Security Based Neighbour Selection for Vehicular Ad-Hoc Networks

Diksha Pandey, Manvendra, Anil Kumar

Abstract: ***This Research work acquaint with algorithms Security Based Neighbor Selection. In Security based neighbor selection vehicles with authentic Id can take part in the network. Disseminating messages in an open access environment makes a real security and privacy challenges in VANETs. For using the application of VANET effectively the Quality of service and security should be maintained. In this piece of work Security Based Neighbor Selection technique is used to enhance the QoS and safety applications in VANETs by providing unique ID to the vehicles so that the secure transmission of messages takes place. This technique is proposed to maintain the security and QoS and to accomplish the aim of reliable information exchange. By using NS-3 simulator we accomplished that our proposed technique shows an enhancements regarding awareness in safety and upgrades QoS metrics in VANETs.***

Keywords: VANETs, QoS, Security level, Neighbour Selection.

I. INTRODUCTION

VANETs composed of vehicle to connect with each other and to form a large network with vehicles acting as network nodes. The main aim behind the VANETs concept is to make a Smart transportation system. Safety associated solicitations are the foremost intent of inter-vehicle communications. With the help of VANETs application accidents could be avoided by disseminating messages in between the vehicles. VANETs gives a wide scope of facilities like collision avoidance, a contrivance for regulating traffic flow, provisions of internet facility to on-road public, info about the parking lots, cafeterias, gas stations also, infotainment applications. Security Adaptation is major concern in VANETs. It establishes a network with the other vehicles using wireless transceivers, GPS, sensors. Distribution of motion information regarding traffic with other vehicles paradigm Local Dynamic Map (LDM) helps better information about the vehicles neighborhood traffic [1],[2]. Periodic spread of Cooperative Awareness Messages (CAMs) is a crucial necessity to circumstance a latest LDM by means of the vehicles [3]. CAMs consist of GPS data of the transferring vehicles in consort with other motion information like its speed, heading, and so on. Depending on data received through CAMs, vehicles sort quick driving verdicts such as track change, smearing brakes and crossroads [4]. For Safety applications of Vehicles it provides precise information to the car driver and propagates CAMs by means of a extraordinary delivery ratio and vigorous security contrivance [5]. Subsequently QoS and Security are the two important parameters to strengthen the Vehicles safety [7].

Revised Manuscript Received on August 03, 2019.

Diksha Pandey, M.tech scholar, Department of ECE, SHUATS, Prayagraj, India.

Manvendra, Assistant Professor, Department Of ECE, SHUATS, Prayagraj, India.

Anil Kumar, Head of Department, Department of ECE, SHUATS, Prayagraj, India.

VANETs exposed to numerous difficulty regarding security that can reason congestion in network or facts venality. To certify its consistency IEEE and ETSI standards suggested a security schemes [6]. Discovery of Neighbor is the primary step to set up the connectivity passage with near-by sensors. The foremost tenacity is discovering of a neighbor at the earliest opportunity while utilizing minimum power in the network [8]. In this piece of work we proposed a technique known as Security Based Neighbor Selection (SBNS). The foremost notion behind is that to compute the security level within the vehicles and with its neighbor vehicles. The vehicles with only the registered ID proof can only transmit the messages. Obtained results through NS-3 simulation determine that the prospective technique achieve significant enhancements in relations to various QoS metrics. This piece of work has been organised as Section II analyses literature related to neighbor discovery problems. Section III explains our proposed security based neighbor selection technique. Section IV presents simulation approach also enactment assessment of the projected technique for VANETs safeness exertions. Section V enticements the finish of the paper.

