XIN-YU HUANG

✉ **xyhuang@std.uestc.edu.cn**
☎ **(+86) 139-7948-2822**

EDUCATION

University of Electronic Science and Technology of China (UESTC) **09/2019 - 06/2023**

B.E. in Optoelectronic Science and Technology

Overall GPA: 3.80/4.00 | Ranked 28 out of 302 students in school

SKILLS

Professional Software	MATLAB, Xcode, Python, MySQL,Microsoft Office, etc.
Other Skills	Management, Giving Public Speech, Writing, Basketball

PUBLICATIONS

[1] **Xinyu Huang,** Yuanming Wu “Identify Selective Forwarding Attacks Using Danger Model: Promote the Detection Accuracy in Wireless Sensor Networks,” *IEEE Sensors Journal,* Apr. 2022

INTERNSHIP

Cloud Service in Big Data of Guizhou Province **07/2021 – 08/2021**

During the summer vacation in 2021, I was invited to the big data and cloud service center in Guiyang.

Undertake Works:

●***Customers Demand Acquisition:*** By communicating with education department of Guizhou province, we determined the data visualization content and designed the scheme of platform constructions.

●***Data Visualization:*** Utilizing the MySQL tools, we finally imported the data from database to fill the platforms. As a result, users can visualize all crucial information from the origina data required. The project has been successfully put into use and gained the critical praise from Government of Guizhou Province.

HONORS

IEEE Student Member	*IEEE Council*
Outstanding Students Scholarship (Top 10% undergrads of China)	*UESTC*
Chinese Collage Students Mathematics Competition, First Price	*Chinese Mathematical Association*
“MathCup” Mathematics Modelling Contest, First Price	*Chinese Mathematical Association*
2022 Mathematical Contest in Modelling: Meritorious Winner	*COMAP*

More than 10 equal or above school-level awards and honors in the area of literary, sports, creation, mathematical model, leadership development, public welfare, volunteer service, etc. including the **highest student honor of academic, sports and leadership development in UESTC.**

RESEARCH & PROJECT

Malicious Nodes Detection in WSNs Based on Danger Signal Model **11/2021- 10/2022**

As the leader of this project, I will just introduce the vital and most successful parts of the whole project.

●***Bionic Algorithm Learning:*** Inspired by human immune systems, establish an artificial immune system (AIS) based on danger signal model to prevent the wireless sensor networks from attacks. The artificial immune system acts when the anomaly in WSNs excesses the normal level.

●***The Mechanism Design of the AIS:*** The intrusion detection system is divided into two phases: screening and confirming. In the screening phase, we first generate five kinds of danger signals of each node, then train the SVM model to classify them. As a result, those nodes with selective forwarding behavior are identified and listed into suspicious nodes. In the confirming phase, we calculate the aggregator outputs of those suspicious nodes and compare them with preset danger threshold. If they are higher than the threshold, intrusions will be confirmed.

●***Optimize the Algorithm Performance:*** Through MATLAB simulations, the results show that the designed system is sensitive to blackhole attacks, wormhole attacks, DDOS attacks and selective forwarding attacks. The detection accuracy is higher than 97% while the false alarm rate stays lower than 4.3%.

Intrusion Detection Systems Construction Based on LSTM Model 01/2022 - Present

To continue the research in intrusion detection systems in WSNs, I just led a brand-new project utilizing the deep learning method: LSTM model. Here are my main contributions and works.

●***Establish the LSTM Model in WSNs:*** When attacks launched in WSNs, the malicious nodes and the normal nodes act differently as time series concerning cumulative forwarding rates. We establish the LSTM model in WSNs as a prediction tool to classify the malicious nodes and the normal nodes.

●***Optimize the Algorithm Performance (Ongoing):*** To make our model effective, we must change settings in neural networks to promote the detection accuracy and keep the false alarm rates lower. The optimization is now in progress.