Signal and Time Based Fuzzy Cluster Scheme to Detect Sybil Attack in VANET

Shivangi Nigam
Department of Computer Application
Shri Ramswaroop Memorial University Deva Road,
Lucknow, India
shivi.nigam15@gmail.com

Abhishek Bajpai
Department of Computer Application
Shri Ramswaroop Memorial University Deva Road,
Lucknow, India
abhishek.srmu@gmail.com

Neeraj Kumar
Department of Computer Application
Shri Ramswaroop Memorial University Deva Road,
Lucknow, India
Corresponding Author: neeraj.cs@srmu.ac.in

***Abstract*: Security is an important issue in the VANET environment and the Sybil attack affects it the most. In Sybil attack a node illegally claims itself as a legitimate node using multiple identities. This paper systematically analyses about Sybil attack and its effect in the VANET. We establish a Signal and Time clustering (STC) algorithm to detect the Sybil attack in VANET. The scheme provides a low complexity and low overhead solution which can be more efficient in a VANET environment.**

***Keywords*-** Smart Transportation System (STS); On-Board Unit (OBU);, Road Side Unit (RSU), Dedicated Short Range Communication (DSRC)

I. INTRODUCTION

Vehicular Ad-hoc network is a wireless network which is an annex of Mobile Ad-hoc network (MANET). A mobile ad-hoc network is based on IEEE802.11 standards for communication between mobile devices connected wirelessly. The VANET is a smart technology which aids road transportation system with communication mediums. The VANET require roadside units with capability to gather information from the vehicles and send it further to the central authorities. In VANET the main challenging issue is to construct reliable and continuous communication between the vehicles in motion. To overcome from this situation VANET uses IEEE802.11p routing protocol for low latency communication called Wireless access in Vehicular Environment WAVE [1]. The WAVE works to provide communication protocols at Physical(PHY) and Medium access Control (MAC) layers, using CSMA/CD access scheme with the Dedicated Short Range Communication (DSRC) of 5.850 to 5.925 GHz or 75 MHz allocated for VANET [2,3]. The architecture of VANET comprises of two types of devices namely On-Board Unit (OBU) and Road-Side Unit (RSU) conversing either OBU and OBU or OBU and RSU (Figure 1.). The vehicles on road are the OBU and these OBU communicate the vehicle status to the RSU. The RSU collect information and is further useful for smart transportation system (STS) to aid Road safety, Vehicle collision warning, Security distance warning, Driver assistance, Cooperative driving, Cooperative cruise control, Dissemination of road information, Internet access, Map location, Automatic parking, Passenger convenience, automated highway applications etc. These boons of VANET are exposed to the threats of an open wireless network affecting the security of the system. Many security threats have been explored under various researches. Some of the attacks which can possible to occur in VANET are list below:

- Bogus information: in this attack the attacker can inject wrong information in the network to affect the behaviour of the other node in the network. Cheating with sensor information: This type of attack is generally done by insider node in which the attacker attack on the roadside unit and change the previous information such as previous position, speed and direction in case of any mishap done by it.
- ID disclosure: this is a passive attack in which the attacker monitors trajectories of a target vehicle for determining the ID of a vehicle.
- Denial of service: in this attack the aim of the attacker is to bring down the performance of the network by sending the various requests at a time.

Sybil attack is the replication of the identities nodes in the network. In this, the attacker wants to achieve the integrity of data, security and resource utilization. It can be performed to halt the activities like distributed storage, routing mechanisms, data aggregation, voting, fair resource allocation and misbehavior detection. The Sybil attack is the salient threat which occurs in VANET. This paper discusses a clustering scheme based on signal soundness and Time of the data as provided by the vehicles to the roadside units.

