https://doi.org/10.48047/AFJBS.6.12.2024.4936-4944

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Security-Enhanced Neighbor Selection for VANETS

Akhil Pannala [1], Komatineni Harinadh [2], Madireddi Venkata Satya Sai Suhaas [3], Dr.A. Raja Basha [4]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh. akhilpannala2004@gmail.com
[2] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh. komatineniharinadh@gmail.com
[3] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh. suhaasmadireddi2004@gmail.com
[4] Principal Investigator - Govt of India Project.
Associate Professor, Department of CSE, Koneru Lakshmaiah Education Foundation (K.L. University), Vaddeswaram, AP India, arajabasha@kluniversity.in

Article History
Volume 6, Issue 12, 2024
Received: June 10, 2024
Accepted: July 5, 2024
doi:
10.48047/AFJBS.6.12.2024.4936-4944

Abstract-This research work introduces the "Security-Based Neighbour Selection" algorithms, which are designed to enhance the security and quality of service (QoS) in Vehicular Ad-Hoc Networks (VANETs). In VANETs, ensuring the authenticity of participating vehicles is crucial due to the open access nature of the network, which poses significant security and privacy challenges. To effectively utilize VANET applications, it is imperative to maintain both QoS and security standards. The "Security-enhanced Neighbour Selection" technique is proposed to address these challenges by assigning unique IDs to vehicles, thereby ensuring secure message transmission. This approach aims to bolster security and maintain QoS while facilitating reliable information exchange. Through the use of the NS-3 simulator, our research demonstrates that the proposed technique leads to improvements in safety awareness and enhances QoS metrics within VANETs.

Keywords: VANETs, QoS, Security Level, Neighbor Selection.

1. Introduction

Vehicle Ad-Hoc Networks (VANETs) indeed aim to create a smart and interconnected transportation system by allowing vehicles to communicate with each other, and with infrastructure such as traffic lights or road signs. The primary objectives and features of VANETs are:

Safety Applications: One of the primary objectives of VANETs is to enhance road safety. Vehicles can exchange real-time information about their position, speed, and any potential hazards. This information can be used to warn drivers about accidents, road conditions, and other safety-related issues.

Accident Avoidance: VANETs enable vehicles to communicate and provide warnings to drivers about potential collisions or hazards ahead. For example, if a vehicle suddenly brakes

or encounters an obstacle, it can broadcast this information to nearby vehicles, which can take appropriate actions to avoid accidents.

Traffic Flow Control: VANETs can help in optimizing traffic flow by providing information about traffic congestion, accidents, and alternative routes. This can lead to more efficient transportation systems.

Internet Access: VANETs can offer internet connectivity to on-road users. This can be useful for navigation, real-time traffic updates, and other online services.

Parking Information: VANETs can provide real-time information about available parking spaces, helping drivers find parking more easily, which can reduce traffic congestion and fuel consumption.

Cafeteria and Gas Station Information: VANETs can share data about nearby services like cafeterias, gas stations, and rest areas, making it convenient for drivers to locate these facilities during their journey.

Infotainment Applications: VANETs can enable infotainment services for passengers, such as in-car entertainment, news, and multimedia content.

The distribution of motion information in the context of traffic with other vehicles and the use of a Local Dynamic Map (LDM) to improve information about the vehicles in the neighborhood [1] [2]. Vehicles use CAMs to share their motion-related information, which is crucial for maintaining an up-to-date LDM [3]. The LDM, in turn, helps vehicles make informed driving decisions by providing a real-time view of the traffic conditions in their immediate vicinity. This is a key component of cooperative intelligent transportation systems designed to improve road safety and traffic flow. 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]. Quality of Service (QoS) and security play vital roles in enhancing vehicle safety in the context of cooperative vehicular communication systems. These systems are designed to minimize accidents, enhance traffic safety, and improve overall driving conditions [7].

VANETs face security challenges that can affect network performance and data integrity. Standards recommended by IEEE and ETSI help address these challenges [6]. The first step in establishing communication within VANETs is the discovery of neighboring devices, and doing so efficiently with minimal power usage is a critical aspect of network operation [8].

SBNS technique as a means to improve security and QoS in vehicular communication networks. It highlights the importance of authenticating vehicles and only allowing those with registered ID proof to transmit messages. The technique's effectiveness is demonstrated through NS-3 simulation, where it is shown to enhance various QoS metrics

SBNS technique as a means to improve security and QoS in vehicular communication networks. It highlights the importance of authenticating vehicles and only allowing those with registered ID proof to transmit messages. The technique's effectiveness is demonstrated through NS-3 simulation, where it is shown to enhance various QoS metrics. This piece of work has been organized 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

