International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Device to Device Communication with Trusted Node Mapping in Cellular Network

Vivek Kumar Sinha[1], Kedarnath Singh[2]

[1]M. Tech Scholar, TIT College of Engineering & Technology, Bhopal-580 031, India

[2]Assistant Professor, TIT College of Engineering & Technology, Bhopal-580 031, India

Abstract: ***After the worldwide resolution of cellular technology, the communication protocols started Fifth Generation (5G) to come out. The previous generations of cellular technology have been a major transforming term that has covered all the backwards deficiency one by one. And 5G will need to be a major shift that includes very high carrier frequencies with massive bandwidths and extreme base station scalability. The outlook towards 5G is much higher as well as better in terms of capacity, bandwidth and throughput as compared with Fourth Generation (4G). But this technology also faces the major challenges like Device to Device (D2D) communication protocols, efficient energy schemes, pervasiveness and autonomous management [1]. In this paper, we propose a security framework to measure and evaluate trust model, trust propagation, and defend trust evaluation systems against malicious nodes. Our security technique is assessed by its ability to detect and isolate compromised nodes over the network. Simulation result indicates that our system effectively detects and prevents malicious nodes in cellular network.***

Keywords: 5G, D2D, Trust Node, LTE and Wi -Max.

1. Introduction

We observe that changes within the field of wireless technologies are increasing their standards rapidly. It can be declared as an accelerating evolution of wireless technology together with significantly growing on user demands and expectations. Previous generations of mobile computing and wireless technology establish the foundation for their upcoming future prospectus. Existing technologies go far beyond traditional telephony scheme and basic data services that were used by Second Generation (2G) scheme. The 5G of mobile networks is seen as an diagnostic technology ,i.e., one global unified standard that will allow completely seamless connectivity without barriers among both, existing standards and scheme, e.g. Long Term Evolution (LTE) and Wireless Fidelity (Wi-Fi),and new wireless systems that are about to emerge.

In the past eras of cell systems, D2D correspondence usefulness has not been considered yet. This is for the most part in light of the fact that it has primarily been imagined as a device to decrease the expense of nearby administration procurement, which used to be fragmentary in the past taking into account the cell administrators' business sector measurements. The administrators' disposition toward D2D usefulness has been changing as of late in light of a few patterns in the remote business sector plan [6].For example, the number of Context-aware services and applications is growing rapidly. These applications require location discovery and communication with neighboring devices, and the availability of such function will reduce the cost of communication. D2D services can also play a vital role in mobile computing and facilitate effective sharing of resources (spectrum, computational power, applications, social contents, etc.) for users.

Some recent works on D2D in cellular Network have reported results on interference management issues and radio resource allocation [4–6] as well as on communication session setup and Management procedures [8]. In this paper, we provide a categorization of D2D communication and also summarize some major challenges that need to be addressed. Specifically, we briefly discuss security, interference management, and resource allocation schemes, and point out some directions for Future research. In this paper, we propose a novel D2D communication mechanism that provides selection of trusted nodes for devices that are in rural area network.

2. D2D Communication

D2D communication in cellular networks can be defined as direct communication between two user end devices without going through the Base Station. In a conventional cellular network, all communications must traverse through the BS even if both communicating devices are in range of D2D communication scheme. This structure fits in the conventional low data rate services like voice calling and text messaging in which users are not usually close enough to have direct communication path. However, user devices in today's scenario use high data rate services (e.g., video sharing, gaming zone) i.e. 5G network in which they could potentially be in range for direct communication. Nevertheless, the advantages of D2D communications is not only limited to enhanced spectrum efficiency. In addition to improving spectrum efficiency, D2D communications can potentially improve throughput and delay time.

We can classify D2D communication in cellular networks based on the spectrum in which D2D communication occurs. Now we provide overview to merits and demerits of each D2D scheme.

