An Efficient Implementation of a Method to Detect Sybil Attacks in Vehicular Ad hoc Networks using Received Signal Strength Indicator

B. Keerthi Samhitha, Suja Cherukullapurath Mana, Jithina Jose, M. Mohith, L. Siva Chandhrahasa Reddy

***Abstract:** Vehicular Ad Hoc Networks (VANET) are useful in implementing a smart transportation system by enabling ad hoc vehicle to vehicle communication. Sybil attack is considered to be one of the most dangerous threats to VANET. Sybil aggressor can produce different phony personalities with false messages to extremely hinder the ordinary elements of wellbeing related applications. In this paper, we are presenting an implementation of a method to detect Sybil attack using received signal strength indicator.*

***Index Terms:** Vehicular ad hoc networks, Sybil attack, RSSI, voiceprint.*

I. INTRODUCTION

Because of the vast number of wounds and fatalities brought about by traffic-related accidents, traffic wellbeing is a major concern overall [11]. Car crashes are essentially brought about by human mistake, for example, a driver's moderate response to nearby visual and acoustic signals or dangerous activities because of deficient traffic data [18]. Vehicular specially appointed networks (VANETs) have risen as a promising way to deal with expanding traffic security and avoiding impacts by upgrading both the exactness of traffic data and the conveyance of alerts. innovation to address the testing issues in the keen transportation framework (ITS, for example, mishap evasion, traffic monitoring and transport productivity. VANETs empower a vehicle to straightforwardly speak with neighboring vehicles (vehicle to-vehicle, V2V) just as roadside frameworks (vehicle to-foundation, V2I). As indicated by a report distributed by National Highway Traffic Safety Administration, VANETs can give a wide scope of correspondence based vehicle wellbeing and non-security applications in ITS, for example, crossing point crash evasion, agreeable impact cautioning, crisis electronic brake lights, traffic stream control and upgraded course direction and route [1].

Numerous kinds of assaults can be propelled in VANETs; however a standout amongst the most hurtful is Sybil assault [2]. As previously mentioned, numerous security or non-wellbeing applications in VANETs, for example, helpful crash cautioning and upgraded course direction and route need participation of different vehicles. This requires one vehicle gets enough believable data from authentic vehicles. Be that as it may, in Sybil assault, foe (malevolent hub) produces various phony personalities to make numerous virtual hubs (Sybil hubs) in VANETs. This disregards the major supposition in actualizing those applications [3]. Because of the extreme harm when Sybil assault occurs, numerous discovery strategies are proposed by specialists. Every one of these networks can be arranged into three classifications: asset testing based, believed accreditation based and position confirmation based components. The asset testing based strategies may end up invalid if the malevolent hub has more calculation or correspondence assets, and they convey additional overhead to the framework.

A large portion of the believed accreditation based strategies run the location calculations in a concentrated way which are not reasonable for the VANETs because of the quick changing powerful topology. What's more, the organization of open key framework and the high unpredictability of cryptographic calculations are likewise dubious issues in this kind of techniques. Thinking about the ease, wide accessibility and decentralized nature, the physical estimation based position confirmation techniques are better to recognize Sybil assaults in the underlying phase of VANETs. In this paper, we propose a novel Sybil assault location technique dependent on RSSI, Voiceprint, to direct a generally appropriate, lightweight and full-circulated identification for VANETs. Not at all like the greater part of past RSSI-based strategies that figure the supreme position or relative separation as indicated by the normal RSSI qualities, or make measurement testing dependent on RSSI circulations, has Voiceprint utilized the RSSI time arrangement as the vehicular discourse to looks at the comparability among all these time arrangement. This methodology depends on the real perception in our genuine examinations that the RSSI time arrangement of Sybil hubs have the fundamentally the same as examples.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

Ms. Keerthi Samhitha*, Assistant Professor, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

Ms. Suja Cherukulapurath Mana, Assistant Professor, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

Ms. Jithina Jose, Assistant Professor, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

