PERFORMANCE ANALYSIS OF OLSR USING BFO

Rajinder Kaur, Dr. Shashi B. Rana

M.Tech Student, Dept of Electronics and Communication, Guru Nanak Dev University Regional Campus, Gurdaspur, Punjab, India
Assistant Professor, Dept of Electronics and Communication, Guru Nanak Dev University Regional Campus, Gurdaspur, Punjab, India

---

Abstract: Driving is one of the most prime factors for traffic security. An early intimation about the collision warning, traffic congestion, roadside alarms, construction place and in-place traffic view will give the driver essential tools to decide the best path along the way. All these suggestions can be provided by a technology called VANETs. Distributed trust management in VANET is a challenging task due to the lack of infrastructure, ingenuousness of wireless links and the usually highly dynamic network topology. In this work, special characteristics of VANETs, existing trust management schemes has been studied, and proposed a distributed trust management strategy based on BFO which helps in evaluation of time by the vehicle that would like to know whether he can trust the vehicle that broadcast the message. The proposed simulation will takes place in MATLAB environment.

Key Words: WSN, OLSR, BFO, QOS, VANET

1. INTRODUCTION

A Wireless Sensor System (WSN) includes a gang of nodes connected with typically low functionality. They work with others collectively to execute realizing tasks during granted surroundings. A secreted detector community might comprise one particular or many drain nodes (Base Stations) to collect understood know-how in addition to exchange that to a central procedure in estimate to storage space method. Any detector node is usually power-driven by means of battery pack and could end up being split into three primary functioned products: a) the realizing unit, b) the communication unit and also c) a processor unit.
Ad hoc network is a framework less system and along these lines decentralized kind of remote system. Inside ad-hoc community, each centre usually takes relate involvement in steering by means of producing info to all or any kind of the particular hubs inside the method in addition to determination of their hubs ahead info can be produced easily on the idea connected with method integration.

1.1 OLSR (Optimized Link State Routing)

The Optimized Link State Routing (OLSR) is a proactive (table driven) routing protocol designed for MANETs. It is an optimization of pure link state protocols in that it reduces the size of control packet as well as the number of control packets transmission required. OLSR reduces the control traffic overhead by using Multipoint Relays (MPRs), which is the main principle followed by OLSR. A MPR is a node's one-hop neighbor which has been chosen to broadcast packets. Packets are just forwarded by a node's MPRs instead of pure flooding of the network. This delimits the network overhead, thus being more competent than pure link state routing protocols. OLSR is well-designed for large and dense mobile networks. Due to use of MPRs, the larger and denser a network, added optimized link state routing is achieved. MPRs help to provide the shortest path to a destination. The only necessity is that all MPRs declare the link information for their MPR selectors (nodes who has chosen them as MPRs). The network topology information is maintained by periodically exchange link state information. In case, if reactivity to topological changes is required then time interval for exchanging of link state information can be minimized.

The OLSR processes are corresponding to a set of parametric predefined in the OLSR RFC 3626 [9] as shown in figure1.1.These parametric are: the timeouts proceeding to resending a) HELLO (HELLO INTERVAL) b) MID-Multiple Interface Declaration (REFRESH INTERVAL) and c) TC (Topology Control) messages (TC INTERVAL) the "validity time" of the information established via three message type that are: a) NEIGHB HOLD TIME (HELLO), b) MID HOLD TIME (MID) and c) TOP HOLD TIME (TC) the WILLINGNE of a node to act as an MPR and DUP HOLD TIME, that represents the time all the way through that the MPRs proof information about the forwarded packets.

Main Parameters	RFC Standard configuration	Extent of Range
HELLO Interval	2.0 s	[1.0,.....,30.0]
REFRESH Interval	2.0s	[1.0,.....,30.0]
TC Interval	5.0s	[1.0,.....,30.0]
WILLINGNE	3	[1,2,3,4,5,6,7]
NEIGBH Hold Time	3Xhello Interval	[3.0,.....,100.0]
TOP Hold Time	3x TC Interval	[3.0,.....,100.0]
MID Hold Time	3XTC Interval	[3.0,.....,100.0]
DUP Hold Time	30.0	[3.0,.....,100.0]

Figure 1.1: OLSR RFC 3626 Configurations [9]

1.2 Routing in VANET

A typical of highly dynamic topology makes the design of efficient routing protocols for VANET is challenging. The routing protocol of VANET can be classified into two categories such as Topology based routing protocols & Position based routing protocols as shown in the Figure 1.2.

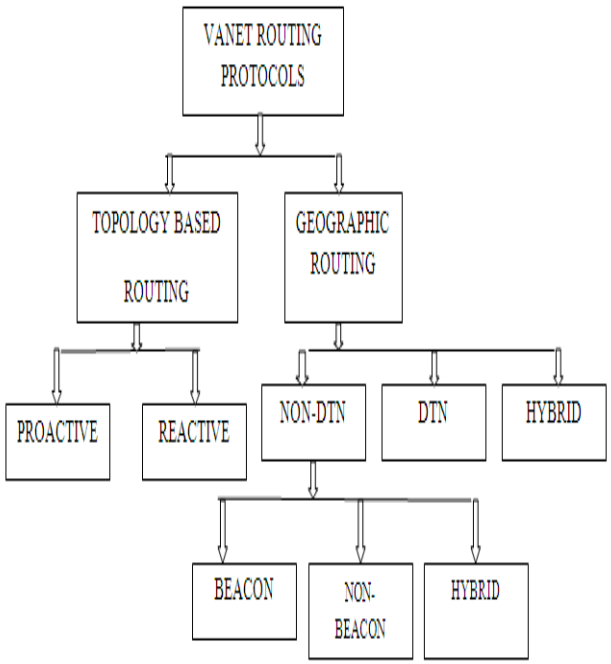

Figure: 1.2 Routing Protocols in MANET

1.2.1. Proactive Routing Protocols

Proactive routing protocols are predominantly based on shortest path algorithms. In the proactive routing protocols, nodes keep information of all linked nodes in form of tables because these protocols are table based. In addition, these tables are also communicated with their neighbours. Whenever any change occurs in network topology then routing table is updated by every node in the network. Pros - No Route Discovery is necessary. -Low Latency for real time applications. Cons - Unused paths occupy a significant part of the available bandwidth [11].

