has to be transmitted to the destination 27. Now the nearest TV for 17 is 12. Hence vehicle 17 will forward the encrypted data to TV 12. Now TV 12 will calculate W for the neighbouring TV's and TV 12 found that TV 13 is having minimum W than other TV's. Hence the data is forwarded to TV 13. Then TV 13 found that the destination vehicle 27 is nearby. Hence, it forwards the encrypted data to the destination and decryption is carried out by vehicle 27. The execution of this process is shown in Figure 4 and Figure 5 shows the simulation results of this execution.



```
user@user-LIFEBOOK-AH530: ~/Music/code
Pairwise key between 16 and 15 is 42998CF32D552343BC8E460416382DCA
Pairwise key between 16 and 16 is B9228E0962A78B84F3D5D92F4FAA000B



Enter Source node between 17~32
17
Enter Destination node between 17~32
27
Enter the text to be sent
accident
The shortest TV junction 12




Encrypted message using the TV to Vehicle key is 2e1fa6fb3ae5cc7b

Decrypted message using the TV to vehicle key is accident


W - 13 === 2.9181570434070907
W - 14 === 2.9882649016273812
W - 15 === 4.335937676518256
W - 16 === 4.3245774972710853
Encrypted message using the TV to TV key is 0eadc58c4506770b

Decrypted message using the TV to vehicle key is accident


i== 13   27
Encrypted message using the TV to Vehicle key is 82947c1953dcf757

Decrypted message using the TV to vehicle key is accident


path == 17 12 13 27
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
user@user-LIFEBOOK-AH530:~/Music/code$
```

Figure 4. Execution phase.

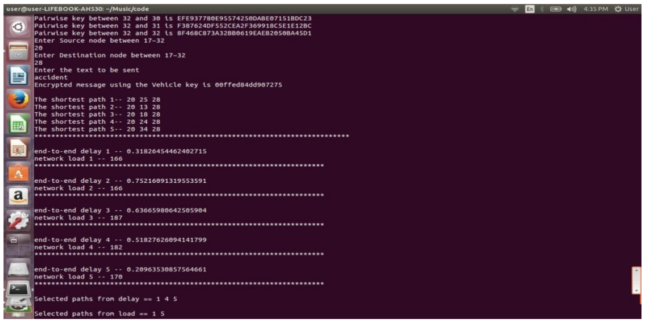


```
Vehicle 17 transmits to TV 12
TV 12 transmits to TV 13
TV 13 transmits to Vehicle 27
```

Figure 5. Execution result.

Here, the protocol has ensured that the data is being transmitted through authenticated vehicles and is traversed in shortest path to reach the destination at smallest time interval.

Using existing SIR protocol with QoS metrics, many possible paths from source to destination is obtained. From the possible paths, PSO algorithm is used to get the best optimal path, considering distance as the parameter. Use of PSO iteration in the proposed work is illustrated in Figure 6.



```
Pairwise key between 32 and 30 is EFE937780E95574250DABE07151BDC23
Pairwise key between 32 and 31 is F387624DF552CEA2F369918C5E1E12BC
Pairwise key between 32 and 32 is 8F468C873A32BB0619EAEB2050BA45D1
Enter Source node between 17~32
20
Enter Destination node between 17~32
28
Enter the text to be sent
accident
Encrypted message using the Vehicle key is 00ffed84dd907275

The shortest path 1-- 20 25 28
The shortest path 2-- 20 13 28
The shortest path 3-- 20 18 28
The shortest path 4-- 20 24 28
The shortest path 5-- 20 34 28
***************************************************************************

end-to-end delay 1 -- 0.31826454462402715
network load 1 -- 166
*********************************************************************

end-to-end delay 2 -- 0.75216091319553591
network load 2 -- 166
*********************************************************************

end-to-end delay 3 -- 0.63665980642505904
network load 3 -- 187
*********************************************************************

end-to-end delay 4 -- 0.51827626094141799
network load 4 -- 182
*********************************************************************

end-to-end delay 5 -- 0.20963530857564661
network load 5 -- 170
*********************************************************************

Selected paths from delay == 1 4 5

Selected paths from load == 1 5
```

Figure 6. Using PSO iteration.

