ISSN: 2348 9510

International Journal Of Core Engineering & Management(IJCEM)
Volume 1, Issue 4, July 2014

Reliability And Efficient Protocol For Position-Based Routing In Vehicular Ad Hoc Network

Smita Garg
Department of Computer Science
Rajiv Gandhi Prodyogiki Vishwavidhyalay, Bhopal, M.P, India
smitagarg20@gmail.com

Abstract

In VANETs intellectual traffic services are proficient if they are associated with technique that oversee and generate confidence between service providers and vehicles. As a consequence, the authentication of the supplier of traffic situation information and the authorization of entity's to admittance this information is essential. Accordingly it's indispensable to expand an advance security method for VANETs protocol. In this paper to proposed progress the security of position-based routing. This illumination can challenge almost each of the attacks, still those attacks which at in attendance obtainable security protocol can't treaty between, such as the maliciously drop-packets-attack approximating black hole attack, a scheme is anticipated to improve the security concert of position-based routing protocols. This method has proved effectiveness and has enhanced security. This method utilizes digital signature to assertion the distinctiveness authentication, data reliability and non-repudiation. The dissimilarity to nearly all of other solutions is that an estimate method is proposed, which can distinguish malicious nodes that drop routing data. This method has been demonstrate effectiveness and has improved security and network NS2 simulation.

Keywords- VANET; protection, LPRP, Authentication, security method.

INTRODUCTION

A mobile ad hoc network is a self-configuring network composed of mobile nodes communicating through wireless links in an environment without any fixed infrastructure support. MANET has applications in emergency search and rescue operations, battlefields, and data acquisition operations in inhospitable terrain, where an established infrastructure is unavailable or unusable. An emerging new type of MANET is the Vehicular Ad Hoc Network (VANET), which is formed by vehicles that are equipped with wireless communication devices based on the standard IEEE 802.11 Wireless-LAN.

In recent years, VANETs have attracted considerable attentions in research community and automotive industry (e.g., VICS [1], Carnet [2], Feetnet [3] and its successor Network-on-Wheels [4]). VANETs can be leveraged to provide a variety of applications, which can be roughly classified in two categories: (1) those that require broadcasting the information from the vehicle to all surrounding vehicles. Most safety applications such as accident alerts that warn drivers of the upcoming obstacles and hazards in the road belong to this category; (2) those that require a routing protocol in order to deliver the information to a particular destination in a multi-hop manner, e.g., sending the query to the parking place miles away when the driver wants its parking lot information in order to make a better road plan, and then sending the reply from the parking place to the queried driver. For the first class of applications, many broadcast-based protocols have been proposed so far [5][6] [7]. Thus, in this paper we focus on the second class of applications, in particular on query related applications: the moving vehicle sends a query request to the fixed location(information server), which provides information and answers the query. Only if the messages are trust-worthy, VANET can improve traffic management. However it is a thorny issue to ensure the conditional anonymous, at the same time it deal with the false messages. To solve the problem, a number of schemes have been proposed so far. The proposals in [2] and [3] use regular digital signatures, but privacy can’t be preserved; In [4],the authors proposed to use a set of anonymous keys that frequently change, but it incurred huge overhead costs; In[5],a novel group-signature-based security framework is proposed, but they provide no concrete scheme; In [6],the authors propose a secure and privacy-preserving protocol by using group signature and identity-based signatures, however the signature’s length and computational complexity is big; In [8],the authors give a better scheme by integrating a posteriori and a priori countermeasures, but they don’t distinguish the vehicles, and the threshold value is difficult to determine. The prompt of this a secure enhanced PBP is proposed in this research. This resolution can oppose approximately all of the attacks, still individuals attacks which presently obtainable security protocol can’t treaty with, such as the spitefully drop-packets-attack like black hole attack. Furthermore, out-of-band attack like wormhole attack together with other attack witch create the routing occupied can also be detected and defense. SPBR for VANETs [16]; Charles Harsch propose defense mechanisms, which relies both on cryptographic primitives and plausibility checks mitigating false position injection. however protocols and security planning talked more than cannot deal with blackhole attack which ruins the routing efficiency. Two security method in position-based routing protocol are deliberate extremely. Hybrid Signature [10] is a security protocol method which makes two type of digital signature: ETE signatures and HTH signatures. Given that there are alterable field and unchallengeable field in the packets of PBP, this security method uses hybrid signatures to create sure the integrity of the dissimilar type data individually. End-to-end signatures protect the mutable data between sources and destination. Hop-to-hop signatures protect the immutable data between two neighbors. While Efficient Security Scheme for Position-Based Routing in VANETs[14], of which the security method primarily employs the HMAC to achieve secure process among in-between nodes, still employs digital signature among end-to-end protections. Evaluate with the hybrid signature method, it is more efficient since the cost of doing HMAC is a reduced amount of than doing digital signature. Greedy Perimeter Stateless Routing for Wireless Networks [16] proposed a PBP in detail. GPRS is a classic position-based routing protocol, into which we PBP functional our method and the hybrid signature scheme to execute in the NS2 for estimation the consequence of each of them. And then we examine the replication data to evaluate the security performance and the network performance of them.

