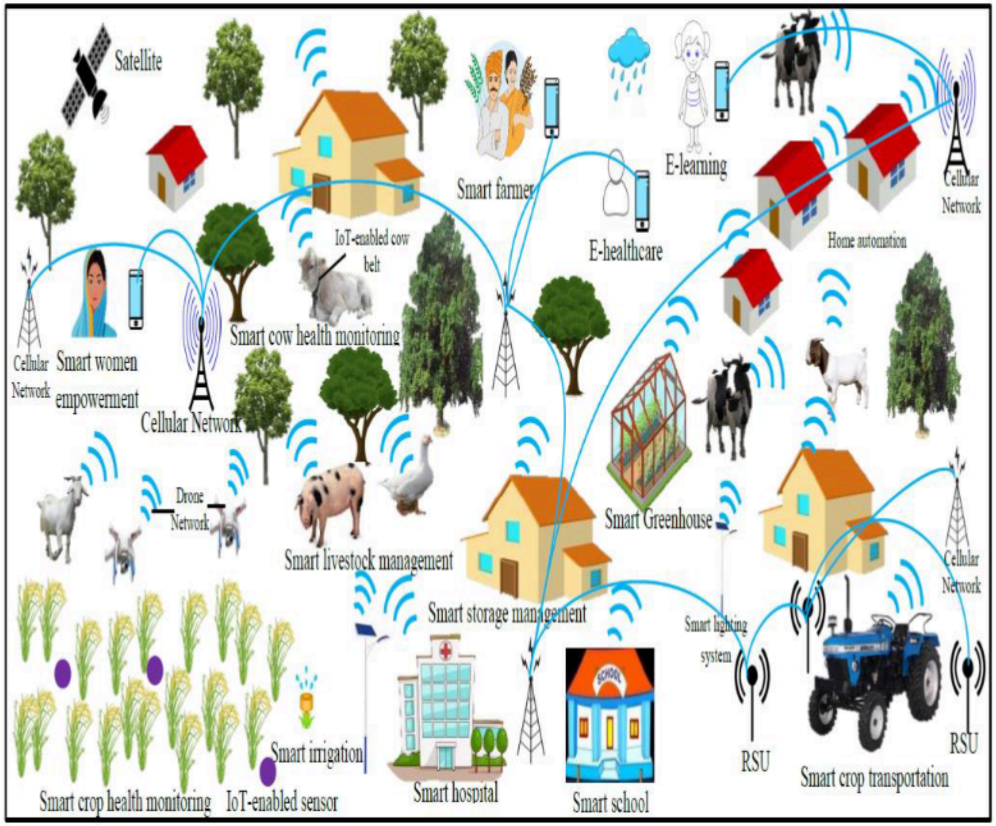
Data-Driven Next-Generation Wireless Networking: Embracing AI for Performance and Security

Dr. Prasenjit Chanak
Assistant Professor

Department of Computer Science and Engineering
Indian Institute of Technology (BHU)
Varanasi-221005, UP, India