II. RELATED WORKS

A. Neighbor Selection

Discovering of Neighbor is the first and foremost route to inculcate a communication passage or to create an ad hoc network with near-by sensors and then we can apply vital security methods. Various conventions have been introduced for the same. Difficulty in discovering of neighbor considered over multiplicity of customs. Several protocols have been acquainted to flabbergast the problem of neighbor discovery so as to prolong the lifespan of system by reducing energy [8]. Aimed at asynchronous discovery of neighbor in stagnant temporary network the Birthday protocols has been proposed and this protocols centres on power savings in networks when nodes are deployed and also on energy effectual finding later disposition [9]. The hypothetical preparation for quantifying the presentation of discovering neighbor named as U-connect protocol. According to this protocol the process of combinatorial has the poor invisibility for discovery of neighbor [10]. The idea of selecting neighbors based on slots has not been new many approaches have been projected regarding selecting neighbors based on time slots. In [11] an algorithm has been used which forecasts the likely amalgamation smashes owing to the overtaking of fast automobiles. Recommends vehicles to acquire new time-slot and provides 2-hop neighbourhood and reduces the merging and access delays. In [12] a scheme based on hybrid MAC which is centred on priority that integrates

TDMA and CSMA/CA schemes each node determines its own slot. Various techniques have been introduced based on slot like in-band control mechanism [13] to exchange TDMA slot information.

III. OUR PROPOSAL

A. Security Based Neighbor Selection

In this section a new framework for secure announcements in VANETs has been presented. The main notion behind the technique stands that vehicles assess the security level in their zone and centred on this facts, the transmission of the CAMs takes place. Vehicle maintains the LDM contains information of nearby neighbors. For improving QoS the adaptive security has progressed toward becoming a key issue in perspective of VANETs. This technique emphasis on constructing the confidentiality and verification procedure more competent in edict to enhance QoS. It uses registered ID to prevent it from external attackers. Only registered vehicles are allowed to receive and transmit messages. The vehicles will have unique IP address which will work as unique ID for the vehicle.

B. Slot Based Neighbor Selection

In Slot Based Neighbor selection (SLNS) the messages are grouped into different slots and then slots are preferred centred on priority. The slot which has highest no. of messages would be given priority and is further transmitted. The below mentioned flow chart explains that the firstly the vehicular network has been created then the neighbors are selected and then divided into different slots then ID verification is applied and if the slot time is less than current time then the processing of packet will take place and security would be applied and further proccessed for transmisssion otherwise the packets would be denied.

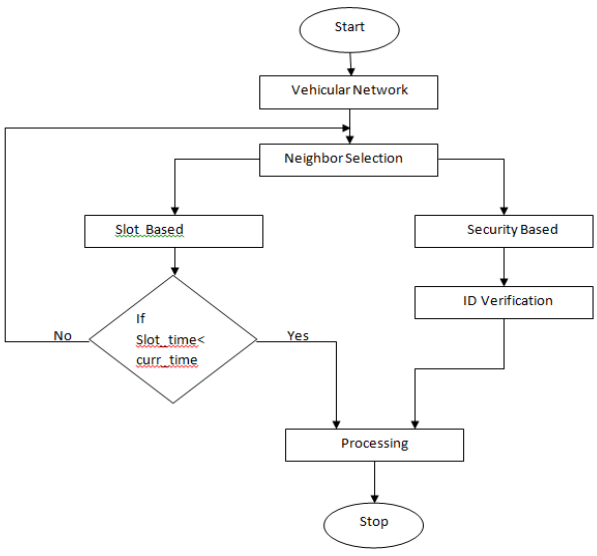

Fig.1. Flow chart

C. Algorithm (Security based neighbor selection)

Set Routing= SBNS
Send Authorization to sender;
For each node u that received an private key
Establish route link;
Send data to established path;
}
Else
{
receiver not exist ;
}
Else
{
node out of range or node is died
}
Sender node transmits the packet;

The above algorithm applies security to the node by providing authentic ID.

IV. PERFORMANCE EVALUATIONS

To appraise execution of Security Based Neighbor Selection accompanied thorough simulation studies. Herein fragment illustrated the simulation settings along with a discussion of the results we have found through simulation NS-3.

A. Simulation Setting

We accompanied the simulation assessments utilizing SUMO, produces realistic traffic traces and NS-3 network simulator. By help of WAVE representative accessible in NS-3 model collections also executed Security Based Neighbor Selection algorithm. For simulation purpose we take a 5 km long road with 3 lanes per direction.