1.2.2. Reactive Protocols

Reactive routing procedure is called on demand routing because it starts route discovery when a node needs to communicate with another node thus it minimizes network traffic. Pros - Periodic flooding in the network is not required to update the routing table. Flooding is done when it is demanded. -Beaconless so it preserves the bandwidth. Cons - For route finding latency is high. - Extreme flooding of the network causes disruption of nodes statement.

1.3 MESSAGE INTERFACE SYSTEM

Three types of messages are generated in our system:

a) Sender message: M = [event, confidence, time, location]. confidence ∈ [0, 1] provide suppleness in exposure an event, time ∈ N is a positive integer and location ∈ N ×N is a geographical coordinate, both being accessible from an equipped GPS device;

b) Trust opinion: O = [reaction, confidence], where reaction ∈ {trust, ¬trust} and confidence ∈ [0, 1]. A trust opinion is a message provided by a peer that serves as a valuation of the sender message;

c) Aggregated message: A = [M, O1. On], a combination of a sender data and a list of trust opinions.

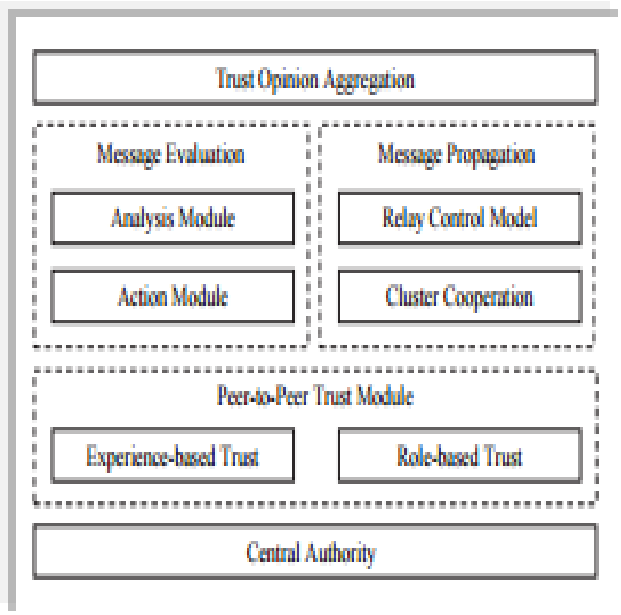

Figure1.3 Trust Based Framework

1.4 Bacterial Foraging Optimization (BFO)

During foraging of the true bacteria, locomotion is achieved by a collection of tensile flagella. Flagella help an E.coli bacterium to fall or swim, that are two essential operations performed by a bacterium at the occurrence of foraging. When they revolve the flagella in the clockwise direction, every flagellum pulls over the cell. Thus results in the moving of flagella separately and lastly the bacterium tumbles with lesser amount of tumbling while in a destructive place it tumbles repetitively to locate a nutrient gradient. Stirring the flagella in the counter clockwise direction helps the bacterium to swim at a very high-speed rate. In the above mentioned algorithm the bacteria undergoes chemo taxis, where they like to transfer towards a nutrient gradient and shun harmful atmosphere.

The BFO algorithm is as follows [10]:
Step1:Initialize parameters p ,S,N_c,N_s, N_r, N_{ed}, P_{ed} C(i)(i=1,2,...S),θ^i.

Step 2: Elimination dispersal loop: l=l+1

Step 3: Reproduction loop; k=k+1.

Step 4: Chemo taxis loop: j=j+1.
[a] For i=1,2,...S take a chemotatic step for bacterium I as follows.
[b] Compute fitness function (i,j,k,l).

Let ,J(i,j,k,l) = J(i,j,k,l)+J_{cc} (θ^i(j,k,l),P(j,k,l).

[c] Let J_{last}= j(i,j,k,l) to save this value since we may find a better rate during a run.

[d] Tumble: generate a random vector Δ (i)∈ R^p each element Δ_m(i),m=1,2,...,p, a random number on [-1,1].
[e] Move: Let

$$\theta^i(j+1,k+1) = \theta^i(j,k,l) + C(i)\frac{\Delta(i)}{\sqrt{\Delta^T(i)\Delta(i)}}$$

This results in a step of=f size C (i) in the direction of the tumble for Bacterium i.

[f] Compute J (I,j+1,k,l) and let

(

$$J(i,j+1,k,l) = J(i,j,k,l) + j_{cc}\theta^i(j+1,k.l), P(j+1,k,l))$$

[g] Swim

i. Let m=0
ii. While m<N_s
- Let m=m+1
- If j(I,j+1,k,l)<J_{last} ,let J_{last}=J(I,j+1,k,l) let,

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + C(i)\frac{\Delta(i)}{\sqrt{\Delta^T(i)\Delta(i)}}$$

- And apply this $\theta^i(j+1,j,k)$ to compute the new $J(i,j+1,k,l)^i$as we did in [f].

iii. Else, let m=N_s. This is the end of the while statement.

[h].Go to next Bacterium (i+1) if i≠S.

Step 5: If j<N_c , go to step 4.is

Step 6: Reproduction:

[a]. For the given k and l , and for each i=1,2,..S. Assume

$$J^{i}_{health} = \sum_{j=1}^{N_c+1} J(i, j, k, l)$$

Be the health of bacterium i. Sort bacteria and Chemo tactic parameters C(i) in order of ascending cost J_{health}.

[b]. The S_r bacteria with the highest J_{health} values die and the remaining S_r bacteria with the best values split.

Step 7: if $k<N_{re}$, go to step 3.

Step 8: For Elimination-dispersal: For i=1,2,...*S* with probability P_{ed}, eliminate and disperse every bacterium. To do this, if a bacterium is eliminated, simply disperse an additional one to a random position on the optimization domain. If $I< N_{ed}$, then go to step 2; or else end.