RELATED WORK

S. S. Dorle in at al[1]Comparison of performance parameters for three routing protocols DSDV, AOMDV and AODV in VANET is carried out Simulation results are matched with the expected output and are found satisfactorily. As expected, reactive routing protocol performance is the best considered because of its ability to maintain link by periodic exchange of information, which is required for TCP based traffic. AODV performs predictably. Virtually all packets delivered at low node mobility, and decreases the converge as node mobility increases and DSDV performs well but still requires the transmission of many routing overhead packets.

Hind AI Falasi in at al[2]they was provided a comprehensive classification of revocation schemes in V ANETs. As far as the authors are aware this is the first paper to provide a comprehensive classification and comparisons of revocation schemes in V ANETs. Centralized revocation schemes leave the responsibility of revoking the vehicles credentials to some centralized authority. On the other hand, decentralized schemes depend on the feedback of the vehicles participating in the network. Decentralized schemes have several advantages over centralized schemes. For example, eviction of misbehaving vehicles can occur as soon as a suspicious activity is reported therefore further damage by that vehicle can be prevented. Moreover, some decentralized revocation schemes rely on the vehicles to evict a misbehaving vehicle, and then report it to a centralized authority to get its credentials revoked.

Dr.G.Padmavathi in at al[3] estimates the applicability of IPSec for MANET network layer to provide security services for both routing information and data message. They was demonstrate simulation results that IPSec-LANMAR outperforms IPSec-FSR and IPSec OLSR. The experiments are carried out using the simulator Qualnet version 4.5. This suggests that IPSec would be a better choice for MANET due to the reason that it can provide security protection for both routing information and data message simultaneously.

Yonglin Ren in at al[4] they was explore the issues of data confidentiality and authentication in a wireless network. With the proposal of a hybrid cryptosystem with a dual authentication strategy, they was make a twofold contribution. On one hand, the application of both symmetric and asymmetric key algorithms in a wireless and mobile environment has been shown. Their proposed scheme provides satisfactory security protection with reasonable computational cost. On the other hand, they take advantage of public key as a solution to deal with the problem of node authentication and thereby enhance the reliability of authentication.

Hui Liu in at al[5] they was distinguish the vehicles into two classes, an efficient and secure scheme is proposed for VANET messages authentication, group signature is used for the messages from private vehicles and identity-based signature for public vehicles and RSU, furthermore, it employs batch message-processing techniques to accelerate the verification. Quantitative comparison determination is explored for handling conflicting information. HOW

MOTIVATION

The increasing mobility of people has caused a high cost for societies as consequence of the increasing number of traffic congestion, fatalities and injuries. Vehicular Ad-Hoc Networks (VANETs) envisage supporting services on Intelligent Transportation Systems (ITSs), as collective monitoring of traffic, collision avoidance, vehicle navigation, control of traffic lights, and traffic congestion management by signaling to drivers. VANETs comprise vehicles and roadside equipments owning wireless interfaces able to communicate among them by wireless and multi-hop communication.