In-band D2D: In-band D2D communication is usually the high control over cellular (i.e., licensed) network. Some scientists assume that the interference in the unlicensed spectrum is uncontrollable which imposes constraints for QoS provisioning. In-band communication can be

subdivided into underlay and overlay categories. In underlay D2D communication, cellular and D2D communications use the same radio stations. In the other side, D2D links in overlay communication are given dedicated cellular networks. In-band D2D can improve the efficiency of cellular networks by reusing spectrum network (i.e., underlay) or allocate dedicated cellular resources to D2D users that accommodates direct connection between two end devices. The key disadvantage of in-band D2D is the interference caused by D2D users to cellular communications and vice versa. This interference can be mitigated by introducing complex resource allocation scheme, which increase the computational overhead of the BS or D2D user devices.

Out-band D2D: The D2D correspondence connections abuse unlicensed spectrum. The inspiration driving utilizing out-bands D2D correspondence is to wipe out the impedance between end devices. Utilizing unlicensed spectrum requires an additional interface and typically receives remote innovations i.e. WiMax or LTE. Interestingly, propose to keep cell interchanges controlled and leave the D2D correspondences to the clients (i.e., self-ruling). Out-band D2D utilizes unlicensed spectrum which makes the impedance issue in the middle of D2D and cell devices superfluous. Then again, out-band D2D may experience the ill effects of the uncontrolled way of unlicensed spectrum. It ought to be noticed that just cell devices with two remote interfaces (e.g., LTE and WiMax) can use out-band D2D, and in this way clients can have concurrent D2D correspondence plan and cell system.

3. Problem Statement

We project a two-tier 5G cellular network with so-called macro cell and device tiers structure. The macro cell tier structure contains base station (BS)-to-device communications as in a traditional cellular network. The device tier involves D2D communication functionality. If a device connects itself in the cellular network through a BS, this device is must be operating in the macro cell tier structure. If a device connects directly with other device or obtain its transmission through the other devices, these devices must be in the device tier structure.

In macro and device tier structures, the BSs will usually serve the devices continuously. However, at cell edges or congested areas, cellular devices will be allowed to communicate with each other, by creating an ad hoc mesh network structure. In the context of device-tier communications, the operator might have different controlling levels. We can define the following four main types of device-tier communication structure.

a) Device relaying with operator controlled link establishment (DR-OC):
A devices at the edge of a cell or in a powerless scope range can correspond with the BS through transferring its data by means of different devices. This takes into account the devices to accomplish a higher QoS or more battery life. The administrator corresponds with the handing-off devices for halfway or full control join foundation.

b) Direct D2D communication with operator controlled link establishment (DC-OC):
The source and destination devices trade information with one another without the assistance of base stations, yet they are helped by the administrator for connection foundation.

c) Device relaying with device controlled link establishment (DR-DC)
The operator is not involved in the process of link establishment. Therefore, source and destination devices are responsible for coordinating communication using relays between each other.

d) Direct D2D communication with device controlled link establishment (DC-DC):
The end devices will have direct communication with each other without any operator control. Therefore, source and destination devices should use the resource in such a way as to ensure limited interference with other devices in the same tier and the macro cell tier. The design of two-tier cellular system can bring significant improvements over the classical cellular system architecture. This D2D functionality faces many technical challenges, particularly in security and an interference management issues must be resolved. Security must be a major issue that has to be addressed because the user data is routed through other end users' devices. The privacy must be maintained in other devices. One possible solution to ensure security is closed access for the devices that needs to communicate in the device tier structure.

In closed access technique, a device has a set of "trusted" devices, and devices on this list must use the device tier scheme to communicate with each other. For example, the users in a near workplace that acknowledge each other, or the users that have been authenticated via a third party, can directly communicate with each other, managing privacy level. The devices in a group can setup various encryption schemes between each other. In open access, each device acts as a relay for other devices without any restrictions or disturbance. Security issues in D2D functionality involve the process of identifying of potential attacks, threats, and vulnerability points. Some recent works on the security issues of machine-to- machine communication [7–9] can be addressed for open access D2D functionality. For example, the work done by Dong in Kim proposes a trusted environment to build up trust connections among M2M equipment [7], while secrecy-based access control is discussed in [8]. Our main objective relies on Security technique that is needed at the time of Communication through relay Devices. The major threats are:-

a) **Confidentiality**: The basic security service is to maintain the privacy of information transmitted between source and trusted nodes.
b) **Integrity**: The integrity property must maintain and guarantee that transmitted messages are not modified by the relaying device.