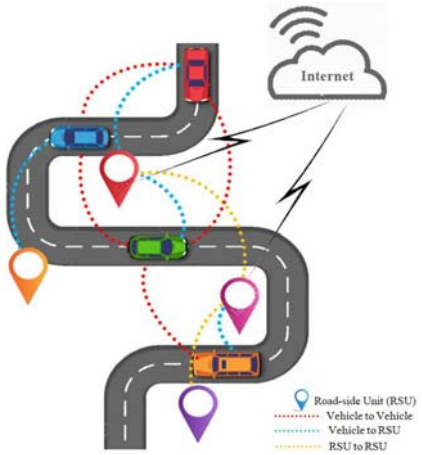

Figure 1. Architecture of VANET

II. SYBIL ATTACK

Sybil attack mutilates the functioning of VANET. The Sybil attacker gets access to the legitimate nodes and then impairing the functionality of the VANET. It sends the wrong or error messages with multiple identities to other nodes to simulate several nodes in the network area. Once the attacker get the accessibility to the legitimate node then attacker can use it in any way. It may also disrupt, forwarding the warning message process to the other vehicles which may put life of passenger in danger. This can be best explained using this example. Let us assume a scenario of accident on a highway which is occur couple of second. Now at that instant of time the first vehicle which is passing from that accident prone region, observe that the accident is occur and for safety reason start sending change the route warning message to all vehicle in that region. If suppose that one Sybil vehicle receive or get this information by any means and will not forward this message to other vehicle, so in this case it will cause the traffic problem or may lead to casualty too. Sybil attack in VANET system can be categorized into three parts:

- Communication: In VANET two way communications is held by Sybil attacker, either direct or indirect. When all Sybil nodes tries to communicate with the legitimate nodes in the network, created by Sybil attacker this is generally called direct communication.
- In contrast when the legitimate nodes enter itself in the area where the possibility of having Sybil nodes and by default communication occurs between them then this is generally called indirect communication. For example: When a message send by a Sybil nodes to the honest node in this case the message is actually send by the Sybil attacker this is called direct communication The attacker replicates identities in the network to random 32-bit integer identity as a fake identity.
- Participation: In Sybil attack participation of attacker nodes can be randomly or one by one which is basically depend on the current situation. A particular identity may leave or join the network many times and the number of identities uses is equal to or less then the number of physical identities.

A. Sybil Attack In VANET

VANET follow the various routing protocol and the most vulnerable routing protocol in which Sybil attack can occur are multi-path routing protocol, geographic routing protocol and cluster-based routing protocol [9]. In multi-path routing, the Sybil attacker attack on the disjoint node to halt the further communication between the nodes. In geographic routing the Sybil attacker can get the access in the network system with this can appear at more than one place at a time in the network. In cluster based routing the Sybil attacker disrupts the head section mechanism in the cluster which may affect the whole network system.

B. Detection Of Sybil Attack

Radio resource testing method: in this method a message is send by each node to its neighboring node with the help of radio signal and then a node randomly selects the node in the network for response [10]. In case the selected node is Sybil node then response will not generated by the node so Sybil node can be detected.

However this mechanism is not fully feasible because in VANET any node can leave the network area at any time and legitimating each node in this short period is not possible.

C. Prevention Of Sybil Attack

It is not possible to totally deny the probability of occurring Sybil attack in VANET but detection and prevention is possible through which it can be reduce to larger extent. The best and possible way to protect the network from Sybil attack is to establish the trust in between the nodes [11]. The trust establishment can be done in following ways:

1. *Digital signature and certificate-based system:* In this technique each message is send to the receiver node/vehicle in encrypted form with digital signature and certificate for authentication and integrity purpose. The receiver node/vehicle receives the message and decrypts it using the private key which is only known by the receiver.

2. *Hierarchy based system*: In this technique the nodes/vehicle in the network are grouped in the different group making the hierarchical form for message passing. Each group in the network has a group admin which provide authentication to the other nodes in the group. The message is passed to all groups with the help of roadside unit and each group admin having the private key to encrypt the message, this message is further send by the group admin to the other nodes/vehicles. In this system the roadside units have to communicate only with group admin which decrease burden of maintaining the database of each and every nodes in the network and also decrease the possibility of Sybil attack.

3. *Rating based system*: In this technique each node/vehicle keeps track of behaviour in the network of it neighbor node/vehicle by observing its routing protocol [12] and rate the node/vehicle based on the consistency in behaviour. In case any node got the negative rating then that node is marked as malicious node and discarded from the network for being sending and receiving message. This technique is difficult to implement because it generate more overhead of database storage.