2. Related Works

A. Neighbor Selection

Neighbor discovery as the first step in establishing communication networks and implementing security methods. It also mentions the existence of multiple protocols and conventions to address the challenges of neighbor discovery, with an emphasis on energy

conservation to extend the system's lifespan. The problem of neighbor discovery so as to prolong the lifespan of system by reducing energy [8]. The Birthday protocol is introduced as a method for asynchronous neighbor discovery in stationary temporary networks. It places a strong emphasis on power savings and energy-efficient discovery, making it suitable for networks where efficient energy use is a priority [9]. The U-connect protocol and its approach to quantifying neighbor discovery performance. It suggests that the protocol has challenges related to poor invisibility in neighbor discovery [10] and mentions that the idea of selecting neighbors based on time slots is not a novel concept, as it has been explored in various approaches to quantifying neighbor discovery performance. It suggests that the protocol has challenges related to poor invisibility in neighbor discovery [10] and mentions that the idea of selecting neighbors based on time slots is not a novel concept, idea of selecting neighbors based on time slots is not a novel concept, as it has been explored in various approaches and protocols in 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 neighborhood and reduces the merging and access delays. In [12] a scheme based on hybrid MAC which is centered 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.

3. Our Proposal

A. Security based Neighbor Selection

Security-based neighbor selection refers to a concept often utilized in networking and computer security. It involves the process of selecting neighboring nodes or devices in a network based on their security properties or characteristics. The goal is to establish a secure and trusted network environment by choosing neighbors that are less likely to pose security risks or vulnerabilities.

Here are some key points related to security-based neighbor selection:

Trust and Security: The selection of neighbors is essential in various networking scenarios, such as in peer-to-peer networks, ad-hoc networks, or Internet of Things (IoT) environments. By choosing secure and trustworthy neighbors, the overall security and reliability of the network can be improved.

Security Metrics: When implementing security-based neighbor selection, specific security metrics and criteria are typically defined to assess the trustworthiness of potential neighbors. These metrics may include factors like device authentication, encryption capabilities, past behavior, reputation, and the presence of security software or mechanisms.

Dynamic Networks: In dynamic networks, where devices or nodes join and leave the network frequently, security-based neighbor selection becomes even more critical. Selecting reliable neighbors can help prevent malicious or compromised devices from infiltrating the network.

Trust Models: Trust models and algorithms are often used to calculate the level of trust or security associated with each potential neighbor. These models can be based on historical data, peer reviews, or other factors, depending on the specific application.

Mitigating Attacks: Security-based neighbor selection can help in mitigating various attacks, such as man-in-the-middle attacks, where an attacker intercepts communications between two legitimate parties. By selecting secure neighbors, the likelihood of such attacks can be reduced.

Resource Efficiency: In resource-constrained environments, like IoT networks, where devices have limited processing power and memory, selecting secure neighbors is crucial to optimize resource allocation and prevent unauthorized access or data breaches.

Challenges: Implementing security-based neighbor selection can be challenging. It requires a balance between security and network performance. Overly stringent security criteria might limit network connectivity, while too lax criteria can expose the network to vulnerabilities.
Security-based neighbor selection is part of a broader framework for network security, ensuring that the devices or nodes in a network can trust each other, communicate securely, and collectively contribute to a more resilient and secure.
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 centered 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 centered 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 processed for transmission otherwise the packets would be denied.

```
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;
```

Set Routing to SBNS: This step seems to indicate that the algorithm will use the Security-Based Neighbor Selection (SBNS) routing method for secure communication.
Send Authorization to Sender: An authorization step is used, which may involve authenticating the sender before proceeding with communication. This is an essential security measure to ensure that the sender is legitimate.
For Each Node u That Received a Private Key:
Establish Route Link: A route link is established for each node that has received a private key. This step likely involves setting up a secure communication channel.
Send Data to Established Path: Once the secure route link is established, data can be sent through this path. The data is transmitted securely over the established path.
Else (Receiver Not Exist): This appears to be an error or an exception handling scenario. If the receiver node does not exist, the algorithm handles this situation.

Else (Node Out of Range or Node Is Dead): Similarly, if the node is out of range or has become inoperative (i.e., "died"), the algorithm deals with this scenario.
Sender Node Transmits the Packet: If all conditions are met, and the authorization and security checks are successful, the sender node transmits the packet securely.
The above algorithm ensures effectiveness and applies security to the node by providing authentic ID.

4. Performance Evaluations

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

A. Simulation Setting

Using NS-3 network simulator we accompanied the simulation assessments utilizing SUMO which produces realistic traffic traces. 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):** is a metric used in the context of network security, particularly in scenarios where data packets or messages need to undergo security checks or processing before being transmitted through the network. It represents the time delay or latency introduced by the security-related processing tasks that packets go through in a network.
- **Packet Delivery Ratio (PDR):** PDR is defined as the ratio of automobiles inside safe zone that positively received messages divided by number of automobiles in a safe zone.
- **Packet-inter Arrival Time (PIAT):** It is the time interval between the arrivals of successive data packets at a network node or device. It's a fundamental concept in understanding and analyzing network traffic and performance.