When the user enters the source and destination vehicle at the terminal, many possible paths from the source and destination is obtained. In the above example, the user has given 20 as the source vehicle and 28 as the destination vehicle. Five possible shortest paths from 20 to 28 are obtained. They are

Path 1 – 20 25 28
Path 2 – 20 13 28
Path 3 – 20 18 28
Path 4 – 20 24 28
Path 5 – 20 34 28

From the obtained 5 paths, the algorithm will find the paths having delay less than the threshold value. Table 2 displays the delay values for the various paths.

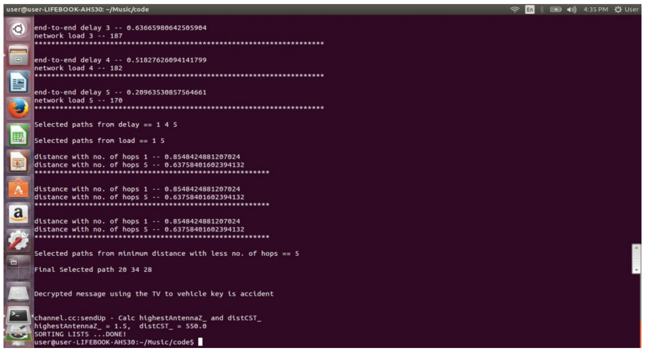
Table 2. Delay values

Path 1 – 20 25 28	0.318264
Path 2 – 20 13 28	0.752160
Path 3 – 20 18 28	0.636659
Path 4 – 20 24 28	0.518276
Path 5 – 20 34 28	0.209635

From this, path-2 and path-3 are eliminated as it falls at upper bound. Thereby the paths considered for next phase are: path-1 -- 20 25 28, path- 4 - 20 24 28, path-5 - 20 34 28. From the selected 3 paths, the algorithm will find the paths having network load less than 70% of the entire network load. Table 3 shows the network load values calculated for the paths remaining after elimination from the previous phase.

Table 3. Network Load values

Path 1 – 20 25 28	166
Path 4 – 20 24 28	182
Path 5 – 20 34 28	170



```

end-to-end delay 3 -- 0.63665980642505904
network load 3 -- 187
*********************************************************************

end-to-end delay 4 -- 0.51827626094141799
network load 4 -- 182
*********************************************************************

end-to-end delay 5 -- 0.20963530857564661
network load 5 -- 170
*********************************************************************

Selected paths from delay == 1 4 5

Selected paths from load == 1 5

distance with no. of hops 1 -- 0.8548424881207024
distance with no. of hops 5 -- 0.63758401602394132
********************************************************

distance with no. of hops 1 -- 0.8548424881207024
distance with no. of hops 5 -- 0.63758401602394132
********************************************************

distance with no. of hops 1 -- 0.8548424881207024
distance with no. of hops 5 -- 0.63758401602394132
********************************************************

Selected paths from minimum distance with less no. of hops == 5

Final Selected path 20 34 28


Decrypted message using the TV to vehicle key is accident


channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
user@user-LIFEBOOK-AH530:~/Music/code$ 
```

Figure 7. Using PSO iteration.

From this, path- 4 is eliminated as it falls at the upper bound.

Thereby we get 2 paths. They are: path-1 - 20 25 28 and path-5 - 20 34 38. Now Particle Swarm Optimization (PSO) is performed and this is illustrated in Figure 7.

Applying PSO to distance optimization over the above paths 1 and 5, the best possible path to reach the destination will be path-5 - 20 34 28. Since path-5 is having minimum distance with less number of hops when compared to path-1. Table 4 shows the distance values computed after applying PSO optimization.

Table 4. PSO iteration values

Path 1 – 20 25 28	0.854842
Path 5 – 20 34 28	0.637584

Hence from this we conclude that by using PSO, we get the best optimal path, where the data can be reached to the destination in shortest path.

6. Result and Discussion

The proposed work is evaluated with performance metrics - throughput, delay, drop, packet delivery ratio and residual energy levels.

Throughput increases marginally up to 1.7600 kbps and then it steadily increases from 1.800 kbps. This shows that the throughput for the enhanced SIR (ESIR) with PSO algorithm is better than the existing SIR protocol and this comparison is shown in Figure 8.