Mr. Mohith, Undergraduate Student, School of computing, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

Mr. Siva Chandrahasa Reddy, Undergraduate Student, School of computing, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

The fundamental commitment of this paper is three-overlay: 1) Voiceprint can be broadly connected to genuine VANETs with no predefined radio spread model. Broad reenactments and analyses demonstrate the pertinence of the proposed strategy. It has high discovery rate over 90% and low false positive rate under 10% in various powerful conditions. (show free, broadly pertinent); 2) Voiceprint can make autonomous identification with no assistance of different vehicles, subsequently, it doesn't require to set up the believability of neighboring hubs (trust sans relationship, lightweight); 3) Voiceprint is a completely circulated calculation with no incorporated control or backing of RSU (infrastructure free, completely appropriated).

II. RELATED WORKS

Because of the quick changing unique topology of VANETs and the high multifaceted nature of cryptographic calculations, the lightweight and decentralized location strategies like position confirmation based techniques are progressively reasonable for the vehicular condition. These techniques as a rule embrace some physical estimation, for example, Received Signal Strength Indicator (RSSI), Angle of Arrival (AoA) and Time Difference of Arrival (TDoA) to evaluate the places of the neighboring hubs. These deliberate qualities just rely upon the equipment what's more, physical condition that can't be effectively manufactured or altered by the malignant hub.

In paper [13] authors describes about an approach based on ant colony algorithm to prevent Sybil attack. RSSI-based networks, on the other hand, are minimal effort techniques with no particular equipment. They are based on the possibility that recipient can assess separate from the sender as indicated by RSSI values utilizing hypothetical radio spread models. Y.Yao et al.[14] utilized RSSI-based strategy to identify Sybil hubs in a static Wireless Sensor Network (WSN) .

M. Li *et al* proposed a statistical scheme to detect Sybil attacks [16].In paper [4] authors suggest a method to detect Sybil attach using MAC &MAP techniques [4] . These techniques are specifically applicable in ad hoc networks.

The asset testing based strategies are futile if the vindictive hub is outfitted with adequate assets and they for the most part convey additional overhead to the framework when in testing. Believed accreditation based strategies are the most famous methods to set up trust relationship among all hubs. This sort of methodologies typically utilizes the endorsement specialist, open key foundation, computerized marks and cryptographic calculations to guarantee the reliability of every personality. They can discover Sybil hubs toward the start of the assault. Be that as it may, this sort of methodologies as a rule requires a brought together trust gathering to issue computerized marks or authentications which can't be effectively connected in the underlying phase of VANETs.

Synchronization in any case, requires additional equipment support. RSSI-based strategies, on the other hand, are ease techniques with no particular equipment. They are based on the possibility that collector can appraise separate from the sender as indicated by RSSI values utilizing hypothetical radio engendering models.

Y. Yao *et.al.* utilized RSSI-based confinement strategy to distinguish Sybil hubs in a static Wireless Sensor Network (WSN) [14]. They embraced proportion of RSSIs from different beneficiaries to beat the time changing and temperamental nature of estimated RSSI values. Most of the RSSI-based strategies are decentralized methods that every hub runs the location calculation locally without the incorporated framework. In any case, these techniques recognize Sybil assault in an agreeable way that every hub needs the data from neighboring hubs, i.e., to get RSSI values seen by different hubs around to illuminate conditions or figure the crossing point of suspect gatherings. In this way, the serious issue in these strategies is the means by which to affirm the believability and trustworthiness of the neighboring hubs, since the Sybil hubs created by the noxious hub may send fashioned RSSI qualities to obstruct the identification.