The Base station can take the edge of the problem of interference management to some extent using centralized methods. On the other hand, in DR-DC and DC-DC, there is no centralized entity to supervise the asset designation between devices. Working in the same licensed bandwidth, devices will inevitably impact macro cell users. To ensure

the performance of existing macro cell base stations with minimum impact, a two-tier network structure needs to be designed with smart interference management strategies and appropriate resource allocation schemes. Besides the interference between the macro cell and device tiers, there is also interference among users in the device tier. The major Drawbacks of Direct D2D communications with device controlled link establishment are given:

a. Why a Device will work as a Relay Device and it will recognize the trusted node.
b. Our main Problem Statement: The major problem of Security that comes while Communication through relay Devices.

Proposed Work

This paper we propose a system to quantitevely significant trust, model trust engendering process and secure. In Trust and Reputation (TR) framework, taking an interest nodes attempt to assess and anticipate the dependability and reliability of other element nodes by heuristic system. These frameworks are normally created closely resembling the stream outline portrayed in Figure 2. Nodes's own affair from connection with nodes is joined with learning of others and time data through a channel metric. The data from others is weighted by trust qualities and the impact of memorable data is diminished. After the channel metric estimation a neighborhood notoriety worth is accessible mirroring the dynamic data on how likely a nodes will carry on well concerning the channel metric. This worth may be extremely unpredictable speaking to different parts of dependability.

4.1 Node Discovery and Trust Initialization

1. To Create Trusted neighbor table with null entries
2. Periodically broadcast one-hop hello packets
3. If response is received
4. Check if node is in trust table
5. If node is not in trust table
6. {Authenticate node
7. If node is authentic
8. {Add node to trust table
9. Initialize node trust level to 0.5
10. }
11. Else blacklist node and set flag
12. }
13. Else discard packet
14. End of Initialization;

In the section 3 we have described the maintenance phase involving updating reputation, trust and confidence metrics according to the modeling parameters. Additionally, nodes periodically verify the location information of their one hop neighbor's nodes. This phase occurs at certain time interval after completing the node discovery, trust initialization phase and cluster formation period. During this phase the nodes monitor the network traffic to obtain their recent neighbors nodes. For each of these updates the corresponding trust and confidence metrics are also updated. Periodically the nodes execute the location verification algorithm, as explained in section, in order to verify the location information of their one hop neighbor. All networks employing such TR systems must provide security mechanism to ensure integrity and confidentially function. Some of the threats are shown for such systems:

- False Accusation: Nodes may also produce false reports or information resulting misbehaving of nodes. Hereby they can reduce the efficiency of trust rating of highly trusted peers.
- Collusion: Malicious nodes communicate with each other often and because of incensement in the influence and communication possibilities of all malicious nodes. In Addition, they can be better secure against low trust ratings from correctly behaving nodes and are able to harm individual other nodes.
- Identity Spoofing: Malicious nodes with a worst reputation index 'capture' the identity of a highly trusted nodes to preserve its high trust value or report and therefore receive better service delivery of other nodes. These attacks are TR system which inherently of a specific TR metric or interaction node selection algorithm. They are mainly produced due to a lack of authentication protocol and non-repudiation in guarantee the security features of cellular network system; the trustworthiness of participating entity nodes is a major concern.

4.2 Frame Work and Security Issues

To cope with the security issues, we introduce a framework maintaining security services such as authentication and non-repudiation for TR system. A key component of the framework is the combination of PKI infrastructure without any validation authority.

The identification of nodes is done using a public key *P*, which is part of the pair *P, S* generated by the node itself as it comes over the network. The public key is distributed over the network during first interactions of nodes. Furthermore, a node can generate not only one key pair but can also preserve multiple pairs reflecting multiple IDs. Using key pairs, a node can left and re-join the cellular network without losing its identification and is able to (re-)'authenticate' itself. If nodes had successful interaction with other entity nodes, they can rely on the nodes identity for further interaction which prevents malicious activities [4].