There is a marginal increase of 10% from 69.000 to 70.000 kbps and then it maintains the ratio till 3.000 seconds and then there is a gradual increase till 10.000 seconds for the enhanced protocol. This proves that the delivery rate is better for the enhanced SIR (ESIR) with PSO algorithm than the existing SIR protocol. The

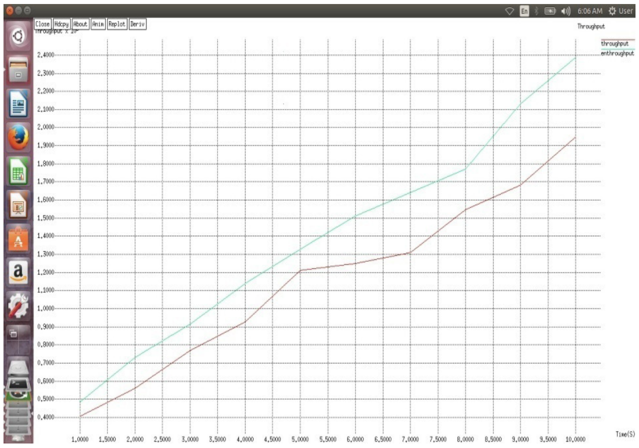


Figure 8. Throughput vs. Time.

increase in packet delivery ratio values with respect to time is shown in Figure 9.

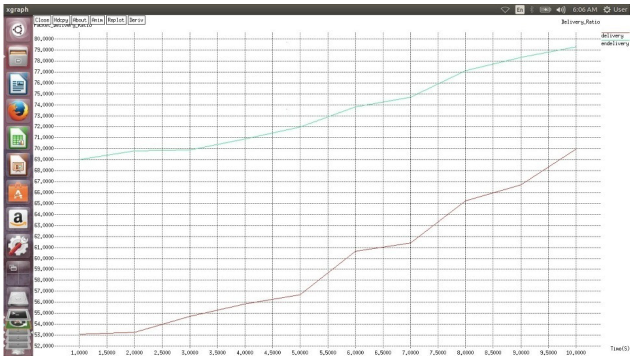


Figure 9. Packet delivery ratio vs. Time.

The energy utilized for enhanced SIR (ESIR) is gradually increasing and it converges at 4.000 milliseconds and then it increases marginally with the difference of 5% between the existing and proposed protocols. From Figure 10, we can determine that the energy utilization for enhanced SIR (ESIR) is less when compared with existing SIR protocol.

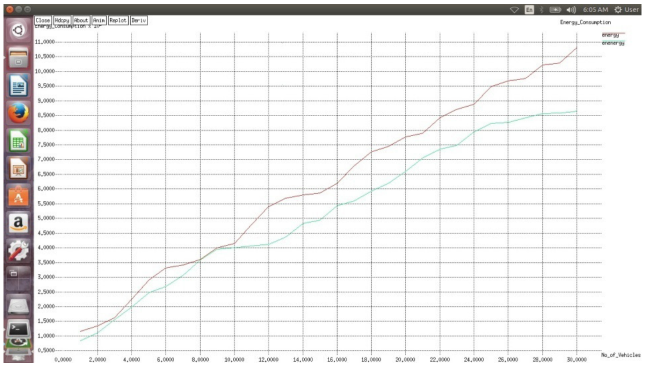


Figure 10. Residual energy levels vs. no. of vehicles.

Delay obtained for enhanced SIR with PSO is marginally increasing to a threshold of 1.000 ms and then steadily increases till 9.000 sec. This shows that delay for the enhanced SIR (ESIR) with PSO algorithm is better when compared to existing SIR protocol and this comparison is shown in Figure 11.

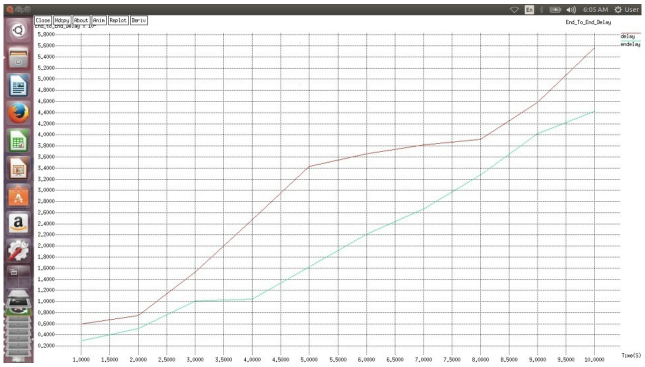


Figure 11. Delay vs. Time.