III. PROBLEM STATEMENT

The asset testing based techniques may end up invalid if the noxious hub has more calculation or correspondence assets, and they convey additional overhead to the framework. Believed confirmation based techniques run the identification calculations in a brought together way which are not appropriate for the VANETs because of the quick changing powerful topology

IV. EXISTING SYSTEM

In Existing Network Protocols can be characterized into three classes: Resource testing based, believed accreditation based, Position check based components. The asset testing based strategies may end up invalid if the noxious hub has more calculation or correspondence assets, and they convey additional overhead to the framework. The majority of the believed confirmation based strategies run the discovery calculations in a brought together way which is not reasonable for the VANETs because of the quick changing powerful topology. What's more, the arrangement of open key foundation and the high intricacy of cryptographic calculations are likewise unsure issues in this kind of techniques

V. PROPOSED NETWORK

In proposed framework we are actualizing a novel Sybil assault identification technique, Voiceprint to lead a broadly pertinent, lightweight and full-circulated recognition for VANETs. Not at all like a large portion of past RSSI-based strategies had that figure the supreme position or relative separation as indicated by the normal RSSI qualities, or make measurement testing dependent on RSSI circulations, has Voiceprint looked at the RSSI time arrangement as the vehicular discourse.

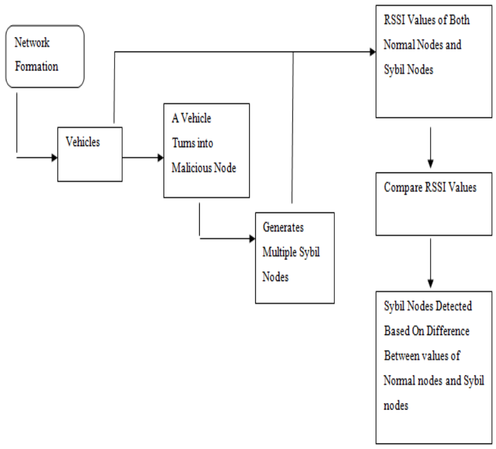

Network Formation
Vehicles
A Vehicle Turns into Malicious Node
Generates Multiple Sybil Nodes
RSSI Values of Both Normal Nodes and Sybil Nodes
Compare RSSI Values
Sybil Nodes Detected Based On Difference Between values of Normal nodes and Sybil nodes

Fig 1 Overview of the Proposed Network

The proposed technique does not depend on any radio spread model which can be generally connected to various street situations (show free, broadly pertinent); Each single hub as an indicator can make autonomous recognition with no assistance of different vehicles, along these lines, it doesn't require to set up the believability of neighboring hubs (trust sans relationship, lightweight); We actualize a full-dispersed calculation with no brought together control or backing of RSU (foundation free, full-appropriated). We enable Voiceprint to lead discovery on SCH which enormously abbreviate the perception time and diminish the bogus positive rate. We influence Bernaola Galvn Segmentation Algorithm (BGSA) [3] to distinguish unexpected changes in RSSI time arrangement so as to recognize those ill-conceived hubs performing power control.

VI. PROPOSED SYSTEM

In proposed system we are implementing a novel Sybil attack detection method, Voiceprint to conduct a widely applicable, lightweight and full-distributed detection for VANETs. In comparison with most of previous RSSI-based methods that compute the absolute position or relative distance according to the average RSSI values, or make statistic testing based on RSSI distributions, Voiceprint compares the RSSI time series as the vehicular speech.

VII. NETWORK MODEL

A. Network Formation

In this module, we make a network arrangement. A network arrangement comprises of hubs and circles. Every Node speaks to a circle which goes about as vehicles in network. Hubs are made dependent on position X-Axis. On the off chance that one hub X-Axis converges with other hub X-Axis they are neighbors. Neighbor hubs can speak with one another on the off chance that they are neighbors to one another. Every hub have one of a kind personality number to distinguish them.

B. Sybil Nodes Formation

After network development where every hub speaks to a hover which thus goes about as a vehicle, a hub in the network winds up noxious hub to assault the network with Sybil assault. Noxious hub will create different phony hubs with phony personalities and positions in the network. Counterfeit hubs are called as Sybil hubs.

