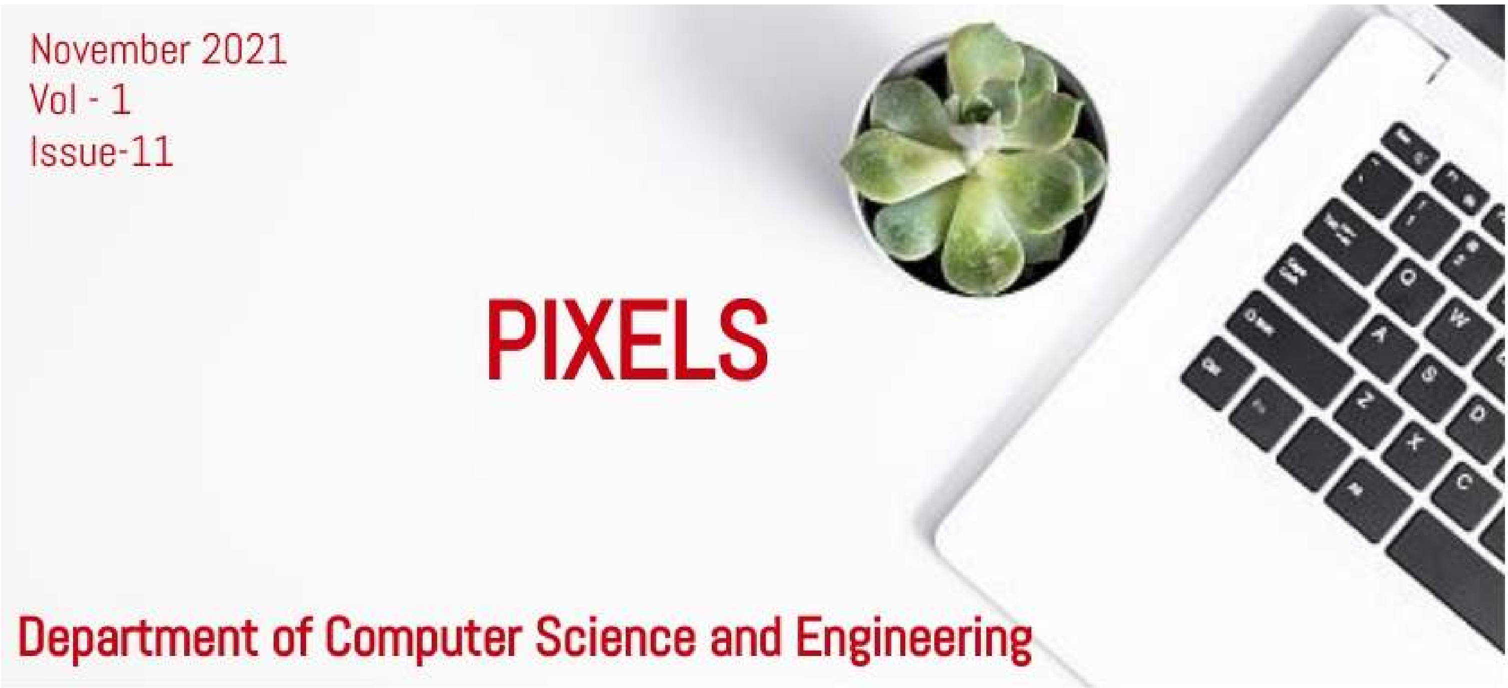


November 2021
Vol - 1
Issue-11

PIXELS

Department of Computer Science and Engineering

FINALIST @ REBOOT KERALA HACKATHON 2020

The certificate awarding ceremony for the team Data Pirate who is selected as the finalists in Reboot Kerala Hackathon 2020 organized by the Kerala State Higher Education Department and the Additional Skill Acquisition Programme on August 7th to 9th. The event aimed at finding solutions to the issues in the education sector, using the technical skills of students of higher education conducted by 36 hours of online hackathon. The Computer Science and Engineering Department held a certificate awarding ceremony at Nova Hall on 30/11/2021. Dr.M. Sivanandan, Chairman, SNGIST Group of Institutions inaugurated the session with his speech. Prof. K.S. Pradeep, Manager, Gurudeva Trust, Head of the Department Ms. Anju Raveendran, and the faculty of the computer science department congratulated the students.