2. LITERATURE SURVEY

Heru Supriyono (2012) described that investigations for the development of biologically-inspired soft computing approaches based on bacterial foraging algorithm (BFA) for modelling and organize the dynamic systems. The work has determined on the modification of BFA so that it could have quicker convergence speed and better accuracy. The convergence speed has been defined as the number of steps needed by algorithm to converge to the optimum value. The modified BFAs have been tested on both benchmark functions and in dynamic modelling to authenticate their performances and control of a flexible manipulator system.

Hsuan-Ming Feng , Ji-Hwei Horng (2012) proposes a novel bacterial foraging swarm-based intelligent algorithm called as the bacterial foraging particle swarm optimization (BFPSO) algorithm to propose vector quantization (VQ)-based fuzzy-image compression systems. It helps to improve compressed image quality when processing many image patterns. The BFPSO algorithm is a well-designed evolutionary learning algorithm that manages complex global optimal codebook generation troubles. The BFPSO algorithm is a combination of bacterial foraging optimization (BFO) behaviour with a particle swarm optimization (PSO) learning scheme to obtain fast convergence and self-adaptive learning benefits. The evolutionary BFPSO algorithm automatically designs appropriate parameters for fuzzy-VQ-based systems using a proper codebook selection machine. Nonlinear image compression applications obtained by computer simulation demonstrate the efficiency of the BFPSO learning algorithm. The differences between the proposed BFPSO learning scheme and the BFO- and LBG-based VQ learning methods demonstrate the superior image results created by the proposed algorithm.

X. Lin et al. (2007) revealed the fact that the unique characteristics of set of signature which is an significant cryptographic primitive, perfectly match the safety and privacy necessities in VANETs. By taking different safety and privacy requirements of two types of VANET communications into account, namely, vehicle-to-infrastructure (V2I) and vehicle-to-vehicle communications (V2V), they propose a novel safe and privacy-preserving protocol for vehicular communication, based on a combination of set of signature and identity (ID)-based signature techniques.

X. Lin et al. (2008) proposes a cooperative message validation protocol, where every vehicle probabilistically validates a definite percentage of its received messages, according to its own computing capacity, and informs about any illogical messages that has been detected. The protocol relies on the supposition that each individual vehicle is eager to contribute its computing resources and contribute in a cooperative effort for message authentication. In reality, there will always be some self-seeking vehicles those do not want to make such contribution and only want to take benefits of others' efforts.

C. Zhang et al. (2008) proposes a novel RSU-aided message authentication scheme named as RAISE, in which RSUs are accountable for verifying the authenticity of the messages sent by the vehicles and for notifying the vehicles of the results. Since MACs are used for authenticating inter-vehicle communication with the aid of RSUs, the message verification process is appropriate for vehicular communication. This requires direct involvement of RSUs in the processing of the message verification phase; when RSUs are not widely available, in the early stage of operation of VANETs for example, it becomes ineffective.

Zhang J. et al. (2010) In this paper, authors present a trust-based structure for message circulation and valuation in vehicular ad-hoc networks where peers distribute information regarding road condition or security and others provide opinions about whether the information can be trusted. More specifically, the trust-based message propagation model collects and propagates peer's opinions in an efficient, safe, and scalable method by dynamically scheming information dissemination.

3. METHODOLOGY

The optimization strategy used to obtain automatically efficient OLSR parameter configurations are carried out by coupling two different stages: an optimization procedure and a simulation stage. The optimization block is carried out by a met heuristic method, i.e. BFO. It is conceived to find optimal (or quasi-optimal) solutions in continuous search spaces, which is the case in this work. We use a simulation procedure for assigning a quantitative quality value (fitness) to the OLSR performance of computed configurations in terms of communication cost. This method will be carried out by means of the MATLAB.

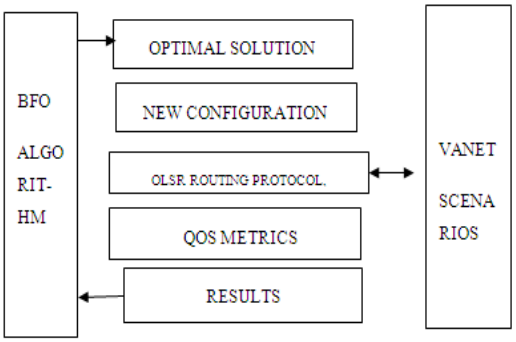

Figure 4.1 Methodology Flowchart

4. RESULTS

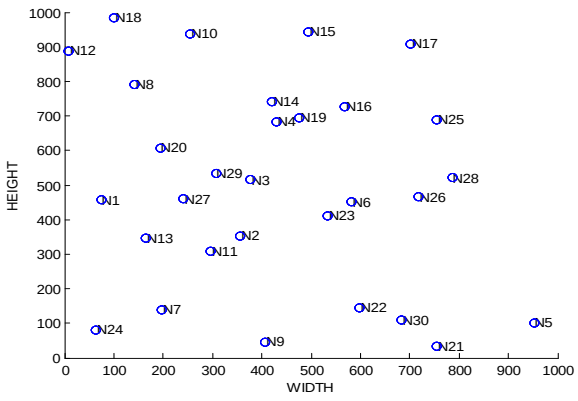

Figure 4.1 Network setup

Above figure shows the network simulation model containing 1000 * 1000 nodes.

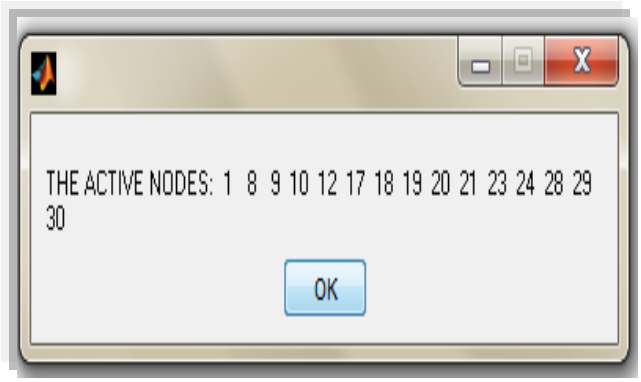

Figure 4.2 Active nodes

One approach to prolong network lifetime while preserving network connectivity is to deploy a small number of valuable, but more powerful, relay nodes whose main task is communication with other sensor or active nodes. 'Active Nodes' that perform customized operations on the data flowing through them. There are four rounds means four times data transmitted through the network.