C. Scenarios Based Sybil Attack

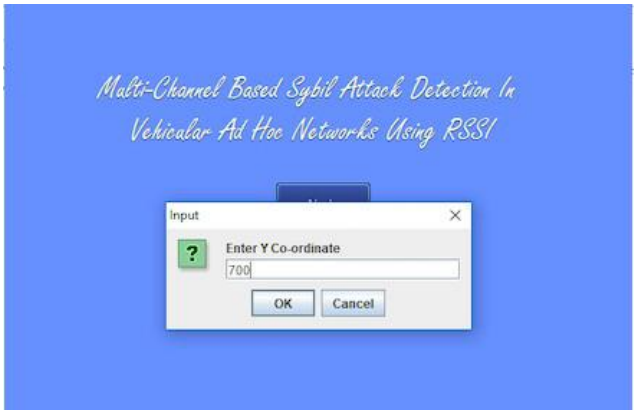
After Sybil hubs are made in the network the vindictive hub in the network begins Sybil assault. Sybil Attack makes a dream of a substantial traffic ahead for different vehicles adjacent. At that point, the neighboring vehicles may pick different courses while the aggressor can get the great street condition. Sybil assault can likewise accomplish more mischief by propelling dark opening assault in the network. We are building up this undertaking dependent on situations. One of the situation is the traffic situation in which we need to check how Sybil hubs respond in rush hour gridlock condition and typical hubs respond in rush hour gridlock condition.

D. Identifying Sybil Nodes

After pernicious hub dispatch Sybil assault we need to distinguish the Sybil hubs in the network utilizing RSSI (Received Signal Strength Indicator). We are utilizing a strategy called Voiceprint. Utilizing Voiceprint we are recognizing Sybil hubs utilizing RSSI time arrangement and look at the likeness among every gotten hub. In view of this Sybil hubs will be distinguished in the network.

VIII. SYSTEM IMPLEMENTATION

This section displays screen captures of the main functionalies of the system.



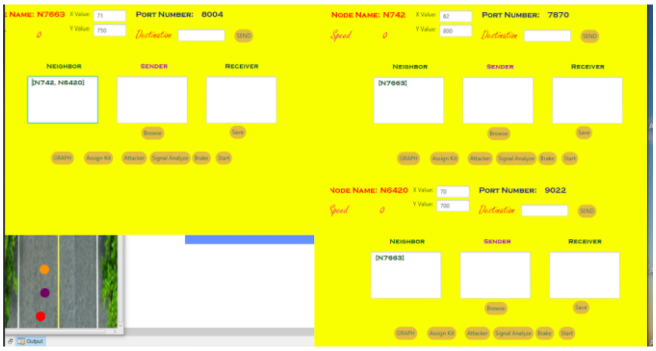
Multi-Channel Based Sybil Attack Detection In Vehicular Ad Hoc Networks Using RSSI

Input

Enter Y Co-ordinate: 700

Fig 2: Input phase

This preview (Fig 2) is the main page where the input has been taken. The user have to enter the co-ordinate value in the numbers and then click on "OK" and that forms a "NODE" in "VANET ENVIRONMENT".



NAME: N7663 X Value: 71 Y Value: 750 PORT NUMBER: 8004
0 Destination
NEIGHBOR: [N742, N6420]
SENDER
RECEIVER

NODE NAME: N742 X Value: 62 Y Value: 800 PORT NUMBER: 7870
Speed 0 Destination
NEIGHBOR: [N7663]
SENDER
RECEIVER

NODE NAME: N6420 X Value: 70 Y Value: 700 PORT NUMBER: 9022
Speed 0 Destination
NEIGHBOR: [N7663]
SENDER
RECEIVER

Fig 3: Node Formation phase

By this(Fig 3) we are creating multiple nodes in “VANET” In this phase it consists of an options like “START”, “BRAKE”, “GRAPH”, “ATTACKER”, “SIGNAL ANALYZE”, “GRAPH”. Depending upon the option the node will do the action.