III. LITERATURE REVIEW

The research studies on VANET's vary from the detection schemes to the prevention schemes. The Detection schemes have been more popular in research. The detection scheme of Sybil attack in VANET by Mortazavi et al. [4] proposes the use of hash function to produce pseudonymph as false names for the authentic users by a Certification Authority. These pseudonymphs are then grouped and a hash function is applied with an excommunicated secret key. This scheme results in considerable reduction in communication time and computations to differentiate the legitimate and illegitimate users. In the research study by Rahbari et. al. [9] proposes a cryptographic solution for the detection of Sybil attackers. The research proves the solution to provide security in four aspects as Authentication, Non-repudiation, Privacy, and Data Integrity. The encryption key cryptography is used to serve the users with public key and authentication in ensured by signature verification. The data integrity is maintained by the use of private keys kept secret by the certification authorities unknown to the RSUs. The drawbacks of the approach involves scalability of nodes which rejoins a new network, there may be some problems in detection which needs to be improved [4]. Yan et. al. [5] proposes a trust based security solution to the VANET. The radar is used to communicate the information of other vehicles. The cosine similarity is used to authenticate the legitimacy of the information communicated. The values found above the threshold limits are accepted and below are rejected and thus providing security from the inauthentic data. The research study by Xiao et. al [6]. deals with all security aspects regarding Sybil attack. The Detection scheme is mainly concerned with position verification. Demirbas et. al. [7] contributes to the detection of Sybil attack by proposing a signal strength indicator to identify the Sybil attacker. The signal strength indicator is the information about the transmission power of the vehicle in WSN. In conjunction with the Sender-Id, the signal strength indicator is checked and in case of any match to the previous indications indicates a Sybil attack. Rahbari et al. [9] proposes a cryptographic solution to the detection of Sybil attacks and deals with various security parameters as Authentication, Non-repudiation, privacy and data Integrity. The communication messages to the RSU and vehicles include authentication key and encryption key for signing a message to other vehicle and to RSU. The signature verification used to authenticate the sending vehicle. The receiving units request the CA for private key of the sender which verifies the sender and also detects the Sybil attack if any. The simulation uses HMAC function to generate message digest which is used for message communication. This approach observes lesser delay than encryption with the disadvantage of poor detection if node rejoins other. The vehicles travelling as a bunch is a Platoon and the dissemination of vehicles in traffic is Platoon Dispersion which can be useful to detect the Sybil attack is researched by Mutaz et al. [10]. The mathematical models of platoon dispersal assume that there is a probability distribution of the travel patterns of the vehicles. Any abnormal platooning is then used to detect the Sybil attacker. The study considers the nodes in current communication with RSU as a platoon. The mean and standard deviations of vehicle travel times is maintained by each RSU and consequently the confidence interval of Sybil detection is computed by probability distribution function. The change in the upstream and downstream platoon is used to detect the Sybil node.

Pouyan et al. [11] scrutinize the various detection schemes proposed for Sybil attack in VANET and present the pros and cons of these schemes. The schemes explored are categorized as resource testing, vehicle verification and encryption/decryption. Similar study is done by Levine et al. [15] where various techniques are categorized under eleven distinct categories. Majority of the research propose certification based solution extending Douceur's approach. The principal categories include Resource Testing, Recurring cost and fees etc. The propagation model for security from Sybil attack is as significant as the detection scheme. The research study by Guetta et al. [12] considers the transmission signal tuning and antenna reception to account for a successful model to detect a Sybil attack. An identity-less scheme may be useful in VANET for maintaining security of vehicles from Sybil attack. The research by Hussain et al. [13] uses pseudonym-less scheme in which the vehicles communicate via token conveyed by RSU to every registered vehicle. The tokens are used by vehicles to report any event to the corresponding RSU. A Tamper Resistance Model is proposed to perform analysis on the data assembled before any event is reported. This saves the system from Sybil attacks by analyzing the patterns and thus preventing scheduled beacons. The existing approach for Sybil detection has extra computational, hardware or software requirements. This research provides a better solution for saving the extra requirements of the Sybil detection system in VANET.

IV. PROPOSED SOLUTION

This research proposes the Sybil detection solution which is free from the overhead of sharing keys and other complexities to ensure the authenticity of the mobile nodes. A scheme named Signal strength and Time (STC) based Clustering technique which is useful to detect the Sybil attack in VANET. The signals of the mobile units are used as one of the parameter for Sybil node detection. The Location of the nodes is also used as another parameter of the identity messages being sent to the RSUs. The series of these messages is further studied for any dispersion. The proposed solution works on studying the dispersion of vehicles based on these time and signal series messages. The clustering techniques are used to examine the outliers of the clusters formed in the traffic. The basic principle behind is that if the mobile node is a Sybil node then it will try to fake multiple identities. These identities are saved as identity messages on each RSU. The clustering technique will determine the node with abnormal behaviour. A probability function determines the probability of the dubious node to be in the threshold limits of being a Sybil node or not. The proposed idea is implemented and the simulation results show that the approach is positive and provides better results than the other key based solutions.