INVITED TALK

SNGIST Group of Institutions
Department of
Computer Science and Engineering
INDUSTRY 4.0
Digital revolution in challenging times
Date - 19/11/2021, Friday
Time - 2 PM
Invited Talk
Invited Talk By
Prof. Dr. C. P. Sunil Kumar FIE
Academic Director
SNGIST Group of Institutions
SNGIST
GROUP OF INSTITUTIONS
99617 92220
99472 81122
0484 2887000
Manjaly P.O., Mannam, N. Paravur, Kochi - 683520 sngist@sngist.org www.sngist.org
An ISO 9001: 2015 Institution | Approved by AICTE, DTE | Affiliated to KTU/MGU

On 19 November 2021, the Department of CSE organized an Invited Talk as a part of industry-institute interaction on the topic " INDUSTRY 4.0 Digital revolution in challenging times" by Prof. (Dr.) C. P. Sunil Kumar FIE, Academic Director, SNGIST Group of Institutions and National Executive Council Member, ISTE, New Delhi was the resource person.

ROUNDED PROFESSIONAL PROGRAM

The Department of CSE organized an interactive session as a part of industry-institute interaction on the topic " ROUNDED PROFESSIONAL PROGRAM" by Sharath Nair, Talent Acquisition Manager, IDatalytics Pvt Ltd , Infopark. RP2 is a unique program that helps final year IT students/Recent IT graduates to secure an IT job of their dreams. RP2 is designed to boost your employability and make you industry ready through a real-life work experience program. Participants will gain hands-on experience and critical skills (technical and non-technical) through direct exposure to commercial software projects.

PLACEMENT

ASHWIN H

Congratulations to Mr. Aswin H (2017-2021 Batch), for getting placement as Junior Software Engineer, VOFOX Solutions INC, Ernakulam.

REVATHY A S

Congratulations to Ms. Revathy A.S (2017-2021 Batch), for getting placement as Software Engineer, ibs Software, Trivandrum.

LEENU MOHAN

Congratulations to Ms. Leenu Mohan (2018-2022 Batch), for getting placement at TATA Consultancy Services (TCS).

WORKSHOPS

Asst.Prof.Noufala T. S attended an FDP on *Familiarization of Syllabus on Introduction to IT System Lab*, organized by State Institute of Technical Teachers Training & Research Department, Govt. of Kerala from 22-25 November 2021

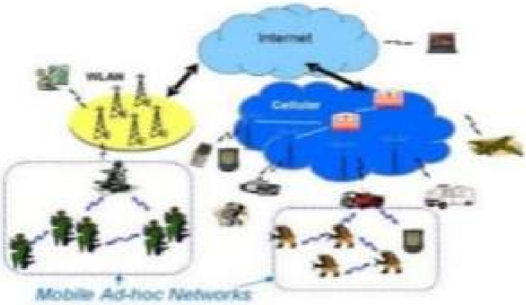
Asst.Prof Gisna Baby attended an FDP on *Familiarization of Syllabus on Introduction to IT System Lab*, organized by State Institute of Technical Teachers Training & Research Department, Govt. of Kerala from 22-25 November 2021

TECH SAVVY

Agamya Pramod E. P, Assistant Professor, CSE, SNGIST

A DETAILED STUDY ON ACCURATE PREVENTION AND DETECTION OF JELLYFISH ATTACK (APD-JFA) IN MANET

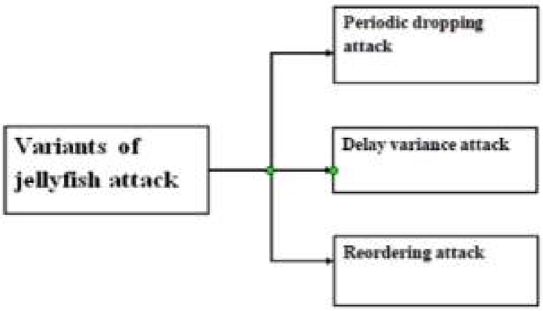
Mobile Ad hoc Network (MANET) is a collection of mobile nodes with no centralized administrator for communication. Every node in this network has to play both host and router at the same time. On the security viewpoint,MANET has no integral security.Wireless channels are avail-able for both legal network users and fraud users. Due to increasing vulnerability, MANET has different security attacks. DoS attack is a major issue in the MANET performance. A sort of DoS attack is a jellyfish attack, which occurs at the network layer on MANET. Jellyfish attack is difficult to detect because of its foraging behavior. The performance is evaluated using different experiments for detecting routing attacks simulated in the NS2 simulator. A novel technique called APD - JFA (Accurate Prevention and Detection of Jelly Fish Attack) is a fusion of authenticated routing based frame-works and Support Vector Machines. Here node property based hierarchical trust evaluation is carried out. SVM is used for learning packet forwarding and to predict any kind of threats and vulnerabilities occurring. This technique is tested using the NS-2 simulator. Parameters such as throughput,packet delivery ratio,dropped packet ratio, and delay are calculated. APD-JFA is more efficient in jellyfish attack detection than existing techniques.