The proposed security framework is highlighted through a typical example as depicted in Figure 3. The user can request for service at any intent e.g. a file transfer, data forwarding etc. from the network (Step 1). The decentralized lookup operation (2), which is application specific, delivers nodes offering those services. This lookup is not always useful or required, e.g. in WMNs the nodes offering data forwarding do not change frequently. The framework is protecting the service requests and offering acknowledgements, so that malicious nodes are prevented from offering services in the name of other entity nodes. After finding a set of nodes, the requestor performs a lookup operation of trust values for nodes (3) corresponding to a given metric. This lookup is defined in syntax *{Si}{IDi, IDj,Ni,Metric, ...}* where *IDi*is the ID of the node *i* requesting trust on node *j* and *Ni* is a random generated number preventing replay attacks.

To the D2D communication we try to achieve faster service .Our overview of paper as follows. Section II we describe the descriptive technologies, section III define the problem in

DC-DC, section IV have proposed work to solve the problem, section V have trust frame work and security analysis to find trust node as relay for D2D communication, section VI have simulation and result with their simulation parameters and at last section VII have conclusion and future scope in D2D.

As development of wireless technologies has greatly improved people has ability to communicate, live in both business operations and social activities. The second generation (2G) mobile communication system had its origin in 1991 to the 3G system first launch in 2001, the wireless mobile network has malformed from a pure telephony system to a communication network that can bring rich multimedia stuffing. Nevertheless, there is still a vivid increase in the number of users who subscribe to mobile broadband systems every year. Fixed workstation relaying brings improvement in cellular systems, but the full potential of cooperation can be realized only through the implementation of *device relaying*. The *device* term here refers to a cell phone or even any supplementary portable wireless device with cellular operability (tablet, laptop, etc) a user owns. Device relaying makes it possible for end devices in cellular network to act as transmission relays for each other and realize a massive cellular network. This is possible with device-to-device (D2D) communication functionality, which allows two nearby devices to communicate with each other in the cellular bandwidth without a base station (BS) involved or with limited access of BS participation.

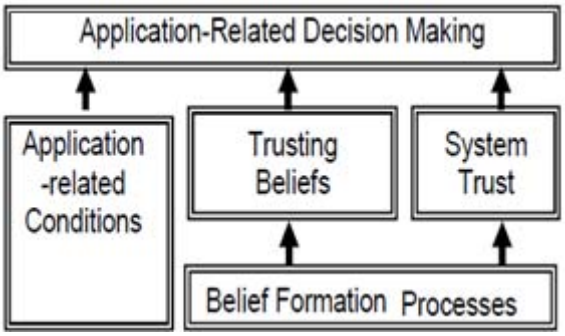

Figure 1: Trust and Reputation Framework

In WMN as example, the metric may be differentiated among trust in delivery, trust in QoS etc. According to the chosen metric a node is selected (4) for interaction and the service is requested in a non-repudiate way (signed). After completion or termination (5), the communication between nodes is inspected (6) and a new trust value is calculated (7). Finally trust points are updated based on the storage location and validity range of trust values which may call as view.

Direct encounter: Only a node's direct experience is taken as the basis for the trust value used for node selection. As a result, each node has its own, independent trust value for each other node.

Local View: The nodes include reputation information from the local neighborhood. In this view, neighboring nodes are more likely to have similar, but different, trust values for other nodes.

Global View: The trust value is determined and updated at certain centralized spots in the network. For example, In the Trust Me [6] protocol, Secure Bootstrapping Servers (SBS) are used to assign so-called Trust Holding Agents (THA) to joining nodes. An interaction report is filed to THA peers for compiling an overall trust value.

5. Result Analysis

In this proposed technique we observe that the mapping of authenticate node to work as trust node and make device to device (D2D) communication possible under the base limit of device to device pair more than 25m as well as less latency by sending authentication to neighbors. This method is more efficient useful when the number of mobile node(UE) is reaching under threshold level of interference for limiting D2D pair [20].Even though the 5G cellular communication dynamic relaying through trust node is identify by their trust factor while selecting device as trust node for relay. Once the device is used as relay its trust factor increases and same time updated by their neighbor table entry.