There is heavy packet drop in existing SIR protocol. This is due to the performance calculation of weight W by the TV. The packet drop for existing SIR protocol is starting from 56.000 kbps and is gradually increasing till 10 milliseconds. But the Enhanced SIR (ESIR) starts from 45.000 kbps and is gradually increasing. As shown in Figure 12 we can say that the existing SIR is having heavy packet drop than the enhanced SIR (ESIR) protocol.

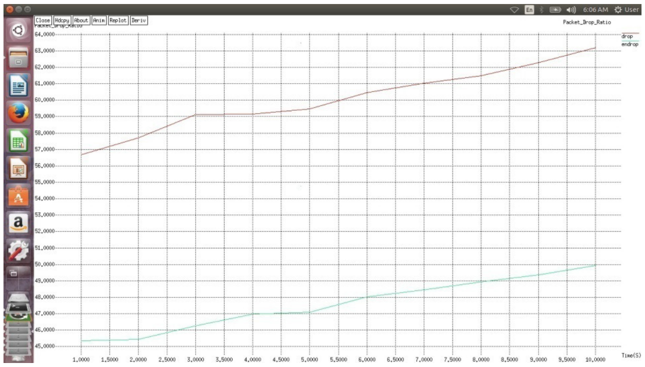


Figure 12. Packet Drop vs. Time.

7. Conclusion

SIR with PSO algorithm is the efficient method to transfer the data from source to destination in a secured and quickest path and the work could be enhanced by considering seamless scalability and Interoperability across heterogeneous platform.

8. References

1. Bhoi SK, Khilar PM. SIR: a secure and intelligent routing protocol for vehicular ad hoc network. Institution of Engineering and Technology in Networks. 2015; 4(3):185-94. https://doi.org/10.1049/iet-net.2014.0053
2. Li F, Wang Y. Routing in vehicular ad hoc networks: a survey. IEEE Vehicular Technologies. 2007; 2(2):12-22. https://doi.org/10.1109/MVT.2007.912927
3. Jerbi M, Senouci SM, Rasheed T, Ghamri-Doudane Y. Towards efficient geographic routing in urban vehicular networks. IEEE Transactions on Vehicular Technologies. 2009; 58(9):5048-59. https://doi.org/10.1109/TVT.2009.2024341
4. Seet BC, Liu G, Lee BS, Foh CH, Wong KJ, Lee KK. A-STAR: a mobile ad hoc routing strategy for metropolis vehicular communications. Networking Technologies, Services, and Protocols, Performance of Computer and Communication Networks, Mobile and Wireless Communications. 2004; p. 989-99. https://doi.org/10.1007/978-3-540-24693-0_81
5. Securing the OLSR protocol. Available from: https://www.thomasclausen.net/wp-content/uploads/2015/12/securing-olsr.pdf. Date accessed: 2003.
6. Perrig A, Canetti R, Tygar J, Song D. The TESLA broadcast authentication protocol. Crypto Bytes. 2002; 5(2):2-13.
7. Eiza MH, Owens T, Ni Q. Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs. IEEE Transactions on Dependable and Secure Computing. 2016; 13(1):32-45. https://doi.org/10.1109/TDSC.2014.2382602
8. Wahab OA, Otrok H, Mourad A. VANET QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks. Computational and Communication. 2013; 36(13):1422-35. https://doi.org/10.1016/j.comcom.2013.07.003
9. Adoption of Shortest Path Algorithm (Dijkstra's) in Distributed VANET Using GRID Computing. Available from: https://www.researchgate.net/publication/261360489_Adoption_of_Shortest_Path_Dijkastra_Algorithm_for_Distributed_VANET_using_Grid_Computing. Date accessed: 12/2011.
10. Cryptography & network security. Available from: https://onlinecourses.nptel.ac.in/noc19_cs28/preview. Date accessed: 2007.
11. Gayathri S, Radhika N. Greedy-Hop algorithm for detecting shortest path in Vehicular Networks. International Journal of Control Theory and Applications. 2016; 2(9):1125-33.