Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 613–623
DOI : 10.47974/JDMSC-1905

Proposed approach for securing VANET by detection and avoidance of Sybil attack

Anil Pal [#]
Department of Computer Applications
Suresh Gyan Vihar University
Jaipur
Rajasthan
India

Dinesh Goyal [†]
Department of Computer Science & Engineering
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India

Satyajeet Sharma [§]
Shruti Mathur [‡]
Jitendra Kumawat [@]
Gajanand Sharma *
Department of Computer Science & Engineering
JECRC University
Jaipur
Rajasthan
India

Abstract

Our world has gone fully mobile, and with advanced technologies, communication in this dynamic era has been possible with MANET and VANET. Along with the facilities extended to our pockets, the security of our data has also been a big concern. The VANET

[#] *E-mail:* anilpalbarala@gmail.com
[†] *E-mail:* dinesh8dg@gmail.com
[§] *E-mail:* sharma.satyajeet24@gmail.com
[‡] *E-mail:* smsavi@gmail.com
[@] *E-mail:* drkumawatjitendra@gmail.com
* *E-mail:* gajanan.sharma@gmail.com (Corresponding Author)

network has numerous obstacles to maintaining information security. One aspect of the suggested study is finding the Sybil node and ensuring measures for avoiding the same in VANET. The proposed model uses improved RC4A data encryption to protect the network from Sybil attacks.

Subject Classification: *68M10, 68M12, 68M25.*

Keywords: *SYBIL ATTACK, NSFRP, OSFRP, AODV, RC4, RC4A, NS2.*

1. Introduction

In recent years, one of the most important areas of emphasis in the field of computer science networking has been the achievement of secure communication between vehicles. A vehicle-mounted ad hoc network (VANET) is a mobile ad hoc network that enables communication between vehicles and fixed roadside equipment nearby. Services related to information and entertainment, as well as traffic management and safety-related information, are the primary functions of the VANET. The VANET system is extremely vulnerable to a variety of attacks, including the dissemination of false alert messages, if it does not have adequate system security.

The Sybil attack, one of the most popular attacks in VANET, is also one of the most well-known active attacks. This type of attack allows the attacker to send multiple messages to other vehicles, each of which contains a different fabricated source identity (ID). It creates a false sense of illusion for other vehicles, which results in a breakdown in communication.

Numerous security standards must be met to preserve the security of vehicle communications that must be met to prevent the Sybil attack from occurring in VANET. These requirements include anonymity and privacy, availability, confidentiality, identity verification, integrity, non-repudiation, traceability, and similar requirements.

2. Review of Literature

By facilitating communication between vehicles, the VANET has demonstrated the potential to lessen the number of fatalities and injuries that occur on the roads. Road operators are also able to control and monitor vehicles through the use of VANET, which enables safer driving and faster rescues. The fact that these networks enable communication through the use of wireless media makes them susceptible to a variety of security

attacks. The Sybil attack in VANET has the potential to cause malicious vehicles to send error messages concerning traffic, traffic accidents that are ahead, road closures, and other related topics. This could force the driver of the car to take a different route, which would make him more likely to be involved in accidents that are not appropriate. As part of this [1] study, the authors investigated various detection strategies that are utilized to identify Sybil attacks. Furthermore, it presents a comparison between various models that are already in existence.

The author of this work proposed Sybil node detection technology implementation using a timestamp technique. Within the scope of this work, the time stamp is the sole certificate that RSU offers to each and every vehicle that is currently operating within VANET. In the work that was proposed for the discovery of Sybil nodes and the transmission of data, they utilized the routing protocol unique to Ad-Hoc On-Demand Distance Vector (AODV) that includes the timestamp for the public key hash function. This allowed them to identify Sybil nodes without any difficulty [2, 6].

A revolution has been brought about in SMART CITY as a result of the onboard ad-hoc network. V2V and V2I are the two modes of communication that are utilized by the VANET, In the work, the authors [3,9] discuss the difficulty of ensuring the safety of networks within vehicles and simulate two different kinds of attacks: Blackhole attacks and Sybil attacks. They also investigate the impact that these attacks have on the performance of vehicle networks using average throughput as a case study.