A. Proposed STC Model

The STC Model uses clustering technique that exploits the time and signal data which are saved by the RSU as a data set. Clustering helps to identify the similar data sets which follow some homogeneity. The homogeneity is defined as a mathematical structure which the clustering algorithms follow to distinguish various clusters. The clustering scheme is an unsupervised learning scheme which probes the data continuously. The STC model employs Fuzzy Clustering to determine the clusters of the datasets as received by RSU. The cluster thresholds allow data items to float among clusters in the fuzzy clustering. Each RSU implements the clustering and by probabilistic partitioning of these datasets in same cluster are further exploited to identify the Sybil attacking node. The RSU maintains Time procession and Signal soundness of the mobile units in the form of matrix. The time procession is the set of time units at which each node sends messages. The Signal Soundness is the magnitude of the signals received by RSU for each incoming messages. This data set can be represented in the equations 1a, 1b:

Time Procession for single mobile unit:

$$T_k = [t_{1k}, t_{2k}, \dots \dots t_{nk}] \quad \text{(1a)}$$

Signal soundness for single mobile unit:

$$S_k = [s_{1k}, s_{2k}, \dots \dots s_{nk}] \quad \text{... (1b)}$$

The matrix of the above data set is retained by RSU for the two criterions as 2a, 2b.

$$T = \begin{vmatrix} t_{11} t_{12}, .., t_{1k} \\ t_{21} t_{22}, .., t_{2k} \\ , \dots \dots \dots \dots \dots .., \\ t_{n1} t_{n2}, .., t_{nk} \end{vmatrix} \quad \text{(2a)}$$

$$S = \begin{vmatrix} s_{11} s_{12}, .., s_{1k} \\ s_{21} s_{22}, .., s_{2k} \\ , \dots \dots \dots \dots \dots .., \\ s_{n1} s_{n2}, .., s_{nk} \end{vmatrix} \quad \text{(2b)}$$

The clustering scheme is objected to produce clusters out of the dataset Z_k.

$$Z_k = \langle T, S \rangle \quad (3)$$

where Z_k can be defined as dataset of two datasets T and S.

$$\{C_i | 1 \leq i \leq c\} \in Z \quad (4)$$

The clusters C_i belong to the dataset Z having c clusters. The fuzzy clustering permits redundancy across clusters. The data items of Z can be in more than 1 cluster. Thus the partition function P for Z can be defined as:

$$P = [\rho_{ik}]_{c \times N} \quad (5a)$$

In generalized fuzzy clustering the partition function is free from constraint on ρ_{ik} where the membership of all z in Z_k sums up to 1.

$$0 < \sum_{i=1}^{c} \rho_{ik} < N \quad .(5b)$$

$$\text{where} \quad 1 \leq i \leq c, 1 \leq k \leq N \ \ \rho_{ik} \in [0,1]$$

The objective function for clustering dataset Z_k into c clusters by the partition function $\prod_{i=1}^{m}(\rho_{ik})$ for N vehicles is given as:

$$J(Z|P,V) = \sum_{i=1}^{c} \sum_{k=1}^{N} (\rho_{ik})^m \|Z_k - V_i\|^2{}_C \quad (6a)$$

Where, P is the fuzzy partition matrix for Z_k, V is the vector of centroids of cluster formed by partitioning the dataset Z_k and m is a constant defining the fuzziness of the clusters.

$$V = [v_1, v_2, \ldots., v_c] \quad (6b)$$

RESULT AND ANALYSIS

The STC model has moderate time and space complexities in comparison to the various cryptographic solutions which become complex for a dynamic locale. The space requirements by the algorithm are minimum as it requires only storage for the Signal and time related data and the centroids of the clusters of these data points which contrast with the cryptographic approaches as they necessitate more space to accommodate the key computations and storage. The Time for computation of centroids and thus the analysis of the clusters is a linear function of number of data points and the attributes i.e. signal and time as considered by STC model. This model thus provides linear convergence of data points for a wide range of variation in data points.