Table 1 Simulation Factors

Parameters	Values
Road Length	5 km
Number of Lanes	6 lanes
Density of Vehicle	51-251 vehicles/km
Speed of vehicles	20-35 m/s
Size of Packet	500-600 bytes
Generation Interval	100ms
Speed of Data	6Mpbs
Range of transmission	500m

Subsequent are performance metrics

- **Security Queuing Delay (QD):** Difference between time while messages are expected by vehicle and the interval time security verification for that message starts. Messages are established at receiver stay positioned in a security row and are confirmed one subsequently the other.
- **Packet Delivery Ratio (PDR):** Number of automobiles inside safe zone that positively received messages divided by number of automobiles in safe zone.
- **Packet-inter arrival time (PIAT):** Interval of time taken among the couple of successive messages commencing a specific source within enclosed safe parts.
- **Percentage Received Packets (PRP):** It is the ratio of received messages by the destination to generation of messages by the source. Four safe zone parts are declared in our presentation i) 0-50m ii) 50-100m iii) 100m-140m iv) less than 250m

We compare our Security Based Neighbor Selection with the other two techniques

- **Slot Based Neighbor Selection:** In Slot Based Neighbor Selection (SLNS) the messages are grouped into different slots and then slots are selected based on priority which is having higher number of messages based on which neighbor is selected and transmit message.
- **Trust Based Security adaptation**: Trust level is figured using three parameters like centrality, duration of connectivity and level of security accordingly the security is mapped.

B. Simulation Results

In the below graphs the red line represents the trust-based, red line represents slot-based neighbor selection and blue line represents security based neighbor selection.

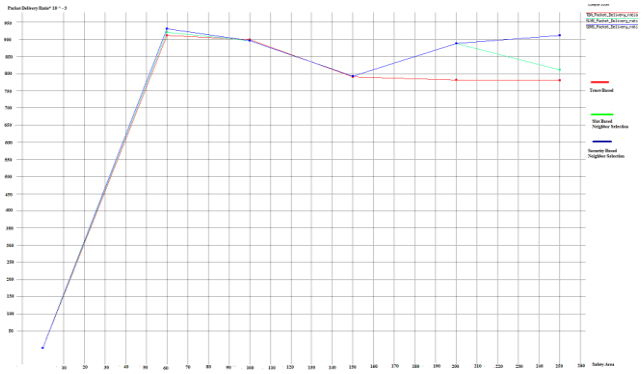

Fig.2. PDR

PDR

Fig.2 demonstrates the delivery ratio of packets at diverse safe parts. Trust-based outcomes in delivery ratio of packets of 0.9 for the safety area of 60m. The delivery ratio of packets falls and touches 0.7 at 250m of safe zone. The Slot Based Neighbor Selection progresses values of delivery ratio in contrast toward Trust-based which results 0.9, 0.8, 0.7, 0.88 and 0.81 of PDR value at 60m, 100m, 150m, 200m and 250m of safety areas respectively. When compared with these two techniques Security Based Neighbor Selection avails a PDR of more than 0.8 for all safe-zone areas.

Table 2 PDR

Safe-Zone Area (m)	PDR (TBA)	PDR (SLNS)	PDR (SBNS)
0-60	0.91	0.92	0.93
100-150	0.79	0.79	0.80
200-250	0.78	0.81	0.91

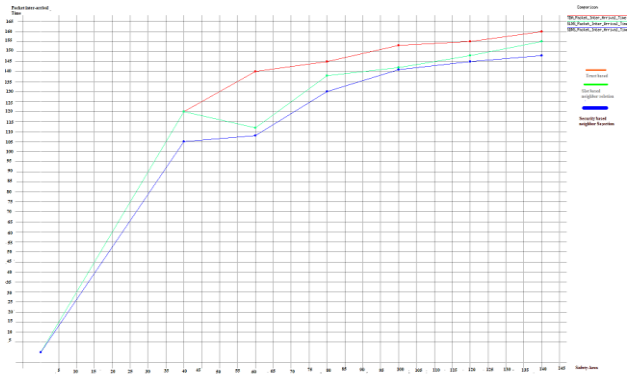

Fig.3. PIAT

PIAT

Fig.3 demonstrates the PIAT for CAMs. Trust based accomplished the utmost CAMs PIAT that confines commencing 120-160ms for mentioned safe-zone. Slot Based Neighbor Selection tactic sustains a PIAT lesser than 145ms for safe part of 100m however outcomes in increased inter-arrival time subsequently. Interestingly, the Security Based Neighbor Selection accomplishes PIAT of beneath 150ms aimed at mentioned safe zone