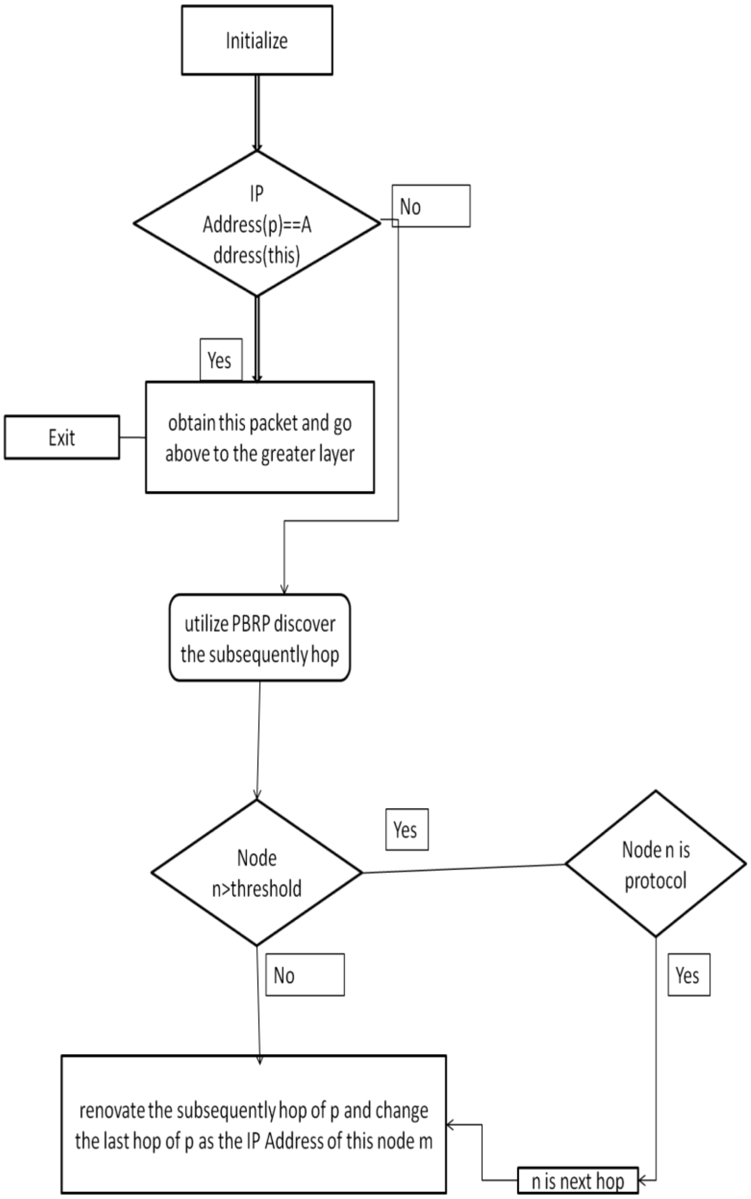
VANETs are prone to interference and propagation issues, as well as different types of attacks and intrusions, that can harm ITS services. These networks are characterized by high mobility nodes, wireless links subject to interference, fading due to multipath propagation and highly changing network topologies. The absence of central entities increases the complexity of security management operations, particularly, access control, node authentication and cryptographic key distribution, allowing the participation of misbehaving (malicious or selfish) nodes in the network and posing nontrivial challenges to security design. Further, wireless communication is susceptible to jamming, eavesdropping and interferences making easy to damage information and service security. Albeit all these drawbacks, it is well known today that guaranteeing information integrity, authenticity, confidentiality, non-repudiation, and, particularly, availability of network services and information are prerequisite for the successful deployment of VANETs.