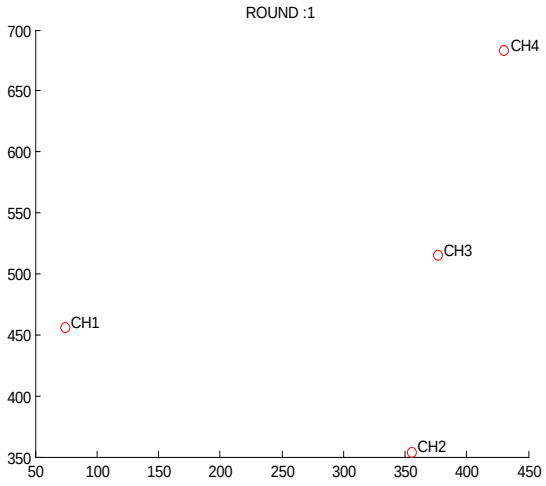

Figure 4.3 active node movements for round 1

As the data transmitted through the network, then movement of nodes happens. Then the cluster heads designed by the network. Cluster head keeps all the information and control of transmission of data through the corresponding cluster. We design a network of four clusters and four cluster heads respectively.

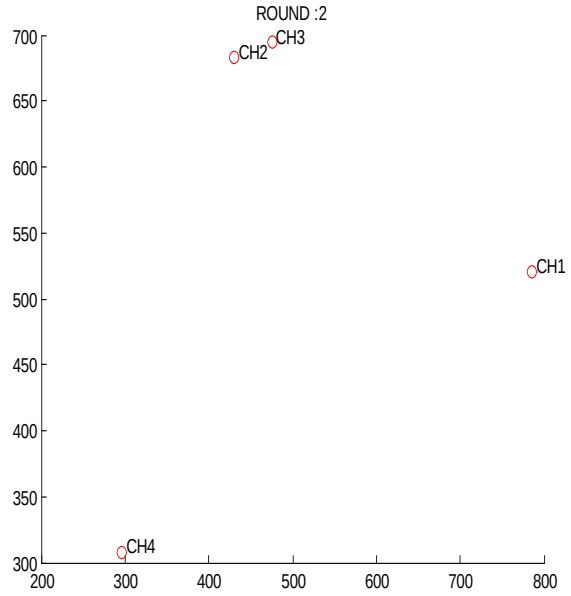

Figure 4.4 Active node movements for round 2

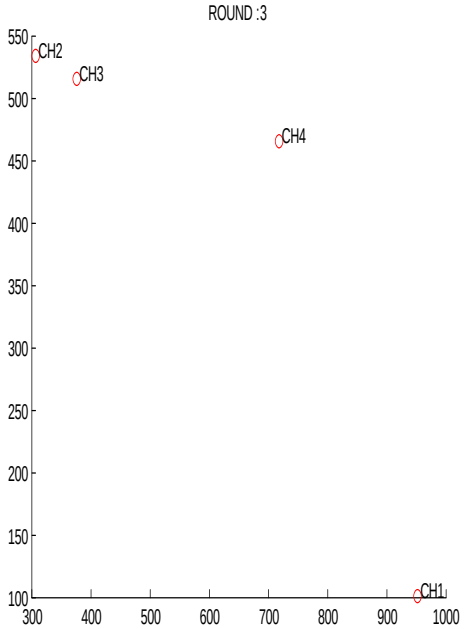

Figure 4.5 Active node movements for round 3

Above figures show the movement of the active nodes.

Rounds means iteration of transmission of data through the network or active nodes.

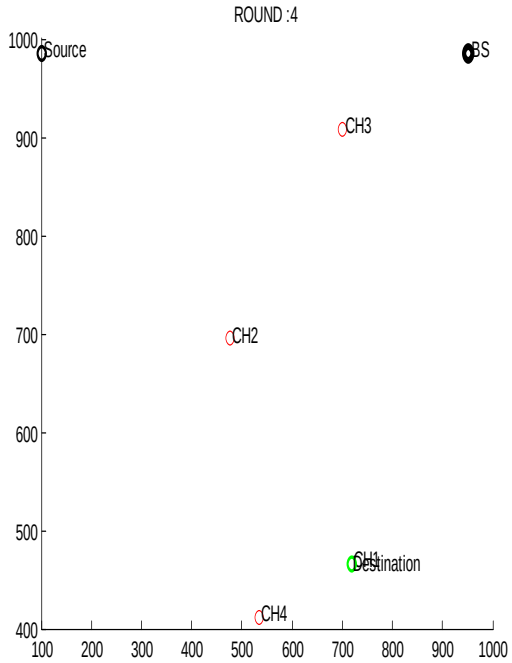

Figure 4.6 active node movements for round 4

In above figure the location of source, destination and base station has been shown.

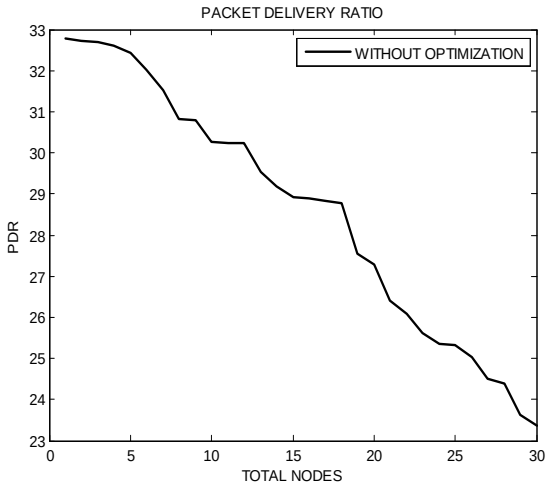

Figure 4.7 Packet Delivery Ratio

Packet Delivery Ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. Above figure shows the delivery ratio without optimization.