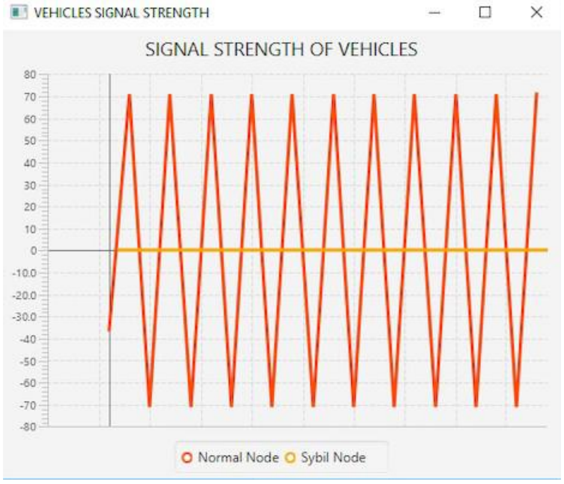


Fig 3: Vehicle Signal Strength

In this phase shown in Fig ,3 we can identify the signal strength of the vehicles and Sybil nodes by using the “GRAPH”. The normal node generates unique values while the Sybil node generates a constant value.

IX. CONCLUSION

In this paper, we have suggested a RSSI-based discovery strategy, Voiceprint, against Sybil assaults in VANETs. The thought behind the execution of the voiceprint is based on our perception that the RSSI time arrangement has fundamentally the same as examples among Sybil hubs and noxious aggressor hub. Voiceprint does not rely upon any radio spread model that makes it generally reasonable for different conditions (show free, broadly appropriate). In addition to that Voiceprint does not require the help of the unified hubs. The recreation and test results represent the adequacy of Voiceprint. In future work, we are planning to consider the Service Channel (SCH) into record. Since there is no strict confinement of reference point rate for SCH, we can expand the signal rate and communicate the examples from SCH a lot speedier. Secondly, Voiceprint can't distinguish the vindictive hub on the off chance that it receives control. We will lead all the more genuine tests to remove different highlights or other quantifiable parameters to counteract keen assaults with power control.

REFERENCES

1. M. S. Devi and K. Malar, "Improved Performance Modeling of Intelligent Safety Message Broadcast in Vanet: A Survey," *2014 International Conference on Intelligent Computing Applications*, Coimbatore, 2014, pp. 95-98.
2. H. Kaur, M. Devgan and P. Singh, "Sybil attackin VANET," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 3201-3204..
3. M. S. Al-kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," *2012 6th International Conference on Signal Processing and Communication Systems*, Gold Coast, QLD, 2012, pp. 1-9.
4. R. Lakhanpal and S. Sharma, "Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique," *2016 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*, Chennai, 2016, pp. 283-287.
5. C. Kumar Karn and C. Prakash Gupta, “A Survey on VANETs SecurityAttacks and Sybil Attack Detection,” *International Journal of Sensors,Wireless Communications and Control*, vol. 6, no. 1, pp. 45–62, 2016.
6. M. Mulla and S. Sambare, "Efficient analysis of lightweight Sybil attack detection scheme in Mobile Ad hoc Networks," *2015 International Conference on Pervasive Computing (ICPC)*, Pune, 2015, pp. 1-6.
7. M. Raya, P. Papadimitratos, and J. p. Hubaux, “Securing Vehicular Communications,” *IEEE Wireless Communications*, vol. 13, no. 5, pp.8–15, 2006.
8. D. S. Reddy, V. Bapuji, A. Govardhan and S. S. V. N. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, Chennai, 2017, pp. 1-5
9. S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: Detecting Sybil Attacks in Urban Vehicular Networks,” *IEEE Transactions onNParallel and Distributed Networks*, vol. 23, no. 6, pp. 1103–1114, 2012.
10. Q. Li, H. Li, Z. Wen and P. Yuan, "Research on the P2P Sybil attack and the detection mechanism," *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, 2017, pp. 668-671..
11. R. Mishra, A. Singh and R. Kumar, "VANET security: Issues, challenges and solutions," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 1050-1055.
12. H. Rasheed and O. Heekuck, “On Secure and Privacy-Aware SybilAttack Detection in Vehicular Communications,” *Wireless PersonalCommunications*, vol. 77, no. 4, pp. 2649–2673, 2014.
13. Bin Zeng and Benyue Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless sensor network," *2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*, Chengdu, 2010, pp. 357-360.
14. Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang and X. Zhou, "Power Control Identification: A Novel Sybil Attack Detection Scheme in VANETs using RSSI," in *IEEE Journal on Selected Areas in Communications*.
15. M. Li *et al*., "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs," *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, 2013, pp. 285-291.
16. M. Li *et al*., "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs," *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, 2013, pp. 285-291.
17. Y. Yao *et al*., "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI," in *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362-375, 1 Feb. 2019. doi: 10.1109/TMC.2018.2833849
18. U. Sabeel, N. Chandra and S. Dagadi, "A Novel Scheme for Multiple Spoof Attack Detection and Localization on WSN-based Home Security System," *2013 5th International Conference and Computational Intelligence and Communication Networks*, Mathura, 2013, pp. 360-367.
19. L. Zhang, H. Yang, Y. Yu and F. Peng, "A Three-Dimensional Node Security Localization Method for WSN Based on Improved RSSI-LSSVR Algorithm," *2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, Changsha, 2018, pp. 182-186.
20. M. T. Garip, P. H. Kim, P. Reiher and M. Gerla, "INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2017, pp. 1-6.
21. Y. Yao *et al*., "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Denver, CO, 2017, pp. 591-602.

