



# Info Edge

Vol : 03, Issue: 01

A Half Yearly Newsletter

Febraury, 2021

## Vision of the Department

“To impart knowledge to young aspirants to develop Information Technology based solutions for the Industrial and Societal needs”

## Mission

- Prepare students to acquire knowledge in the field of Information Technology through effective teaching learning methodologies.
- Establish conducive environment for better learning through the state of the art curriculum to exhibit talents and ingenuity.
- Nurture the students to be industry ready by enhancing their employability skills and entrepreneurial skills
- Develop Information Technology based solution as per the need of Society.

## Program Specific Outcomes(PSOs)

- Able to apply appropriate techniques for storage of huge amount of data and ensuring its integrity.
- Choose appropriate method for data acquisition from real world and propose suitable solutions to solve problems.

## Editorial Board

### Chief Editor:

Mr. Prasanna kumar M, Assistant Professor

### Student Editors:

1. Gowamma S H, 3<sup>rd</sup> Year
2. Sachin S Naik, 3<sup>rd</sup> Year

## Department Activities

- “2nd International e-Conference on Computer Networks and Soft Computing (ICCNCS2020)” on 28th & 29th December 2020 jointly organized by department of CSE and ISE at Sri Siddhartha Institute of Technology, Tumkur.
- A webinar series “Machine Learning in Real life” is organized in the department for students on 21<sup>st</sup>, 28<sup>th</sup> November, 5<sup>th</sup> Decemeber, 2020. Resource persons are Mr Rajesh P Hegde, Co-Founder, Dblue Inc and Mr Ramjee Ganti, Co-Founder, Dblue Inc.
- A webinar on “SAP Basis and Hana” is organized for students on 18/12/2021. Resource persons are Mr. Abhishek Singhal, Senior SAP BASIS Consultant, SAP Labs, Bengaluru and Mrs. Subhashree Kanungo Senior SAP BASIS Consultant, SAP Labs, Bengaluru.



*Congratulations*



**Prof. Chethan B K** Completed PhD in VTU in December -2020 on the topic “Mobile Agents Security in Mobile Adhoc Networks” under the guidance of Dr. M Siddappa and Co-guide Dr. H S Jayanna.

## Department Activities

- Prof. Naveen Kumar A N has delivered a webinar on “Java @25” for students and staff on 17/11/2021.
- The department has organized a Rally of National Energy Conservation Week on 18/12/2020.
- Chinmaya Udupa, Student, 4th semester, presented a technical talk on “Cloud computing” under departmental student activity for 4th semester students.
- Rashmi H C presented the paper “Security considerations in energy efficient resource constrained device environment: A Survey” in the 2nd International e-Conference on Computer Networks and Soft Computing (ICCNCS2020) on 28th & 29th December 2020 jointly organized by department of CSE and ISE at Sri Siddhartha Institute of Technology, Tumkur.

## PUF Technology in IOT Security

Physically unclonable function, or PUF, is a device-level technology approach for data security that is being explored by more IC suppliers. Despite the precision of silicon manufacturing methods, this technology takes advantage of the fact that each circuit made contains minor differences. These minute variances are utilised by the PUF to create a unique digital value that can be used as a secret key. Digital security necessitates the use of secret keys.

Internet of things (IoT) devices are increasingly concerned about security, especially given the significant danger of hacker assaults, information compromises, and security breaches. It is feasible to avoid the limitations of traditional key storage with a good implementation of PUF.

Physical probing of the key will substantially alter the characteristics of the PUF circuit, resulting in a new number. The PUF key is only generated when it is required for a cryptographic operation, and it can be wiped at any time.

Artificial intelligence of things (AIoT) is a new trend in which artificial intelligence (AI) and the internet of things (IoT) are combined to create networks of digital devices that interact and process data. While the Internet of Things (IoT) builds huge networks, AI brings these gadgets to life. For instance, an IP camera system can be utilised to secure an apartment. However, without AI, individuals will have to watch live video from the system in order to respond to situations. IP cameras that use AI can detect threats and issue alerts automatically. In the same way that the internet spawned a slew of new high-value enterprises, AIoT is expected to grow quickly and produce new high-value products. Those that start making AIoT devices will be able to tap into a huge new market. The number of IoT devices on the market today is in the billions. Electronic devices and appliances that are networked together and communicate over internet protocols are included in these small, connected gadgets

Hardware security based on PUFs is the ideal answer. The present security-for-performance tradeoff is addressed with PUF. "Data and firmware assaults," "transmission attacks," and "data integrity attacks" are three types of AIoT attacks. Complex encryption and decryption are impracticable for the protection of AI assets. PUF has evolved into a reasonably simple and quick security solution.