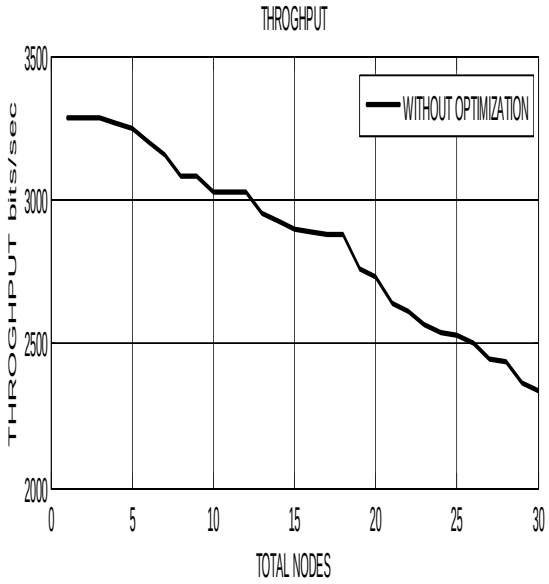

Figure 4.8 Throughput

It is the total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity. Above figure shows the throughput without optimization.

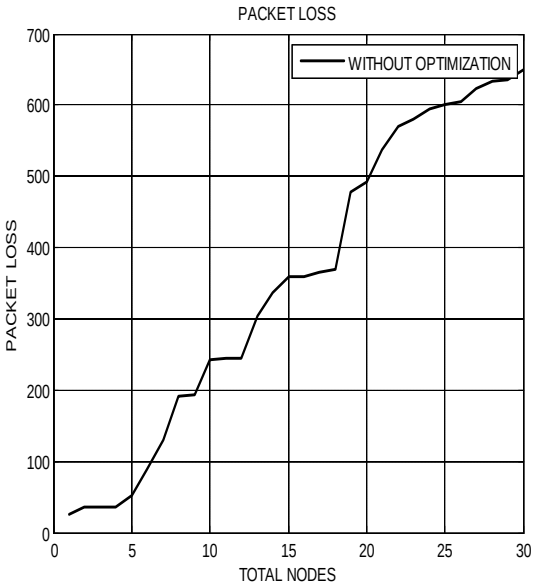

Figure 4.9: Packet losses without optimization

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Above figure4.9 shows the large number of packet loss in the network.

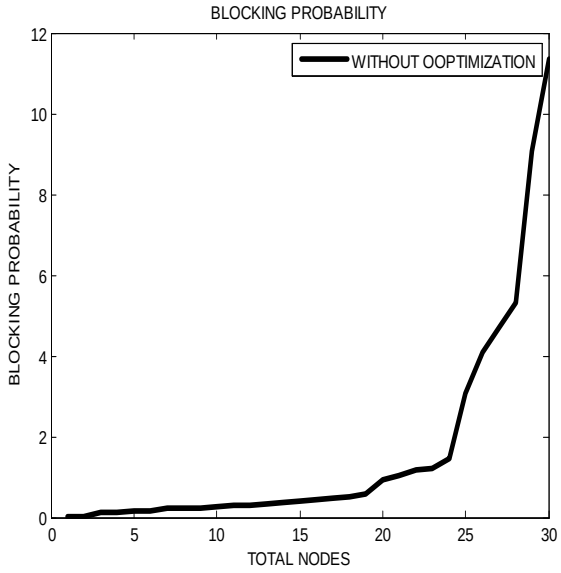

Figure 4.10 Blocking probabilities without optimization

Blocking probability is the fraction of time a trunk request is denied because all channels are hectic. This probability is typically specified for a given system. It is typically desired to be 2%. Above figure shows the blocking probability without optimization.

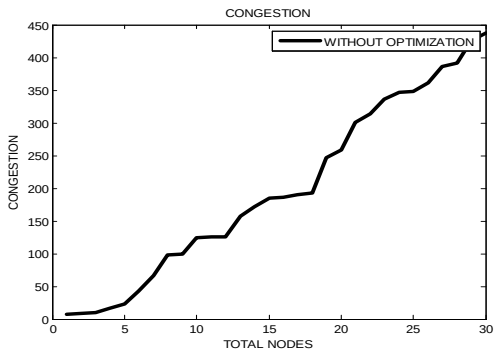

Figure 4.11 Congestion without optimization

It refers to a network state where a node or link carries so much data that it may deteriorate network service excellence, following in queuing delay, frame (data) or packet loss and the new connections get blocked. In case of congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is not sufficient and network data traffic exceeds capacity. Above figure shows the congestion graph without optimization.

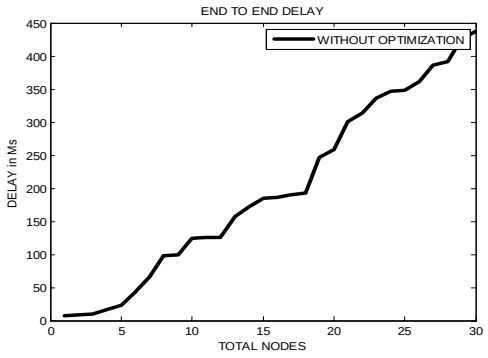

Figure 4.12 End to end delay without optimization

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows the end to end delay without optimization.