Different types of security attacks in MANETs :

1. Black Hole Attack: - Malicious node injects false route replies to the route requests, announcing it as having the shortest path to a destination.
2. Wormhole attack: - Routing can be disrupted when the routing control message is tunneled. This tunnel between two colluding attacks is known as a wormhole.
3. Denial of service attack:- The complete disruption of the routing function and therefore the entire operation of the ad hoc network. It consumes the resources of the participating nodes and disrupts the establishment of legal routes.
4. Flooding:- Malicious nodes may also inject false packets into the network.
5. Sinkhole attack:- The path presented through the malicious node appears to be the best available route for the nodes to communicate.
6. Eavesdropping attack:- To obtain any confidential information that should be kept secret during the communication.

The Jellyfish attack is regarded as one of the most difficult attacks to detect and degrades the overall network perform ance. Accurate prevention and detection of jellyfish attack is a fusion of authenticated routing-based framework for det-e cting attacks and support vector machine (SVM). SVM is utilized for learning packet forwarding behavior. The technique chooses trusted nodes in the network for performing routing of packets based on hierarchical trust evaluation property of nodes. The technique is tested using the NS-2 simulator. Jellyfish attack is primarily targeted towards closed-loop flows with the ultimate goal to disrupt the normal operation of the network by packet dropping. Jellyfish attack is highly vulnerable in TCP traffic in which cooperative nodes can hardly distinguish between attacks from network congestion.



1. *Jellyfish reordering attack*: In this attack, the malicious node has performed packet reordering before transmitting packets to the destination node. Some of the ACKs of the reordered packets are not received by the destination node in prespecified time so that the sender has to perform packet retransmission.The jellyfish attack node creates a buffer reordering before transmitting packets. The resulting reordering increases the number of ACK packets in the network, which decreases the overall throughput and impacts the network utilization performance.

1. *Jellyfish periodic dropping attack*: The jellyfish performs discarding of packets for a certain period of time, which makes the sender enter into a timeout situation. In order to handle the timeout situation, TCP enters into the slow start phase of packet transmission which impacts the throughput of the network. As a result, packet dropping increases and the overall network becomes unreliable and inefficient as packets do not reach the destination in the correct shape and time.
2. *Jellyfish delay variance attack*: The node impacted by jellyfish attack makes delay the packet delivery at random intervals without changing the packet order. This in turn can impact the network via congestion.

Node property based hierarchical trust evaluation is carried out in this technique. The jellyfish attacks are prevented by choosing only trusted nodes for route path construction. Support vector machines are utilized for packet forwarding behavior learning. This technique guarantees the detection of Jellyfish attack with high precision

(i) *Node property-based hierarchical trust evaluation*: For assessing the trust value of sensor node to determine intrusions in MANET, the trust calculation is dependent upon the node's properties and endorsements from neighbor technique. Any node in MANET can determine trust of neighboring nodes. Neighbor nodes are those in the radio range of another. The trust is known as the confidence level, which is based on time. st is computed on the basis of previous experience with nodes and the endorsements, provided by neighboring nodes. Here, previous experience signifies the behavior of the node that is dependent upon diverse aspects i.e. trust metrics:- direct trust (DT), indirect trust (IT), overall trust (OT). Direct trust (DT) is computed dependent upon trust metrics. Indirect trust (IT) is computed dependent upon the indirect information provided via recommendation of neighbor nodes. Overall trust (OT) is computed by direct as well as indirect trust dependent upon the individual effect of that kind of trust.
(ii) *Node behavior and attack learning using SVM classifier*: Support Vector Machine (SVM) classifier is used to detect and identify jellyfish attack in MANETS. SVM is based on supervised learning and is highly useful for prediction in any type of dataset. Considering the concept of intrusion detection system, SVM is highly useful for predicting any sorts of threats and vulnerabilities. In order to yield improved outcomes, especially prediction, SVM based models are used.

In the future, detection accuracy will be enhanced by integrating deep learning technology. In addition to that, try to implement the APD-JFAD technique on some real-time MANET scenarios using emulations.