**Mr. Prasanna Kumar M**  
**Assistant Professor, Dept of ISE.**

## Application of Machine Learning in Ad hoc Networks Routing

As wireless ad hoc networks do not have any predefined topology or structure, the communication links are built through nodes moving randomly with dynamic connectivity. The performance of the whole system depends on the efficiency of routing algorithm. That is why, it is more desirable that algorithms adapt to their network faults and congestion enabling the system to find alternative paths. In recent years, this way of adapting to environment by itself which is called machine learning (ML) has been a major focus and emerged as an essential field of research for wireless network routing. Nowadays wireless ad hoc networks are not only for emergency signaling or data transfer, but also for high throughput transmission like video streaming, gaming on the go. Hence while evolving the learning methods, different QoS parameters such as throughput, average end to end delay, packet delivery ratio, routing overhead etc. need to be considered the most.

Because of frequently changing topology and infrastructure-less environment, link failure is very common in ad hoc network scenarios. There are few more problems arise such as packet loss, high delay, lack of synchronization. Therefore, ML techniques are applied which makes the nodes automatically learn about the environment, and take proper action accordingly to quickly adapt to the system. By learning and reacting accurately, nodes can even make the best out of this challenging situation. Upon receiving the indication on current environment, a node takes an action which eventually changes the environment. This change returns another indication to the node in the form of reward or penalty. The goal is to maximize the number

of rewards as much as possible to exploit the network in an efficient way. Protocols designed with ML techniques are found to have less broken links, improved QoS, faster data transfer, and better tolerance to network changes. Protocols adapt machine learning feature to their algorithms so as to find the best path, improve the QoS, and support link break. In recent years, different machine learning methods have been the point of interest for researchers working on routing protocols. Some of the mostly used machine learning procedures is Reinforcement Learning, Q-Learning, Game Theory, Learning Automata and Swarm Intelligence.

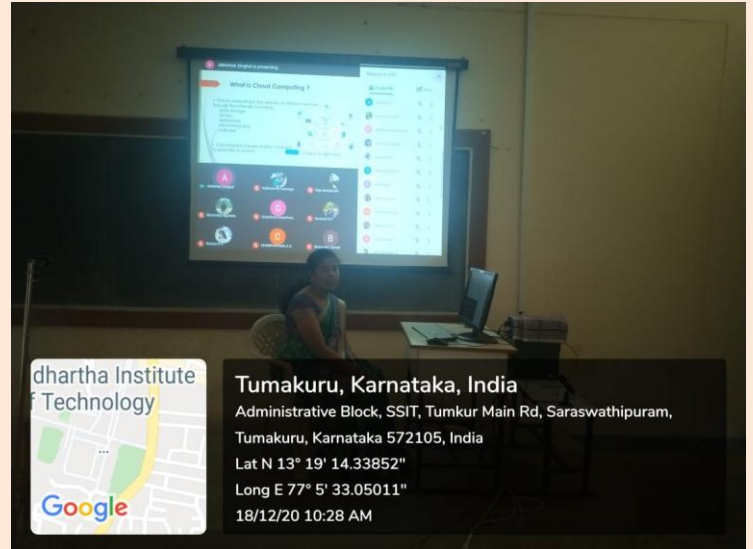
Reinforcement Learning has better optimization of throughput in MANET and WSN because of its flexibility to topology changes, easy implementation, and optimal results. Second learning method Q Learning can be employed in all three types of networks, but it usually finds better routing policy in WSNs. Non-cooperative Game Theory works well under both WSN and MANET networks, since each node individually tries to maximize its utility choosing own strategy. Cooperative Game Theory is used effectively in WSNs by forming coalition with neighbouring nodes and working as groups in the network. However it is difficult to implement Game Theory in VANET due to its dynamicity and short connection time. Learning Automata method fits better in MANETs as it is suitable for environment with high mobility rate and high number of nodes. In recent years, a large number of researchers have focused on machine learning of routing protocols in order to learn the environment changes and react to them automatically.

**Dr. Suma R**, Associate Professor, Dept. of ISE.

## Photo Gallery



Webinar Series on Machine Learning in Real life



Webinar on SAP Basis and Hana



2nd International e-Conference on Computer Networks and Soft Computing (ICCNCS2020)



Webinar on "JAVA @25"



Rally of National Energy Conservation Week