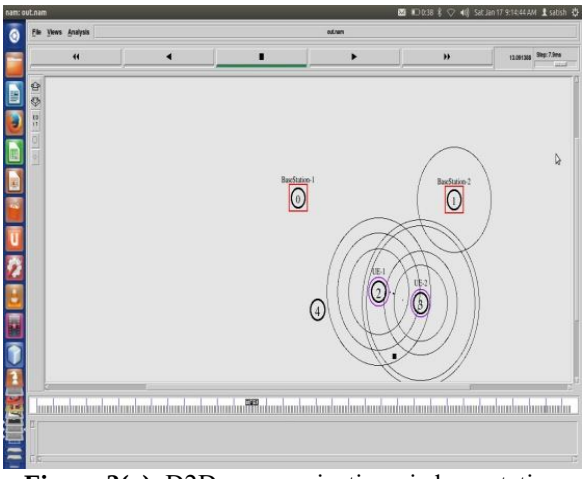

Figure 2(a): D2D communication via base station

Through the Figure 6 and 7 we can know that the initial communication is via Base Station we transfer packet and make communication but as we move out from the transmission range or crossing the threshold level we hand over to other BS. As we move on from other BS we make communication via BS-1-Bs-2.But when condition occur we passing data through D2D and crossing the Base limit of D2D (25 m) we need another node relay between D2D ,so we discover the trust node to perform D2D communication .Through this approach we neither save energy but reduce the overhead of BS.

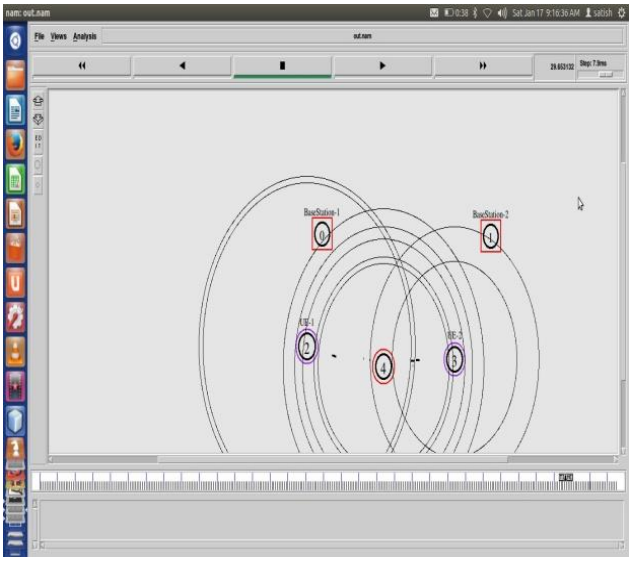

Figure 2 (b): D2D communication through Relay using Trust Node

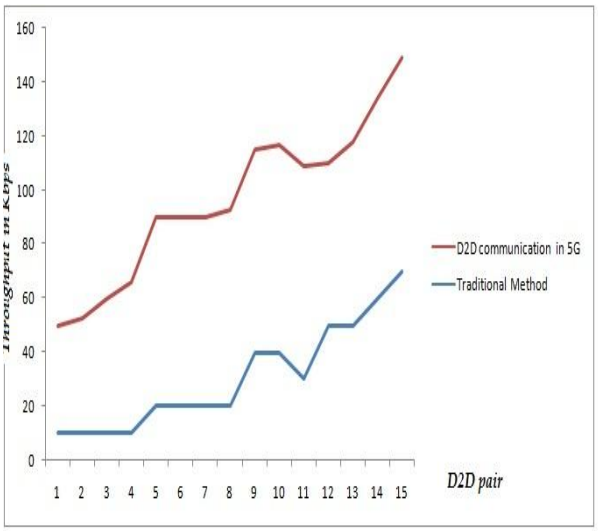

Figure 3:

Figure states that the D2D distance is maximum for simulation is 25m and Bandwidth is 10MHz using channel model of urban and TTI is 1ms for number of nodes per cell is 9, using transmission range of 450.As SINR value increases we compute with threshold if value is more than the threshold we take another node as relay in between D2D And perform communication for one hop relay to reduce the energy as well as reduce overhead of BS.