An author in [4] has made an effort to discover the potential security measures that can be implemented over VANET by utilizing the AODV to identify and handle particular kinds of attacks. Intending to stop the source node from attacking the network, they make use of the RSA algorithm to identify attacks on sensors and the messages they send containing them.

3. Methodology

The rogue node will reflect its identity in several places in the case of a Sybil attack, which will ultimately lead to the disappearance of the route or a delay in the transmission of packets. The malicious nodes are taken into account by the proposed protocol, which is known as NSFRP. This is because the malicious nodes are not encrypted using RC4, and the success

of the protocol can be evaluated by analyzing the reduction in the delay in packet transmission.

OSFRP, which stands for Old Secure Framework Routing Protocol, is a method that adheres to the idea that every node that is participating in the communication must always have a public/private key pair and be able to perform digital signature verification. This method is used to defend against Sybil attacks in the network. The keys need to be associated with the MAC address and the IP address of the node, and they should also be allowed to other nodes that are within the transmission range. This ensures that the nodes are verified uniquely if the public keys are already known for communication purposes.

An improved RC4 security technique was appended to the novel protocol known as NSFRP (New Secure Framework Routing Protocol), which was originally discussed in our earlier paper [5]. This was done to prevent the Sybil attack from occurring in VANET. To prevent the attack, we employ encryption and authentication by utilizing the improved RC4 Algorithm. However, if an attack does occur, we are required to identify the malicious nodes, and our NSFRP technique prevents the participation of such nodes in the network is shown in Figure 1.

3.1 *Improved RC4 A (RC4 Advanced) Encryption technique used for securing packets*

RC4 uses 2 state arrays Sa1 and Sa2, and 2 indexes k1 and k2. Every time i incremented, and two bytes were generated:

```
i = 0, k1 = 0, k2 = 0
While Producing Results:
    i = i + 1
    k1 = k1 + Sa1[i]
    swap the values for Sa1[i] and Sa1[k1]
    output Sa2[Sa1[i] + Sa1[k1]]
    k2 = k2 + Sa2[i]
    swap the values of Sa2[i] and Sa2[k2]
    output Sa1[Sa2[i] + Sa2[j2]]
endwhile
```

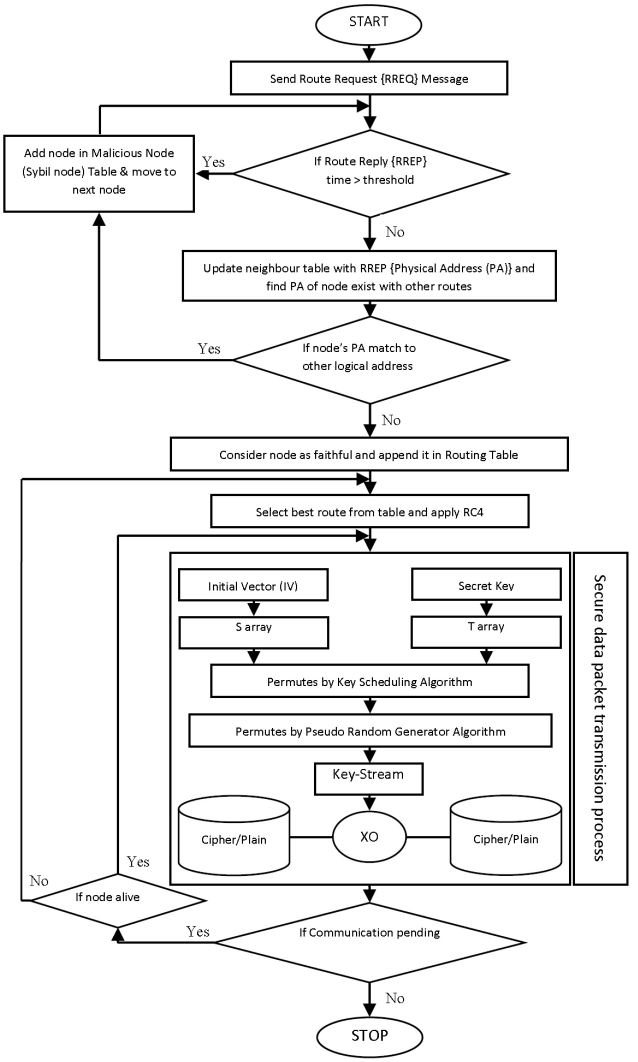

Figure 1

The NSFRP flow diagram for detection and avoidance of sybil disorders

4. Result and Analysis

The model that was proposed earlier is currently being evaluated on NS2 to accomplish a greater accurate realization of the suggested model's performance.