22. S.C.Mana,"A Feature Based Comparison Study of Big Data Scheduling Algorithms", 2018 *International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai 2018, PP1-3*, doi:10.1109/ICCCSP.2018.8452837
23. Suja Cherukullapurath Mana, B.Keerthi Samhitha, Jithina Jose, Mydam Venkata Sawroop, Palagiri Chaitanya Kumar Reddy, "Traffic Violation Detection using Principal Component Analysis and Viola Jones Algorithms" *International Journal of Recent Technology and Engineering (IJRTE) ISSN:2277-3878,* Volume-8 Issue-3, September 2019
24. R.Surendran, B.Keerrthi Samhitha, "Energy Aware Grid Resource Allocation by Using a Novel Negotiation Model", *Journal of theoretical and Applied Information Technology, 2014, ISSN:1992-8645,* E ISSN: 1817-3195, Vol-68 No-3.
25. Jithina Jose, Suja Cherukullapurath Mana, B Keerthi Samhitha, "An Efficient System to Predict and Analyze Stock Data using Hadoop Techniques" *International Journal of Recent Technology and Engineering (IJRTE) ISSN:2277-3878*, Volume-8 Issue-2, July 2019
26. A.Brodsky, Suja Cherukullapurath Mana, Mahmoud Awad and N. Egge, "A Decision guided advisor to maximize ROI in Local Generation and Utility contracts, "*ISGT 2011, Anaheim, CA, 2011, pp. 1-7, doi:10.1109/ISGT.2011.5759185*

AUTHORS PROFILE

Ms. Keerthi Samhitha is working as an Assistant Professor at Sathyabama Institute of Science and Technology. Her research interests are in the field of Machine Learning, Deep Learning, Iot, Wireless Sensor Networks, Image processing, Big Data.

Ms. Suja Cherukulapurath Mana is working as an Assistant Professor at Sathyabama Institute of Science and Technology. Her research interests are in the field of Data science, Big data, Iot, Machine Learning.

Ms. Jithina Jose is working as an Assistant Professor in Sathyabama Institute of Science and Technology. Her research interests are in the field of Big data, wireless sensor networks, machine learning

Mr. Mohith is an undergraduate student in School computing at Sathyabama Institute of Science and Technology

Mr. Siva Chandrahasa Reddy is an undergraduate student in School of computing at Sathyabama Institute of Science and Technology