V. CONCLUSION

The STC model utilizes the fuzzy clustering to identify the outliers with the help of probabilistic partitioning. This algorithm does all the computations on the data given to RSU by the mobile units communicating through messages. This reduces the overhead of previously used cryptographic solutions as they had extra complexity of key communication and computation. The algorithm proposes membership function based on Signal soundness and time of communication of the messages to determine the clusters and then extract the outliers through objective function minimization.

VI. ACKNOWLEDGEMENT

We acknowledge the Uttar Pradesh Council of Science and Technology, Lucknow (India) for providing the research grant.

REFERENCES

[1] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "Performance Analysis of 802.11 and 802. 11p in Cluster Based Simple Highway Model." International Journal of Computer Science and Information Technologies 1.5 (2010): 420-426.

[2] Su, Hang, and Xi Zhang. "Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks." IEEE Transactions on Vehicular Technology 56, no. 6 (2007): 3309-3323.

[3] Ho, Kai-Yun, Po-Chung Kang, Chung-Hsien Hsu, and Ching-Hai Lin. "Implementation of WAVE/DSRC devices for vehicular communications." In Computer Communication Control and Automation (3CA), 2010 International Symposium on, vol. 2. 2010.

[4] Douceur, John R. "The sybil attack." International Workshop on Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002.

[5] Mortazavi, Reza, and Maryam Rahbari. "Distributed sybil attack detection in vanet." International Journal of Computer Applications 29.12 (2011): 25-27.

[6] Rahbari, Mina, and Mohammad Ali Jabreil Jamali. "Efficient detection of sybil attack based on cryptography in VANET." International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[7] Manjunatha, T., M. Sushma, and K. Shivakumar. "Security Concepts and Sybil Attack Detection in Wireless Sensor Networks." International Journal of Emerging Trends and Technology in Computer Sciences vol 2 no. 3 ,2013.

[8] Yan, Gongjun, Stephan Olariu, and Michele C. Weigle. "Providing VANET security through active position detection." Computer Communications 31.12 (2008): 2883-2897.

[9] Xiao, Bin, Bo Yu, and Chuanshan Gao. "Detection and localization of sybil nodes in VANETs." Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks. ACM, 2006.

[10] Demirbas, Murat, and Youngwhan Song. "An RSSI-based scheme for sybil attack detection in wireless sensor networks." Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks. IEEE Computer Society, 2006.

[11] Grover, Jyoti, Manoj Singh Gaur, Vijay Laxmi, and Nitesh Kumar Prajapati. "A Sybil attack detection approach using neighbouring vehicles in VANET." In Proceedings of the 4th international conference on Security of information and networks, pp. 151-158. ACM, 2011.

[12] Rahbari, Mina, and Mohammad Ali Jabreil Jamali. "Efficient detection of Sybil attack based on cryptography in VANET." International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[13] Al-Mutaz, Muhammad, Levi Malott, and Sriram Chellappan. "Detecting Sybil attacks in vehicular networks." Journal of Trust Management 1.1 (2014): 1-19.

[14] Pouyan, Ali Akbar, and Mahdiyeh Alimohammadi. "Sybil Attack Detection in Vehicular Networks." Computer Science and Information Technology 2, no. 4 (2014): 197-202.

[15] Guette, Gilles, and Bertrand Ducourthial. "On the Sybil attack detection in VANET." 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems. IEEE, 2007.

[16] Hussain, Rasheed, Heekuck Oh, and Sangjin Kim. "AntiSybil: standing against Sybil attacks in privacy-preserved VANET." 2012 International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2012.

[17] Erritali, Mohammed, and Bouabid El Ouahidi. "A review and classification of various VANET Intrusion Detection Systems." Security Days (JNS3), 2013 National. IEEE, 2013.

[18] Margolin, N. Boris, and Brian Neil Levine. "Quantifying resistance to the Sybil attack." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2008.

[19] Dinger, Jochen, and Hannes Hartenstein. "Defending the Sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration." First International Conference on Availability, Reliability and Security (ARES'06). IEEE, 2006.

[20] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the Sybil attack." University of Massachusetts Amherst, Amherst, MA 7 (2006).