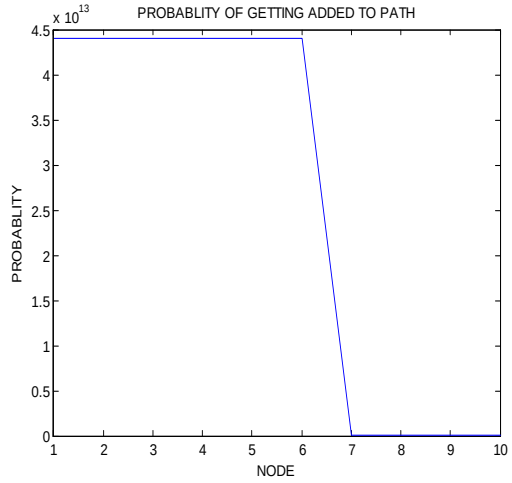

Figure 4.13 Probability to getting added to path

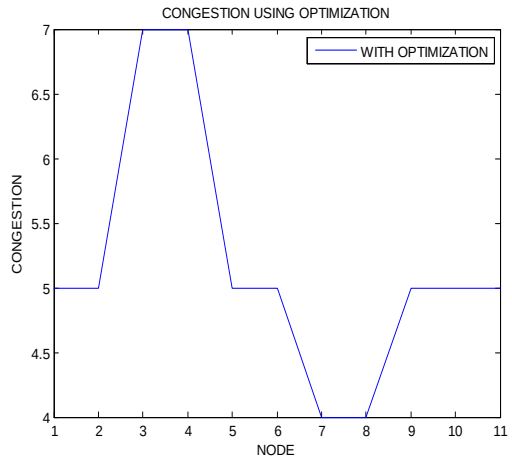

Figure 4.14 Congestion optimization

It refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the new connections get blocked. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is not sufficient and network data traffic exceeds capacity. Above figure shows the congestion graph with optimization.

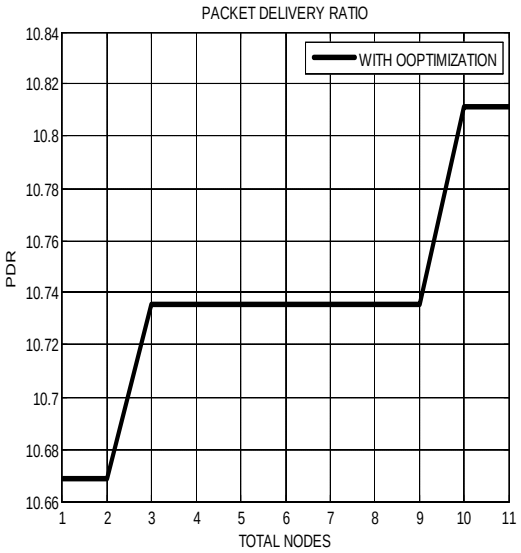

Figure 4.15 packet delivery ratio with optimization

It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. Above figure shows the delivery ratio with optimization.

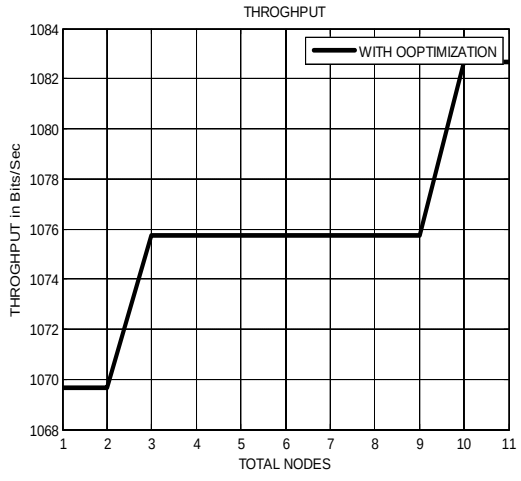

Figure 4.16 Throughput with optimization

It is the total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity. Above figure shows the throughput with optimization.

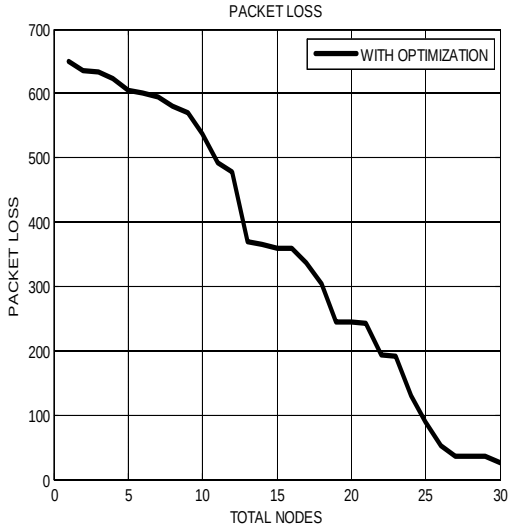

Figure 4.17 Packet loss with optimization

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Above figure 4.17 shows the less number of packet loss in the network using optimization.

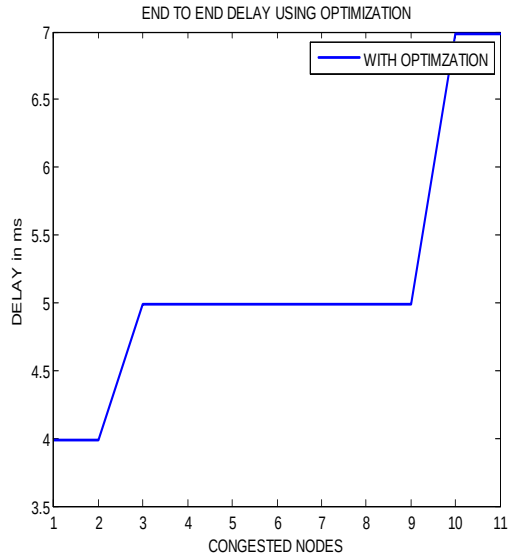

Figure 4.18 end to end delay with optimization.

End to end delay is average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure 4.18 shows the end to end delay with optimization.

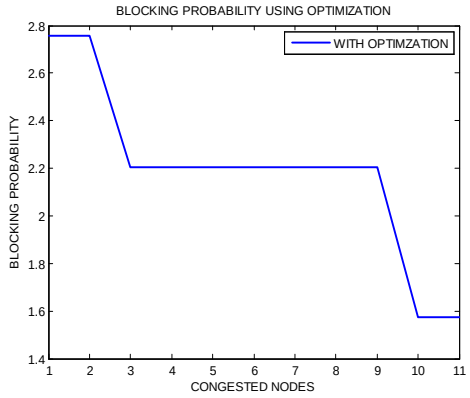

Figure 4.19 blocking probability with optimization (BFO algorithm)

Blocking probability is the fraction of time a trunk request is denied because all channels are hectic. This probability is usually specified for a given system. It is typically desired to be 2%. Above figure 4.19 shows the blocking probability with optimization. Nodes can be change depend upon the how much vehicles are in the coverage range of each other.