4.1 *Simulation Scenario*

To evaluate the efficacy of the suggested protocol, both the existing protocols (SFRP) and the proposed protocols (NSFRP) were put into action in the Scenario that is presented below in Figure 2, both with and without an attack.

SN	Parameters	Specification
1	Simulator	NS2
2	Simulation time	10000 msec
3	Routing Protocol	OSFRP, NSFRP
4	Number of node in each module	50
5	Node Movement	Random
6	Traffic Model	CBR(Constant Bit Rate)
7	MAC type	Mac/802_11
8	Antenna Model	Omni antenna
9	Channel type	Channel/WirelessChannel
10	Network interface type	Phy/WirelessPhy
11	Radio-propagation model	Propagation/TwoRayGround
12	Interface queue type	Queue/DropTail/PriQueue
13	Type of packet send	User Datagram Protocol
14	Data Packet	512 bytes
15	Max packet in Interface queue	200

Figure 2

Simulation parameters used in NS2

4.2 *Performance Parameter metrics*

1. $PDR = \frac{DR}{DR+DL}$
2. $\text{AVERAGE\_DELAY} = \sum_{i=0}^{n} \left(\frac{End\ time - Start\ time}{Total\ no.of\ Packets} \right)$
3. $\text{ENERGY\_SPEND} = Total\ Energy - Remaining\ Energy$

4.3 *Result of the Experiment*

The current protocol (SFRP) and the suggested protocol (NSFRP) were compared in two distinct scenarios: the Sybil attack scenario and the regular Scenario. Three parameters were used in this investigation. This analysis was conducted to assess the effectiveness of our suggested paradigm as shown in Table 1.

Table 1

The outcomes of the average delay, energy spend, and packet delivery ratio for SFRP and the NSFRP under assault and without attack are compared.

SN	PROTOCOL	TIME	PDR	AVG._DELAY	ENERGY_SPEND
1	SFRP (In Normal Environment)	0	0	0	0
		2	0.45	1504	16.4
		4	0.49	1277	16.57
		6	0.5	1198	16.73
		8	0.53	1135	16.92
		10	0.56	1103	17.1
2	NSFRP (In Normal Environment)	0	0	0	0
		2	0	0	3.62
		4	0.71	78	12.78
		6	0.68	103	13.05
		8	0.74	98	13.19
		10	0.73	103	13.46
3	SFRP (Under Attack Environment)	0	0	0	0
		2	0.32	3112	16.51
		4	0.35	2317	16.74
		6	0.4	1933	16.93
		8	0.45	1685	17.14
		10	0.48	1592	17.27
4	NSFRP (Under Attack Environment)	0	0	0	0
		2	0.8	44	12.63
		4	0.83	86	12.66
		6	0.86	106	13.11
		8	0.89	105	13.29
		10	0.9	108	13.58