VEHICULAR NETWORKS WORK

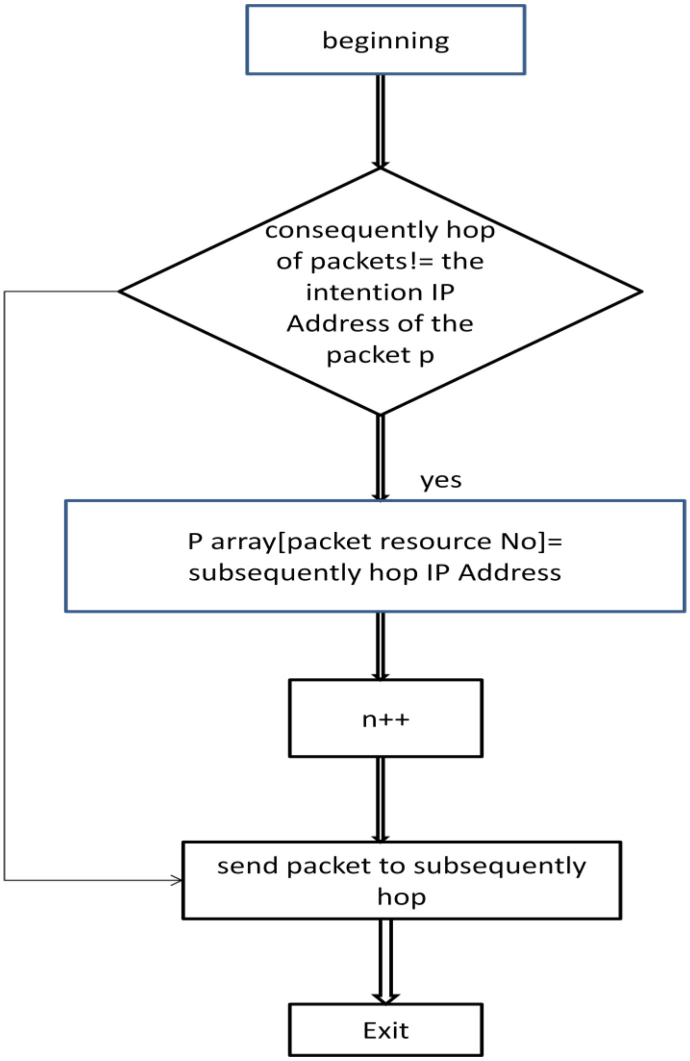
VANETs System consists of huge number of nodes, around number of vehicles exceeding million in the world today [13], these vehicles will necessitate an authority to govern it, every vehicle can communicate with other vehicles using short radio signal for range can reach 1 KM, this communication is an Ad Hoc communication that means each associated node can progress liberally, no wires required, the routers used called Road Side Unit, the Road Side Unit works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit attach the vehicle with Road Side Unit via DSRC radios, and a dissimilar device is Tamper Proof Device this device benefit the vehicle secrets, all the information about the vehicle approximating keys, drivers distinctiveness, trip details, speed, rout …etc,