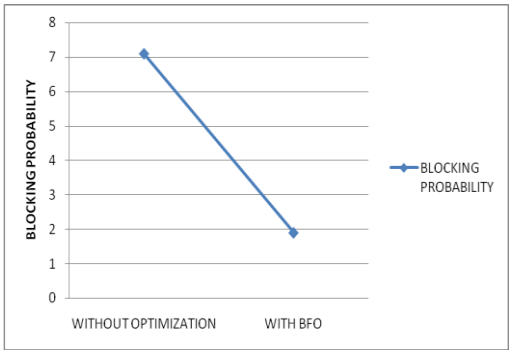

Figure 4.20 blocking optimization with and without optimization (comparison)

Blocking probability is the fraction of time a trunk request is denied because all channels are busy. This probability is usually specified for a given system. Above figure shows the comparison of blocking probability with and without optimization. It has been seen that for proposed approach it founds to be small.

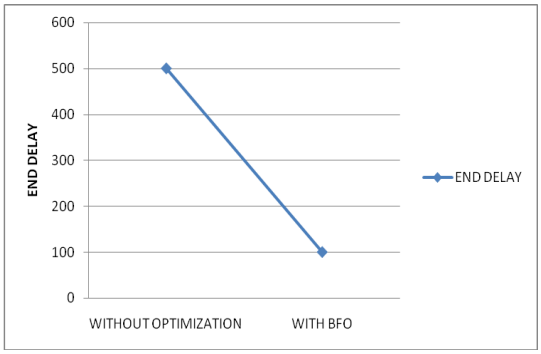

Figure 4.21 End to end delay with and without optimization

the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted. End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows the end to end delay with optimization. Above figure shows the comparison of end to end delay with and without optimization. It has been seen that for proposed approach it founds to be small.

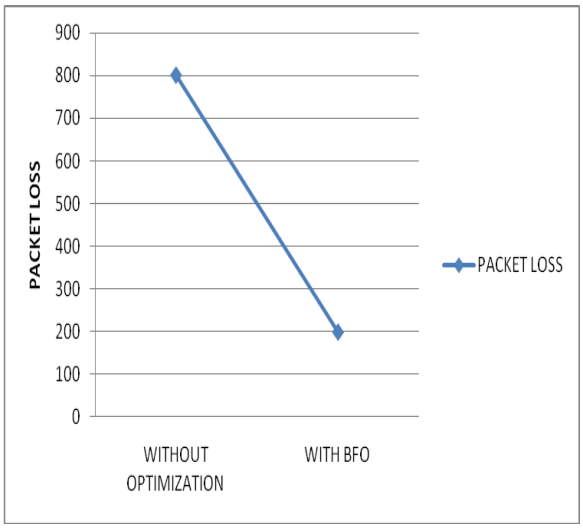

Figure 4.22 Packet losses with and without optimization

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Above figure shows the comparison of packet loss with and without optimization. It has been seen that for proposed approach it founds to be small.

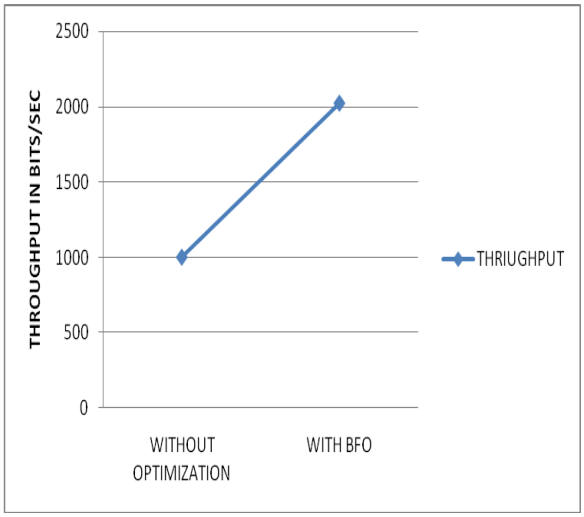

Figure 4.23 Throughput with and without optimization

It is the total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity. Above figure shows the comparison of throughput with and without optimization. It has been seen that for proposed approach it founds to be high.

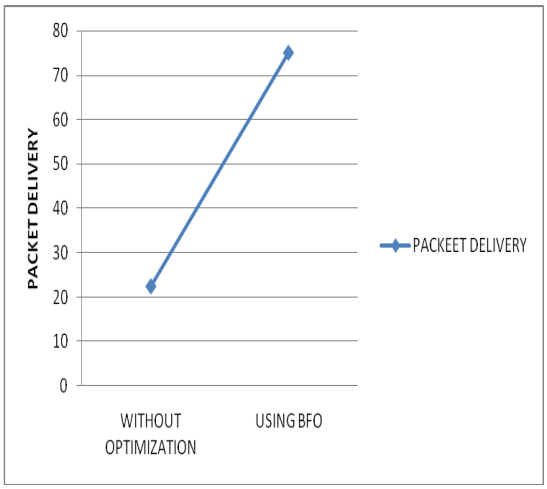

Figure 4.24 Packet delivery ratio with and without optimization

It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. Above figure shows the comparison of throughput with and without optimization. It has been seen that for proposed approach it founds to be high.

5. CONCLUSION

Trust is a key part in security because one altered message creates problem for the users in many ways. Users can obtain benefit of these applications if we can secure the communication between all entities (components) of the network and hence no chances for attackers to create trouble for users in the network. Attackers generate problem directly and indirectly by launching different kind of attacks. Hence, it is necessary to develop trust in vehicular networks. Trust management is a challenging task since there is a lack of infrastructure, candidness to wireless links and highly dynamic.