Table 3 PIAT

Safe-zone Area (m)	PIAT (TBA)	PIAT (SLNS)	PIAT (SBNS)
0-60	120	112	108
60-100	150	142	141
100-150	160	155	148

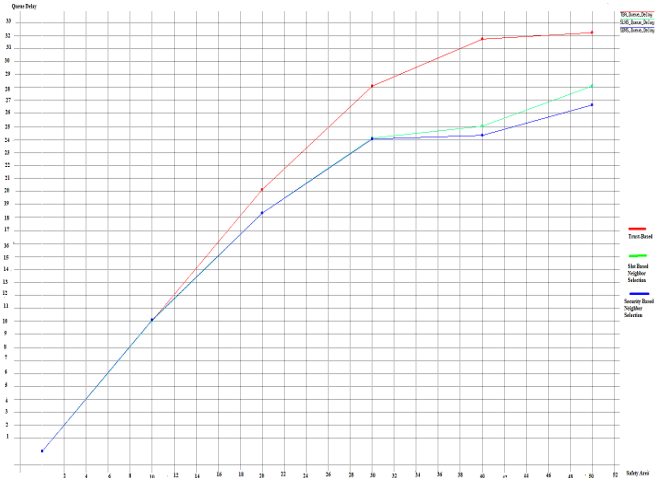

Fig.4. Security Queuing Delay

QD

Fig.4 demonstrates the queuing delays for different safe parts. Trust-based mechanism delivers a security queuing deferral of about 22ms for safe-zone parts. In Slot Based Neighbor Selection the security queuing delay results in 20ms for almost all safe zones. In contrast, the Security Based Neighbor Selection provides a queuing delay of less than 20ms for mentioned safe zone.

Table 4 QD

Safe-Zone Area (m)	QD (TBA)	QD (SLNS)	QD (SBNS)
0-30	28.09	24.10	24.02
30-50	32.23	28.12	26.66

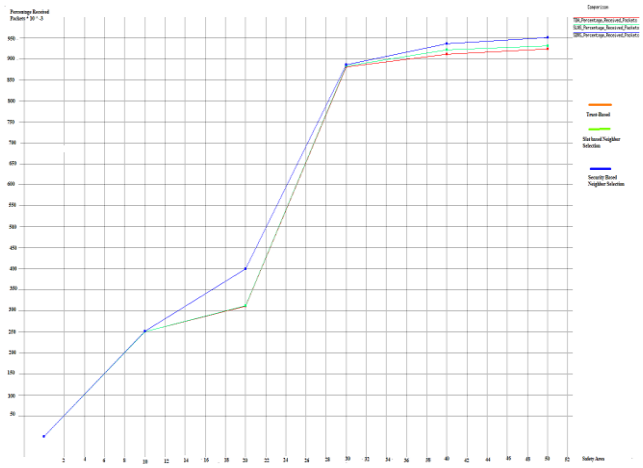

Fig.5. PRP

PRP

Fig.5 shows that the percentage received packets in trust-based gives better result as the safety area increases from 10m to 50m at 50 m the percentage received packet is 0.9. In Slot based neighbor selection it gives a better result than Trust-based, but in Security Based Neighbor Selection at 50m it exceeding 0.95.