SYSTEM REPLICA AND SECURITY NECESSITIES

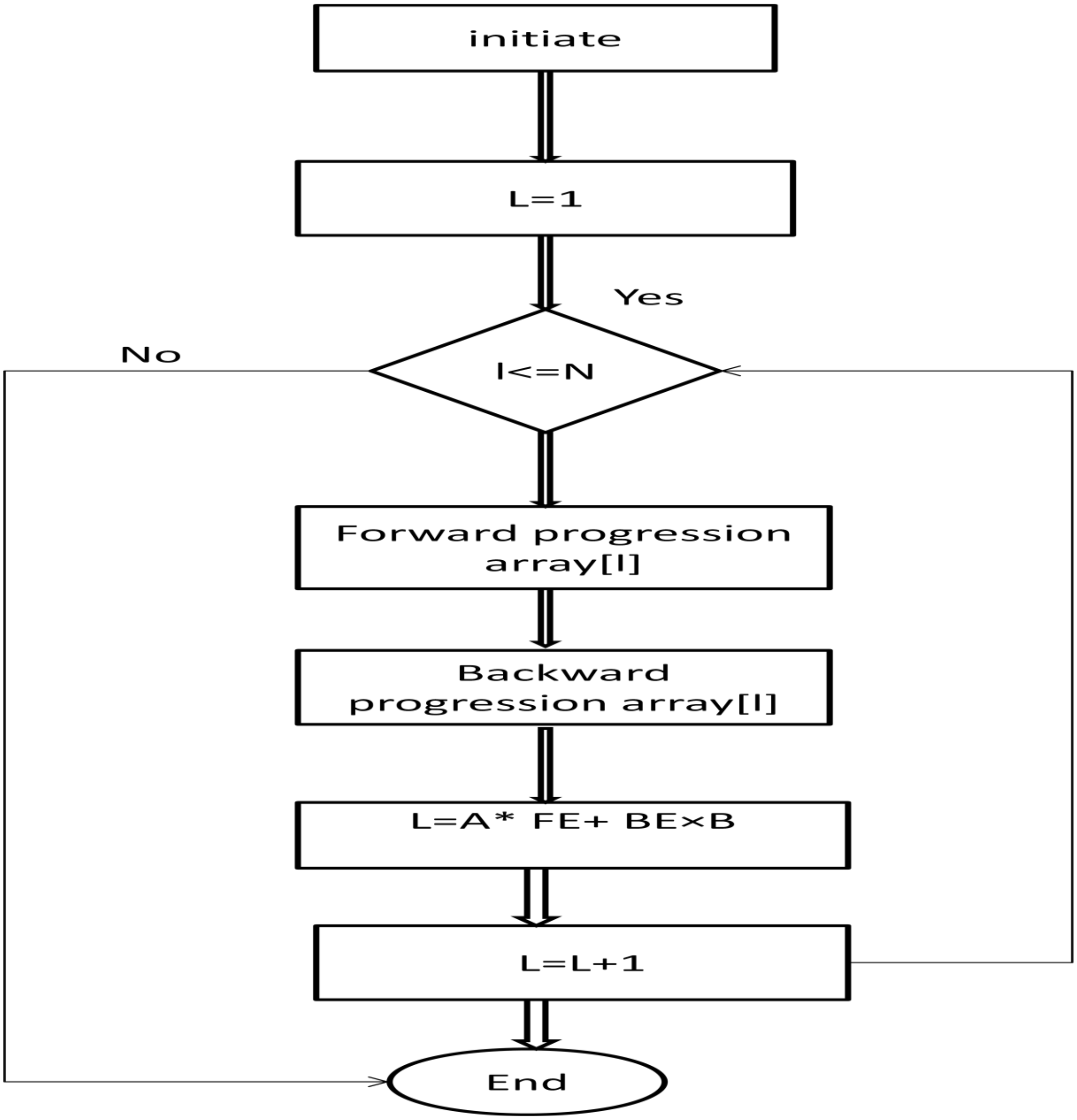
The system replica and security necessities will be obtainable in this section. When security method is declare, we assume that there is a public key supervision method obtainable. The data transfer among each two vehicles is signed by the sender and the signature requirements to be established no issue which node received it. The VANETs System replica is immediately consisted of several wireless nodes set on vehicles. The vehicles are set to move through a crossroad for the meantime some of them do multi-hop wireless communications based on the protocol. Figure 1 show the structural design of the network, and the regular routing multi-hop path. When one vehicle requirements to send a message to a further far away it will get the position information of the target vehicle several way, such as during GPS or other position located devices. And then it is packaged jointly with the sending message, routed by the position-based protocol resourcefully to the destination. nodes send message by attractive benefit of the position information of added nodes and jointly with the security strategy to prefer which node is the subsequently hop. furthermore this replica tries best to fit the district of the real transportation system. The method can be abbreviation into two aspects: (1) Routing message protection mechanism; (2) Node evaluation mechanism. For the protection of the routing message, a signature verified scheme is employed to achieve end-to-end authentication and integrity of the data. And for the evaluation mechanism, every node is turned on hybrid surveillance mode and checks every packet send by its neighbor. The protocol estimate the reliability of neighbor nodes by checking its forwarding ratio (the ratio of packets forwarded to received).


Initialize
IP Address(p)==Address(this)
No
Yes
obtain this packet and go above to the greater layer
Exit
utilize PBRP discover the subsequently hop
Node n>threshold
Yes
Node n is protocol
No
Yes
renovate the subsequently hop of p and change the last hop of p as the IP Address of this node m
n is next hop

Phase I


beginning
consequently hop of packets!= the intention IP Address of the packet p
yes
P array[packet resource No]= subsequently hop IP Address
n++
send packet to subsequently hop
Exit

Phase II



Phase III

The assessment method is divided into two aspects: forward progression and backward progression. Forward progression is employed to discover out the drop malicious nodes. The operational opinion of the forward progression is as follows: Assuming that node n is the neighbor of node m, and taking an example that node m access node n to give details how forward progression method workings. When node m forwards or sends packets to node n, node m process the packet as approach described.

Phase III of technique is how the node m records every exact packet to node n.