Table 1: Simulation Parameter

Parameter	*Value*
System Type	Single Cell
Simulation Time	150
Number of Nodes per cell	9
Packet size	512 Bytes
D2D Distance max.	25 m
Bandwidth	10MHz
Active Users in Cell	8
Topology Size	1100*600
Transmission Range	450
Transmission Time Interval (TTI)	1ms
Channel Model	Urban

6. Conclusion

We have reposed an aware trust based localized protocol that is able to detect and isolate compromised or malicious nodes over the network. Our security system is designed in the context of a relaying node based network model with nodes. We introduce a simple verification technique that validates reported location information. Our protocol is assessed by its ability to detect and isolate compromised nodes over the network. Simulations indicate that our system effectively detects and prevent compromised nodes even in the presence of colluding nodes.

References

[1] Mohsen Nader Tehrani, Murat Uysal, and HalimYanik omeroglu ."Communication in 5G Cellular Networks: Challenges, Solutions, and Future Directions" IEEE Communications Magazine • May 2014

[2] **Tao** Han, Rui Yin, YanfangXu and Guanding Yu Department of Information Science and Electronic Engineering Zhejiang Provincial Key Laboratory of Information Network technology Zhejiang University, Hangzhou 310027, P.R. China 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)-2012.

[3] S. Marti and H. Garcia-Molina. Taxonomy of trust: Categorizing p2p reputation systems. In Management in Peer-to-Peer Systems, volume 50, pages 472–484, March 2006.

[4] Gu, S. J. Bae, B.-G. Choi, and M. Y. Chung, "Dynamic Power Control Mechanism for Interference Coordination of Device-to-Device Communication in Cellular Networks," in Proc. of IEEE 3rd International Conference on Ubiquitous and Future Networks (ICUFN), Jun. 2011.

[5] DaquanFeng, Lu Lu, Yi Yuan-Wu, Geoffrey Ye Li, Gang Feng, and Shaoqian Li" Device-to-Device Communications Underlaying Cellular Networks" in IEEETRANSACTIONS ON COMMUNICATIONS, VOL. 61, NO. 8, AUGUST 2013.

[6] Yi yang Pei, Member, IEEE, and Ying-Chang Liang, Fellow, IEEE Resource Allocation for Device-to-Device Communications Overlaying Two-Way Cellular Networks in IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 7, JULY 2013.

[7] Xiao hang Chen, Li Chen, Mengxian, Zeng, Xin Zhang, and Dacheng Yang, Wireless Theories and Technologies (WT&T), Downlink Resource Allocation for Device-to-Device Communication Underlaying Cellular Networks in 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC).

[8] PhondPhunchongharn, Ekram Hossain, and Dong in Kim, "RESOURCE ALLOCATION of DEVICE-TO-DEVICE COMMUNICATIONS UNDERLAYING LTE-ADVANCED NETWORKS "in IEEE Wireless Communications • August 2013.

[9] Osman N. C. Yilmaz, Zexian Li, KimmoValkealahti, Mikko A. Uusitalo, MarttiMoisio, PetteriLundén, Carl Wijting "Smart Mobility Management for D2D

Communications in 5G Networks" in 978-1-4799-3086-9/14 in 2014 IEEE

[10] Youngjae Park and Sungwook Kim"Trust-based Incentive Cooperative Relay Routing Algorithm for Wireless Networks",AICT2014 : The Tenth Advanced International Conference on Telecommunications.

[11] Mrs. Chinchu .V. S1 , Ms. Meji Jose2 " Trust Based Secure Payment Scheme for Multi-hop WirelessNetworks",e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VI (Mar-Apr. 2014), PP 38-43.

[12] Tao Han, Rui Yin, Yanfang Xu and Guanding Yu "Uplink Channel Reusing Selection Optimization for Device-to- Device Communication UnderlayingCellular Networks", 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC),pp 42-45.

[13] Yan Lindsay Sun¤, Zhu Hany, Wei Yuy and K. J. Ray Liu ,"A Trust Evaluation Framework in DistributedNetworks: Vulnerability Analysis and DefenseAgainst Attacks",in Proceedings of MobiCom

Author Profile

Mr. Vivek Kumar Sinha received the B.E. in Computer Science engineering from MPCCET Bhilai in 2007 and PGDM (HR& Marketing) from RBS, Raipur in 2012 and Pursuing M.Tech. Degrees in Computer Science and Engineering from TIT & S, Bhopal. During 2008-2011 worked as an Assistant Professor in Computer Science in SRI-Tech, New Raipur.