In this work, we have discussed about existing trust based models .It has become a challenging task due to the lack of infrastructure, openness of wireless links and the usually highly dynamic network topology. Trust-based approaches have been largely applied to provide reliable routing in computer networks So far, trust has been used to cope with packet dropping attacks or to select trusted paths between the source and the destination. We have proposed a trust management strategy based on Bacterial Foraging Optimization (BFO) which mainly concentrates on how fast the vehicle can take decision to trust the vehicle that broadcasts the message and proceed.

REFERENCES

[1] M. Gerlach and F. Friederici. Implementing trusted vehicular communications. In Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th, pages 1 –2, april 2009.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Zhendong Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. Communications Magazine, IEEE, 46(11):100 –109, november 2008.

[3] P. Ardelean and P. Papadimitratos. Secure and privacy-enhancing vehicular communication: Demonstration of implementation and operation. In Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, pages 1 –2, sept. 2008.

[4] J. P. Hubaux P. Papadimitratos, V. Gligor. Securing vehicular communications - assumptions, requirements, and principles. november 2006.

[5] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. Communications Magazine, IEEE, 46(11):110 –118, november 2008.

[6] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. Wireless Communications, IEEE, 13(5):8 –15, october 2006.

[7] P. Papadimitratos, L. Buttyan, J. P. Hubaux, F. Kargla, A. Kung, and M. Raya. Architecture for secure and private vehicular communications. 2007.

[8] T. Leinmüller, L. Buttyan, J. P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. Sevecom - secure vehicle communication. june 2006.

[9] L. Buttyan and J. P. Hubaux. Security and Cooperation in Wireless Networks. http: //secowinet.epfl.ch, 2007. Cambridge University Press.

[10] C. Leckie and R. Kotagiri, "Policies for sharing distributed probabilistic beliefs," in Proceedings of ACSC, 2003, pp. 285–290

[11] P. Papadimitratos and J. P. Hubaux. Report on the secure vehicular communications: Results and challenges ahead workshop. april 2008.

[12] D. Djenouri, W. Soualhi, and E. Nekka. Vanet's mobility models and overtaking: An overview. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, pages 1 –6, april 2008

[13] S. D. Ramchurn, D. Huynh, and N. R. Jennings, "Trust in multi-agent systems," The Knowledge Engineering Review, vol. 19, no. 1, pp. 1–25, 2004.

[14] M. Gerlach, "Trust for vehicular applications," in Proceedings of the International Symposium on Autonomous Decentralized Systems, 2007.

[15] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," International Journal of Computational Intelligence Theory and Practice (IJCITP), vol. 5, no. 1, 2010.

[16] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," Technical Report, LCA-REPORT-2007-003, 2007.

[17] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in Proceedings of VANET, 2004

[18] Marcela Mejia, Néstor Peña, José L. Muñoz, Oscar Esparza, and Marco A. Alzate. A game theoretic trust model for on-line distributed evolution of cooperation in manets. Journal of Network and Computer Applications, 34(1):39 – 51, 2011.

[19] C. S. Eichler. Solutions for Scalable Communication and System Security in Vehicular Network Architectures. Dissertation, Technische Universität München, Munich, 2009.

[20] Aifeng Wu, Jianqing Ma, and Shiyong Zhang. Rate: A rsu-aided scheme for data-centric trust establishment in vanets. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, pages 1 –6, sept. 2011.

[21] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous, 2006, pp. 1–8.

[22] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust-based message propagation and evaluation framework in vanets," in Proceedings of the Int. Conf. on Information Technology Convergence and Services, 2010.

[23] B. Yu and M. Singh, "Distributed reputation management for electronic commerce," Computational Intelligence, vol. 18, no. 4, pp. 535–549, 2002.

[24] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Intelligent agents in mobile vehicular ad-hoc networks: Leveraging trust modeling based on direct experience with incentives for honesty," in Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT), 2010.

[25] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in Proceedings of International Autonomous Agents and Multi Agent Systems (AAMAS), Bologna, Italy, 2002.

[26] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, 2008, pp. 246–250.

[27] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[28] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[29] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011

[30] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[31] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE ICC, Beijing, China, May 2008, pp. 1451–1457.

[32] X. Lin, "Secure and privacy-preserving vehicular communications," Ph.D. dissertation, Univ. Waterloo, Department of Electrical and Computer Engineering, Waterloo, ON, Canada, 2008.

[33] Dotzer F, Fischer L, Magiera P (2005) Vars: a vehicle ad-hoc network reputation system. In: IEEE international symposium on a world of wireless mobile and multimedia networks,pp 454–456

[34] Schmidt RK, Leinmuller T, Schoch E, Held A, Schafer G (2008) Vehicle behavior analysis to enhance security in vanets. In:Workshop on vehicle to vehicle communications

[35] Lo N-W, Tsai H-C (2009) A reputation system for traffic safety event on vehicular ad hoc networks. EURASIP – Journal on Wireless Communications and Networking. doi:10.1155/2009/125348

[36] Minhas UF, Zhang J, Tran T, Cohen R (2010) Towards expanded trust management for agents in vehicular ad-hoc networks. IJCITP 5(1):3–15

[37] Zhang J, Chen C, Cohen R (2010) A scalable and effective trust-based framework for vehicular ad-hoc networks. JoWUA 1(4):3–15.

[38]. T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). IETF RFC 3626, [online] Available in URL http://www.ietf.org/rfc/rfc3626.txt, 2003.

BIOGRAPHIES

Rajinder Kaur, Pursuing M.TECH in Electronics and Communication (specialization in comm.) from Guru Nanak Dev University and I have done B.TECH in Electronics and Communication from Punjab technical University (Jalandhar). My research area of interest in Wireless Sensor Network.

Dr. Shashi B. Rana, Assistant Professor, Electronics and communication department, Guru nanak dev University regional campus, Gurdaspur. I have done M. Tech from Guru Nanak Dev University (Amritsar) and done Ph.D From Punjab Technical University (Jalandhar). My area of intesrest are Nanoelectronics and Antenna. I have 35 Publications. I am a Member of IEEE, SWIDC, Ceditor of horizon publishing and Member of american journal of circuit and communication journal.