Phase II is functional in listening function. a different part of forward progression, node m counts the packets of neighbor n usually send depending on it. PhaseII is to verify if the packet p send by node n is received from node m. And then increases on the counter which records the number of packets node n send usually. Phase III is a part of a timer implementation in the protocol. This algorithm essentially used to analyze the estimate value of each neighbor of node m. A certain time slot can be set to adjust the valuation frequency is to figure out the forward progression value based on the data record prior

different parameters used for performance estimate are: Throughput*:* It is the quantity of data per time unit that is deliver from one node to a different via a communication link The throughput is deliberate in Packets per unit TIL or bits per TIL. TIL(Time Interval Length)additional is the throughput of sending and receiving packets enhanced is the performance. minor is the throughput of dropping packets enhanced is the performance. standard throughput: It is the standard of entirety throughput. It is moreover deliberate in Packets per unit TIL or bits per TIL Packet Drop: It illustrate entirety number of data packets that might not accomplish destination effectively. The explanation for packet drop may arise due to congestion, faulty hardware and queue. Simulation time consider 200s , packets size 64bytes Rate 2 packets/s ,radio radius 100m max speed of nodes 5 m/s data flow varies node thresholds ψ ,evaluation Δt ,2s spiteful nodes quantity 1 overflow etc. Lower packet drop rate shows higher protocol performance. Packet size: Size of packets in bytes. Average simulation End to End delay. This metric give the on the whole delay, from packet transmission by the application agent at the source node till packet reception by the application agent at the destination node. Lower delay illustrate higher protocol performance. The subsequent equation is used to estimate the average end-to-end delay, Average End to End Delay = (T_DataR – T_DataS), Where T_DataR = Time data packets received at destination node T_DataS = Time data packets sent from source node. The end to end delay is significant metrics because VANET requirements a diminutive latency to deliver quick messages. It demonstrates the appropriateness of the protocol for the VANET. Simulation time*:* Total time taken for simulation. It is deliberate in seconds. Experiment has been carried out for three dissimilar numbers of nodes under a variety of cases and consequences are drawn and estimate. The numbers of nodes used are:

I. 4 nodes

II. 10 nodes

III. 25 nodes
consequences are evaluate for following cases:

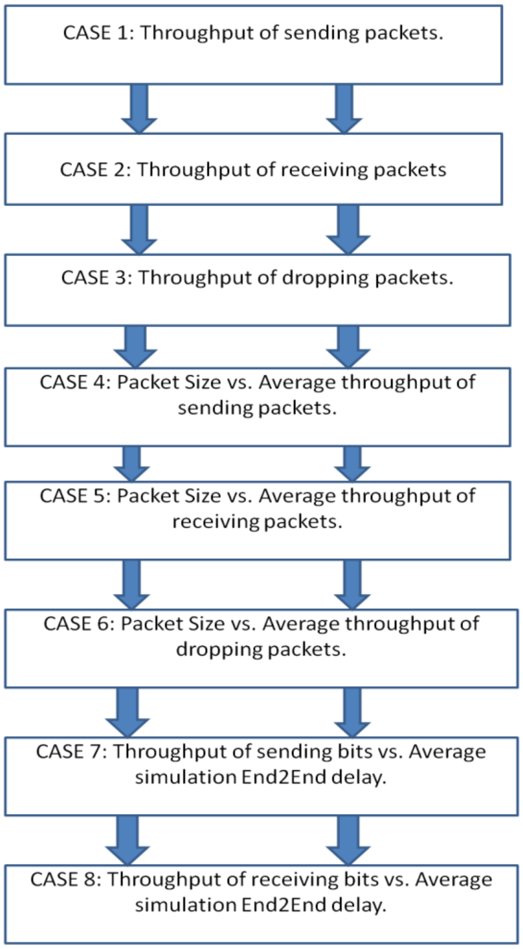
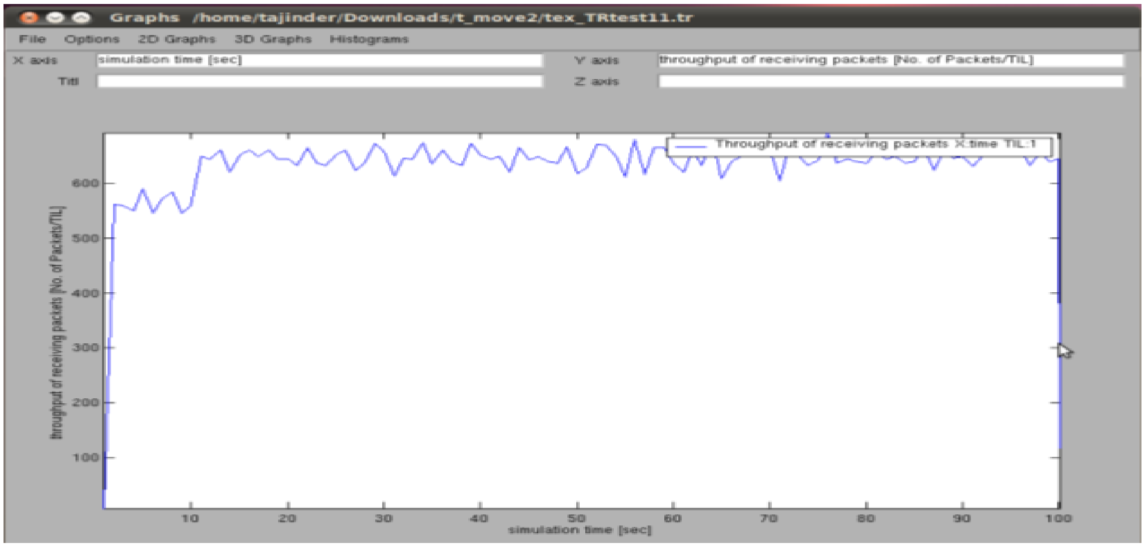