Table 5 PRP

Safe-zone Area (m)	PRP (TBA)	PRP (SLNS)	PRP (SBNS)
0-30	0.81	0.84	0.86
30-50	0.92	0.93	0.95

V. Conclusions

In this piece of work we talked about the security issues faced by VANETs. Keeping in mind the security issues proposed a security based neighbor selection technique to enhance security and QoS. Improving Security is key contrivance that can enhance QoS and safety in VANETs. It is problematic to adapt the vital security method that might be adjusted. Facing this confrontation we acquaint with a Security Based Neighbor Selection technique in which we apply effective algorithm and get an improved results when compared to other two techniques. Using NS-3 simulation results we presented that our Security Based neighbor Selection outperforms other two techniques such as Slot Based Neighbor Selection and Trust-based in respect to different QoS metrics.

REFRENCES:

1. L.W. Chen and H.W. Shih "Design and analysis of an infrastructure less framework for lane positioning, tracking, and requesting through vehicular sensor networks," IEEE Communications Letters, vol. 20, no. 10, pp. 2083–2086, Oct 2016.
2. A. Ghosh, V. V. Paranthaman, G. Mapp, O. Gemikonakli, and J. Loo, "Enabling seamless v2i communications: toward developing cooperative automotive applications in vanet systems," IEEE Communications Magazine, vol. 53, no. 12, pp. 80–86, 2015.
3. K. Liu, J. K. Y. Ng, V. C. S. Lee, S. H. Son, and I. Stojmenovic, "Cooperative data scheduling in hybrid vehicular ad hoc networks: Vanet as a software defined network," IEEE/ACM Transactions on Networking, vol. 24, no. 3, pp. 1759–1773, June 2016.
4. Muhammad Awais Javed, Sherali Zeadally and Zara Hamid "Trust Based Security Adaptation Mechanism For Vehicular Sensor Networks" Computer Networks.
5. F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985–2996, Dec 2015.
6. .M. A. Javed, E. B. Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice." Sensors, vol. 16, no. 6, p. 879, July 2016.
7. 7. F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," Proc. IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp.2985-2996, Dec 2015.
8. 8.Sangil Choi and Gangman Yi "Asymmetric Block Design-Based Neighbor Discovery Protocol in Sensor Networks".
9. McGlynn, M.J.; Borbash, S.A. Birthday protocols for low energy deployment and flexible neighbor discovery in Ad Hoc wireless networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, CA, USA, 4–5 October 2001; pp. 137–145.
10. Kandhalu, A. Lakshmanan, K. Rajkumar, R. U-connect: A low-latency energy-efficient asynchronous neighbor discovery protocol. In Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks, Stockholm, Sweden, 12–15 April 2010; pp. 350–361.
11. Ranbir Singh and Kulwinder Singh Mann "Efficient Time Slot Allocation to Minimize Collision in TDMA Based VANETs" Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 12, December (2017).
12. W. Cho, "Hybrid MAC scheme for vehicular communications," International Journal of distributed Sensor Networks, vol. 2013.
13. F. Yu and S. Biswas, "A Self-Organizing MAC Protocol for DSRC based Vehicular Ad Hoc Networks," Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on, Toronto, Ont., 2007, pp. 88-88.

AUTHORS PROFILE

Diksha Pandey received Bachelor of Technology in Electronics & Communication from SHUATS (Formerly known as A.A.I-DU), Allahabad in 2017. Pursuing Masters of Technology in Wireless Communication Engineering. One publication in UGC approved journal Member at IEEE Organization. Area of intrest is Ad-hoc Networks..

Manvendra He received his Bachelor of Technology in Electronics & Communication from Hindustan College of Science & Technology, (Uttar Pradesh Technical University Lucknow) Mathura in 2009 and completed M.tech in Communication System Engineering from SHUATS In 2012 and Qualified UGC-NET in 2014. He is currently Pursuing PhD in Antenna theory and Wave propagation.

Dr. Anil Kumar is Assistant Professor in ECE Department at SHUATS Prayagraj (Allahabad). He obtained B.E from MMMEC Gorakhpur in ECE, M.Tech. from IIT BHU Formerly IT B.H.U. Varanasi in Microelectronics Engg. And he has done Ph.D. from SHIATS-DU Allahabad. He guided various projects & research at undergraduate & postgraduate level. He published many research papers in different journals. He has more than 14 years teaching experience and actively involved in research and publications. His area of interest includes Antenna, microwave, artificial neural network and VLSI