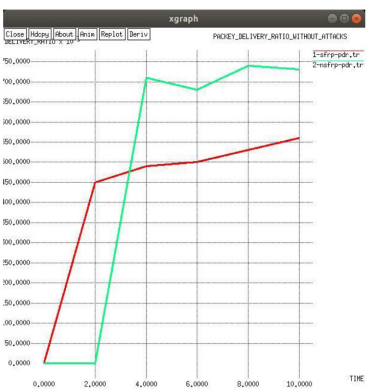

Figure 3

Comparing the packets delivered in SFRP and NSFRP

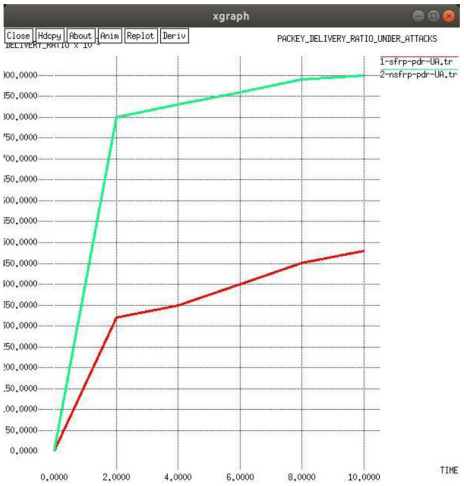

Figure 4

PDR in NSFRP-UA and SFRP-UA

Because of the security measures that have been implemented and measured in NSFRP in VANET as shown in Figure 3 and Figure 4, it is possible to effortlessly observe, the proposed protocol has a packet delivery ratio that is significantly higher than the existing protocol, SFRP, by 23.62 and 85.72 percent, respectively.

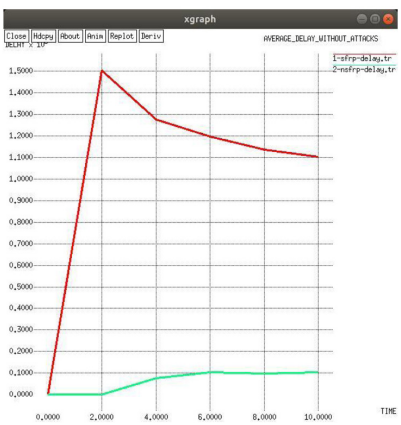

Figure 5

Average delay in SFRP and NSFRP environments

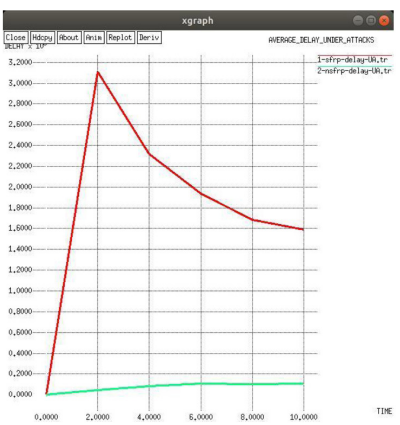

Figure 6

Average delay in SFRP-UA and NSFRP-UA

Because of the security measures that have been implemented and measured in NSFRP in VANET as shown in Figure 5 and Figure 6, it is possible to effortlessly observe, the proposed protocol has an average delay that is between 92.09 and 93.21% less than the delay that is experienced by the SFRP protocol that is currently in use.

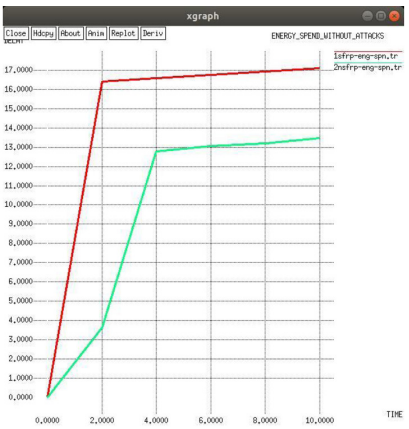

Figure 7

Comparing the amount of energy spent in SFRP and NSFRP

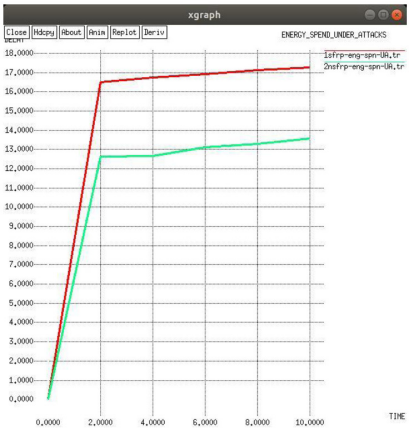

Figure 8

Comparing the energy spent in SFRP-UA and NSFRP-UA

Because of the security measures that have been implemented and measured in NSFRP in VANET as shown in Figure 7 and Figure 8, it is possible to effortlessly observe, the proposed protocol consumes 24.70 and 21.34 percent less energy than the protocol that is currently in use, which is SFRP to begin with.