CASE 1: Throughput of sending packets.
CASE 2: Throughput of receiving packets
CASE 3: Throughput of dropping packets.
CASE 4: Packet Size vs. Average throughput of sending packets.
CASE 5: Packet Size vs. Average throughput of receiving packets.
CASE 6: Packet Size vs. Average throughput of dropping packets.
CASE 7: Throughput of sending bits vs. Average simulation End2End delay.
CASE 8: Throughput of receiving bits vs. Average simulation End2End delay.

figure : 1 flows chart position-based routing in vanets



Graphs /home/tajinder/Downloads/t_move2/tex_TRtest11.tr

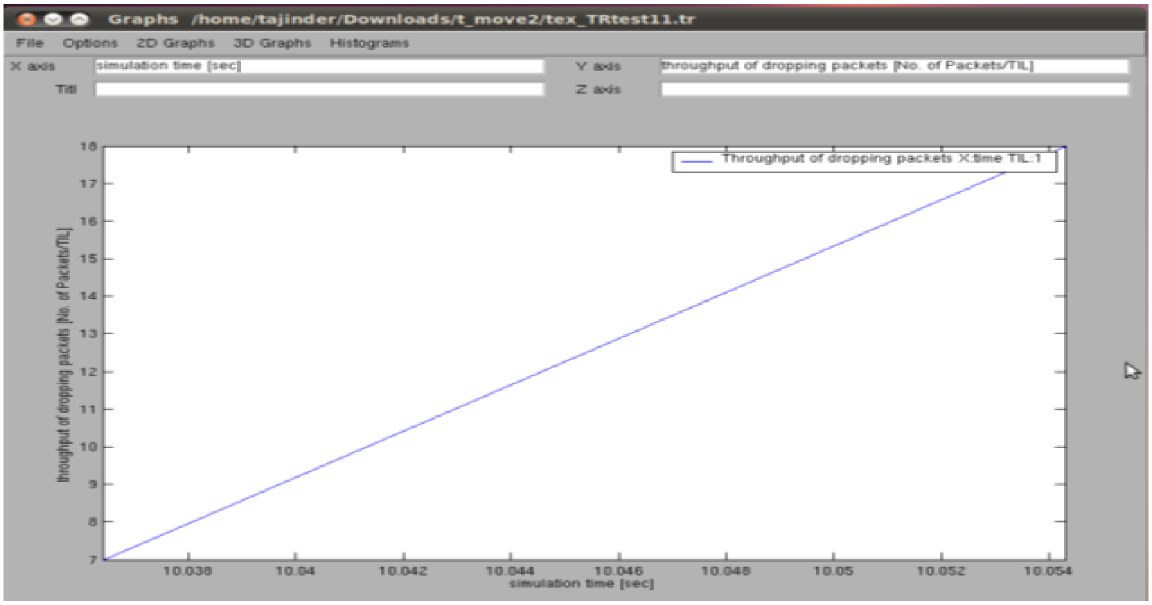
X axis: simulation time [sec]