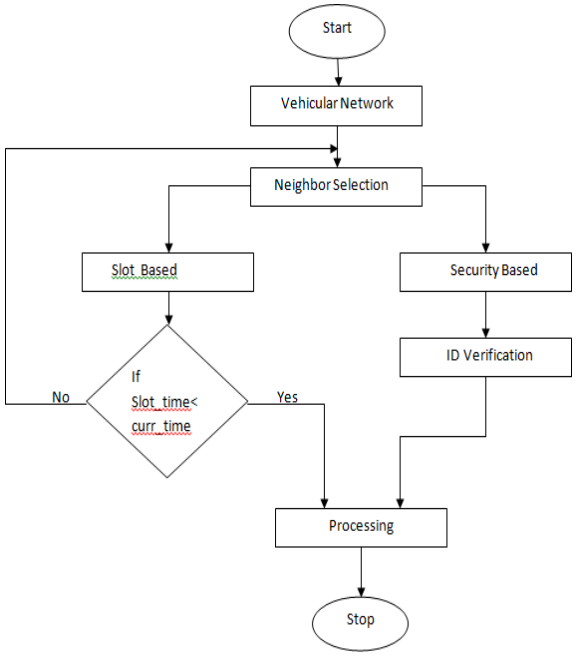

Figure 1. Flow Chart

B. Algorithm (Security based Neighbor Selection)

- **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.

C. Simulation Results

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

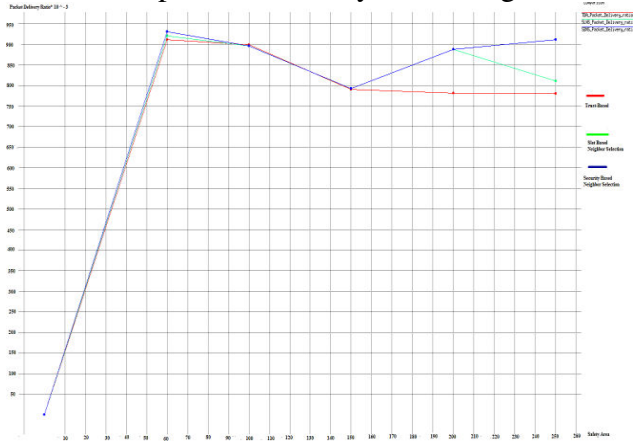

Figure 2. PDR

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. Neighbor Selection avails a 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**

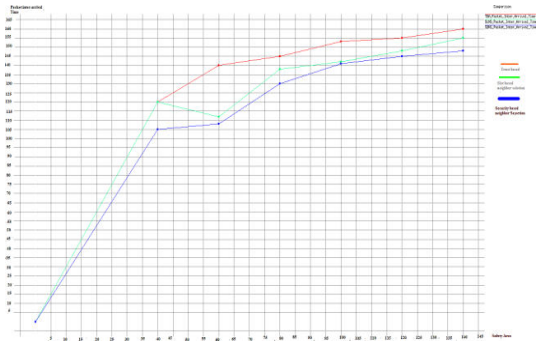

Figure 3. PIAT

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**

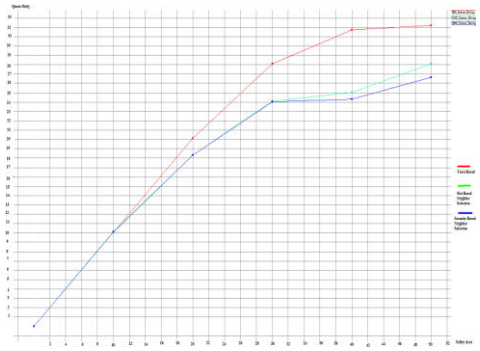

Figure 4. Security Queuing Delay

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

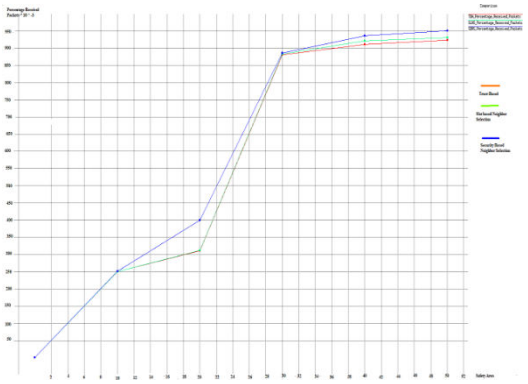

Figure 5. PRP

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.

5. Conclusions

This research focused on the security issues in Vehicular Ad Hoc Networks (VANETs) and have proposed a Security-Based Neighbor Selection technique to enhance security and Quality of Service (QoS). The combination of security and QoS is indeed crucial for the efficient and safe operation of VANETs. We have conducted simulations using NS-3 and found that your Security-Based Neighbor Selection technique outperforms other techniques like Slot-Based Neighbor Selection and Trust-Based methods in terms of various QoS metrics.

References

[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] 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] 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] 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.