[21] Zhu, Wen Tao, et al. "Detecting node replication attacks in wireless sensor networks: a survey." Journal of Network and Computer Applications 35.3 (2012): 1022-1034.

[22] Liu, Yu, Cristina Comaniciu, and Hong Man. "A Bayesian game approach for intrusion detection in wireless ad hoc networks." Proceeding from the 2006 workshop on Game theory for communications and networks. ACM, 2006.

[23] Banković, Zorana, José M. Moya, Álvaro Araujo, David Fraga, Juan Carlos Vallejo, and Juan-Mariano de Goyeneche. "Distributed intrusion detection system for wireless sensor networks based on a reputation system coupled with kernel self-organizing maps." Integrated Computer-Aided Engineering 17, no. 2 (2010): 87-102.

[24] Yang, Qiuwei, et al. "Survey of security technologies on wireless sensor networks." Journal of Sensors 2015 (2015) Volume 2015, pp 1-9.

[25] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks." Journal of Computer Security 15.1 (2007): 39-68.

[26] Ho, Kai-Yun, Po-Chung Kang, Chung-Hsien Hsu, and Ching-Hai Lin. "Implementation of WAVE/DSRC devices for vehicular communications." In Computer Communication Control and Automation (3CA), 2010 International Symposium on, vol. 2. 2010.

[27] Demirbas, Murat, and Youngwhan Song. "An RSSI-based scheme for Sybil attack detection in wireless sensor networks." Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks. IEEE Computer Society, 2006.

[28] Dutta, Neelanjana, and Sriram Chellappan. "A time-series clustering approach for Sybil attack detection in vehicular ad hoc networks." Int. Conf. Adv. Veh. Syst., Technol. Appl. 2013.

[29] Aliahmadipour, Laya, Vicenç Torra, and Esfandiar Eslami. "On Hesitant Fuzzy Clustering and Clustering of Hesitant Fuzzy Data." Fuzzy Sets, Rough Sets, Multisets and Clustering. Springer International Publishing, 2017. 157-168.

AUTHORS PROFILE

Shivangi Nigam received her Masters in Computer Science & Engineering from National Institute of Technology, Hamirpur, India and the Bachelor of Technology (First Class) in Computer Science from India. She is currently an Assistant Professor of Computer Networks at the Department of Computer Application, Shri Ramswaroop Memorial University, Barabanki, India. Her research interests include Cloud Computing, Wireless Ad-hoc Networks. She is a member of various societies and has also reviewed researches for peer forum

Abhishek Bajpai received his Masters in Wireless Communication and Computing from Indian Institute of Information Technology, India and the Bachelor of Technology (First Class) in Information Technology from India. He is currently a Assistant Professor of Computer Networks at the Faculty of Computer Science and Engineering, Shri Ramswaroop Memorial University , Barabanki, India. Prior to joining SRMU, he was a Research Student at IIIT-A, Wireless Sensor Network Laboratory. His current research interests include Wireless Computing, Body Area Network. Mr. Bajpai has published many technical papers in major international journals and conferences of his fields. He serves as Review Member of several journals, including OJCST, IJAIEM. He is in member of Editorial Board of JACOTECH. He is a Member of ACM, Computer Society of India. He is serving as member, Technical Program committee NGCT.

Dr. Neeraj Kumar is an Associate Professor and founder Head of Department of Computer Application in Shri Ramswaroop Memorial University's. He received Doctoral degree in Information Technology from the BBAU (A Central University-NAAC 'A' Grade) Lucknow-India. He has received Accreditation Certificates from EACCME Italy (2012) and Switzerland (2013). His major areas of interest are Next Generation Mobile Communication, Green Communication, E-health, and ICT. He has been honored for VIRA Young Scientist Award (2016) at Chennai, India; Melvin Mayr International T. Award (2013) at Geneva, Switzerland; ISPAD's Official Greeter & Ambassador Award (2013) at Gothenburg, Sweden; CAEN-ISN Award (2010), Switzerland; WCN Best Paper Award (2010) at Rome, Italy. Dr. Neeraj has also been recommended more than 30 National and International fellowships & grants including academic visits Japan (2015 & 2014); Italy (2014); Canada (2014); Sweden (2013); Japan (2012); Italy (2012); USA (2011); Greece (2011); Italy (2010); USA (2010); S. Korea (2009); UPCST RA-Young Scientist Fellowship (2009-2012); USA (2008).