Y axis: throughput of receiving packets [No. of Packets/TIL]

Titl:

Z axis:

Figure 2: Throughput of receiving packets [no. of packets/TIL]



Graphs /home/tajinder/Downloads/t_move2/tex_TRtest11.tr

X axis: simulation time [sec]

Y axis: throughput of dropping packets [No. of Packets/TIL]

Titl:

Z axis:

Figure 3: Throughput dropping packets [no. of packets/TIL] Throughput of Sending packets for 10 nodes Throughput of receiving packets for 10 nodes Throughput of dropping packets for 10 nodes

CONCLUSIONS

A protection technique for PBRP was proposed in this research. The major initiative of the method is the estimate method. The resolution joins the digital signatures/ certificates. Digital signatures applied to end-to-end, hop-to-hop to protect the routing message from being tampered by malicious nodes, and assistant to backward progression method. Another part of the progression mechanism is forward progression method. It mostly used to perceive the drop-malicious nodes. The major contribution of the resolution is that the difficulty which the cryptosystem can't treaty with has been solved, such as drop packets to remains the efficiency of the routing protocol. The throughput and losing rate are mutually improved than other two protocols.

REFERENCES

[1]. S. S. Dorle, Bhushan Vidhale,Megha Chakole," Evaluation of Multipath, Unipath and Hybrid Routing Protocols for Vehicular Ad Hoc Networks" Fourth International Conference on Emerging Trends in Engineering & Technology-2011.

[2]. Hind AI Falasi, Ezedin Barka," Revocation in V ANETs: A Survey" International Conference on Innovations in Information Technology-2011.

[3]. Jie Hou, Lei Han, Jiqiang Liu, Jia Zhao," Secure and Efficient Protocol for Position-based Routing in VANETs" 978-1-4673-1332-2/12-2012 IEEE.

[4]. Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna," Hybrid Routing Protocols to Secure Network Layer for Mobile Ad hoc Networks" 978-1-4244-5967-4/10/2010 IEEE.

[5]. Yonglin Ren, Azzedine Boukerche and Richard Werner Nelem Pazzi," Performance Evaluation of a Hybrid Cryptosystem with Authentication for Wireless Ad hoc Networks " This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

[6]. Hui Liu, Hui Li, Zhanxin Ma," Efficient and Secure Authentication Protocol for VANET" International Conference on Computational Intelligence and Security-

2010.

[7]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures," Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)"

[8]. Charles Harsch, Andreas Festag , Panos Papadimitratos, "Secure Position-Based Routing for VANETs," VehicularTechnology Conference, Baltimore, Fall, 2007, pp. 26-30.

[9]. G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in VANET '07: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. ACM, 2007, pp. 19–28. [Online].Available:http://dx.doi.org/10.1145/1287748.1287752.

[10]. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications," in INFOCOM. IEEE, 2008, pp. 1229–1237.

[11]. S. D. Galbraith, K. G. Paterson, and N. P. Smart,"Pairings for cryptographers," Discrete Appl. Math., vol.156, pp. 3113–3121, September 2008.[Online]. Available: http://portal.acm.org/citation.cfm?id=1450345.1450543

[12]. S. Biswas and J. V. Misic, "Deploying proxy signature in vanets," in GLOBECOM. IEEE, 2010, pp. 1–6.

[13]. SUMO-Simulation of urban mobility [EB/OL]. http://sumo.sourceforge.net/. Access time: 2011-08-27.

[14]. Nizar Alsharif, Albert Wasef, and Xuemin (Sherman) Shen, "ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks," GLOBECOM-IEEE Global Telecommunications Conference, Miami, December, 2010, pp. 1-5.

[15]. Brad Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking, New York, August, 2000, pp. 243-254.

[16]. SUMO-Simulation of urban mobility [EB/OL]. http://sumo.sourceforge.net/. Access time: 2011-08-27.