5. Conclusion

Using improved RC4A (RC4 Advanced) encryption and decryption cryptography over VANET, the work that is being proposed presents a robust mechanism for the secure transmission of data in an attack environment. It is possible to deliver data packets with more secure mechanisms thanks to the detection of the Sybil node and the countermeasures that are taken against it, as well as the RC4A-generated encryption and decryption keys. In light of the experiment's results, the proposed model demonstrates superior performance in terms of energy consumption, the ratio of packets delivered, and the average delay, and

this holds true regardless of whether the VANET environment is subject to a Sybil attack or not. The proposed model has the potential to be utilized in the future to work on other types of attacks in VANET and MANET.

References

[1] Upadhyay, U., Kumar, A., Sharma, G., Saini, A. K., Arya, V., Gaurav, A., & Chui, K. T., Mitigating Risks in the Cloud-Based Metaverse Access Control Strategies and Techniques. *International Journal of Cloud Applications and Computing (IJCAC)*, 14(1), 1-30 (2024).

[2] Syed Mohd Faisal and Taskeen Zaidi, "Timestamp Based Detection of Sybil Attack in VANET", *International Journal of Cyber Security*, Volume 22, Issue 3, pp. 399-410 (May 2020).

[3] P. Shah and T. Kasbe, "Detecting Sybil Attack, Black Hole Attack and DoS Attack in VANET Using RSA Algorithm", 2021 Emerging Trends in Industry 4.0 (ETI 4.0), pp. 1-7 (2021), https://doi.org/10.1109/ETI4.051663.2021.9619414.

[4] Anil Pal, Bright Keswani and Dinesh Goyal. "Analysis and design of secure VANET by detection and avoidance of blackhole attack", *Journal of Discrete Mathematical Sciences and Cryptography* (2022), ISSN 0972-0529, https://doi.org/10.1080/09720529.2022.2075091

[5] Muhammad Arif et al., "SDN-based VANETs, Security Attacks, Applications and Challenges", *Applied Science,* Volume 10, Issue 9, pp. 3217(1-51) (May 2020), ISSN 2076-3417, https://doi.org/10.3390/app10093217.

[6] Sharma, S., Sharma, G., & Menghani, E., The Role of CNN in Detection and Prediction of Tomato Leaf Disease: A review. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence, pp. 1-5 (2022, December).

[7] D. Manivannan, Shafika Showkat Moni and Sherali Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)", *Vehicular Communications,* Volume 25, pp. 100247 (2020), ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2020.100247.

[8] Ayoub Toubi and Tomader Mazri, "Attacks against security in the vehicular network and the impact of Sybil attack and Blackhole attack on the vehicular network performances: average Throughput as a study of case", *International Journal of Information Science and*

Technology (IJIST), Volume 4, Issue 2, pp. 12-21 (July 2020), ISSN 2550-5114, http://www.innove.org/ijist/index.php/ijist/article/download/70/103

[9] Sharma, G., Hemrajani, N., Sharma, S., Upadhyay, A., Bhardwaj, Y., & Kumar, A., Data management framework for IoT edge-cloud architecture for resource-constrained IoT application. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(4), 1093-1103 (2022).

[10] Ajay N. Upadhyaya and J. S. Shah, "ATTACKS ON VANET SECURITY", *International Journal of Computer Engineering & Technology* (IJCET), Volume 9, Issue 1, pp. 8-19 (Jan-Feb 2018), ISSN 0976-6367, https://www.researchgate.net/project/Security-in-VANET.

[11] T. Zaidi and Syed.Faisal, "An Overview: Various Attacks in VANET", 4th International Conference on Computing Communication and Automation (ICCCA), pp. 1-6 (2018), ISSN 2642-7354, https://doi.org/10.1109/CCAA.2018.8777538.

[12] Waleed Kh, and Shaimaa Hameed, "Methods of Secure Routing Protocol in Wireless Sensor Networks", *Journal of Al-Qadisiyah for Computer Science and Mathematics*, Volume 10, Issue 3, pp. 38-55 (2018), ISSN 2074-0204, https://doi.org/10.29304/jqcm.2018.10.3.437.