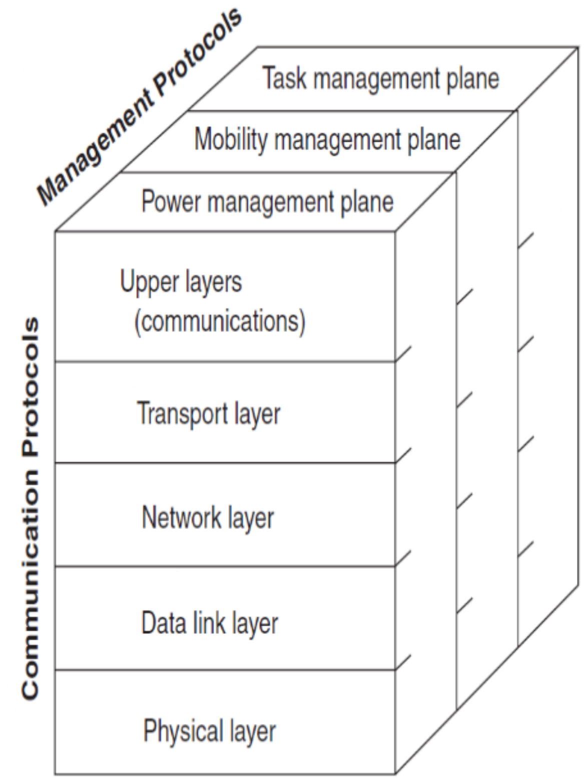
Next-Generation Wireless Networks



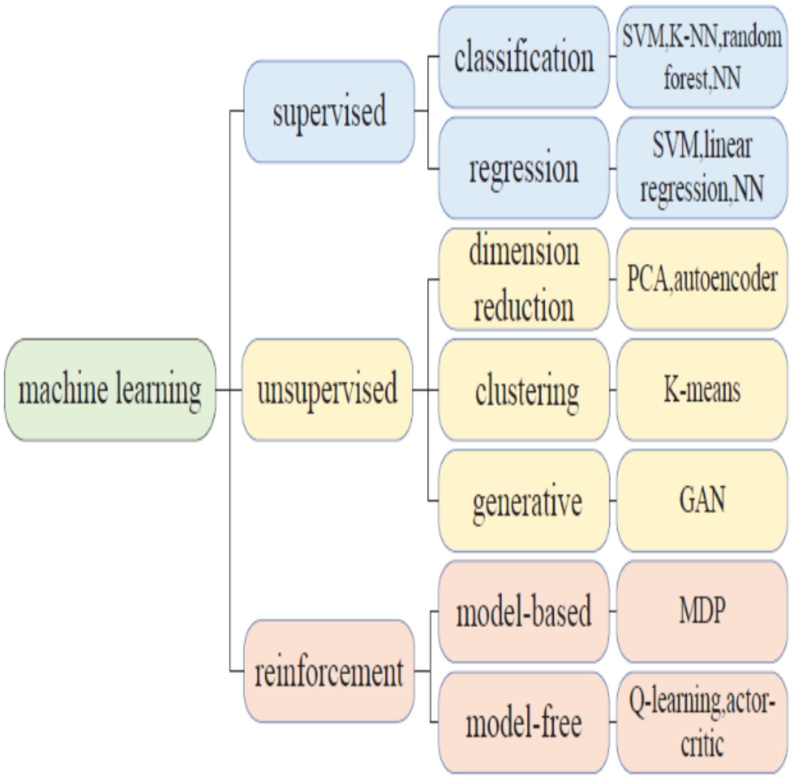
- **Properties of Next-Generation Wireless Networks**:
  - Ultra-High Data Speeds
  - Ultra-Low Latency
  - Massive Device Connectivity
  - High Reliability and Availability
  - Edge Computing and Decentralized Processing
  - Energy Efficiency
  - Security and Privacy
  - Flexible, programmable networks

Applications of AI Across Different Layers of Wireless Networks

- Traditional wireless networking methods struggle to handle the complexities of modern networks
- AI and machine learning offer a data-driven approach to enhance network performance, efficiency, and security
- AI techniques, including supervised, unsupervised, and reinforcement learning, are increasingly used across all network layers improving throughput, security, and energy efficiency while addressing future challenges in wireless network design

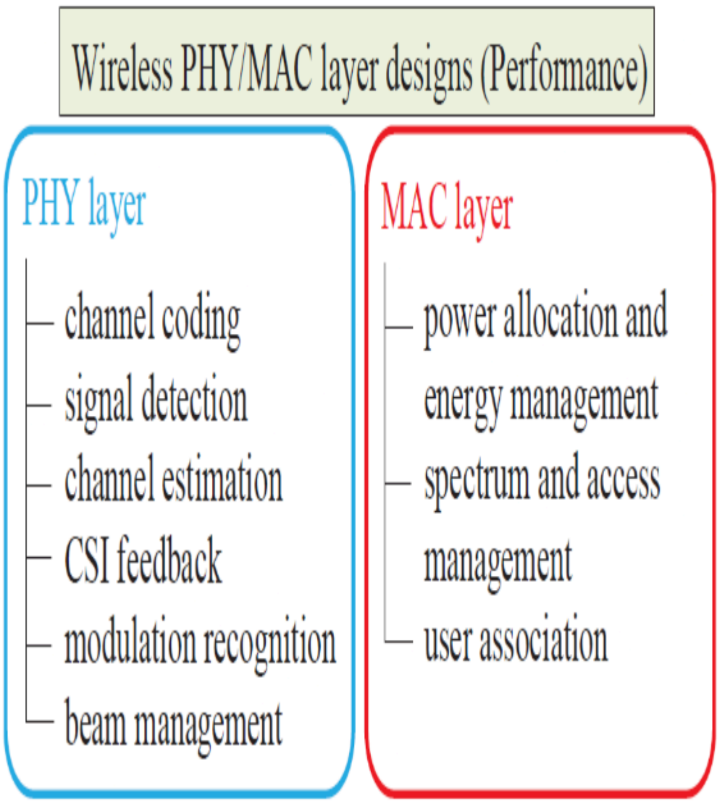


Taxonomy of AI/Machine Learning Techniques



- Supervised learning involves techniques that are trained by explicit labels
- Supervised learning includes classification and regression algorithms
- Unsupervised learning does not need labeled data, which is classified into dimension reduction, clustering, and generative algorithms
- Principal component analysis (PCA) and autoencoder are two common dimension reduction algorithms
- Reinforcement learning is categorized into model-based and model-free algorithms

AI in PHY-MAC Layers



- **Signal Processing & Channel Estimation**: Machine Learning algorithms to predict and compensate for noise, interference, and fading in wireless channels
- Techniques like deep learning can improve channel estimation, ensuring higher data rates and better signal quality
- **Adaptive Modulation & Coding:** AI-based algorithms dynamically adapt the modulation schemes and error-correcting codes based on network conditions
- **Interference Management:** Machine learning models can identify interference patterns and implement solutions such as beamforming, interference cancellation, or power control to minimize signal degradation and maximize coverage

MAC Layer Performance

• **Power Allocation and Energy Management:**

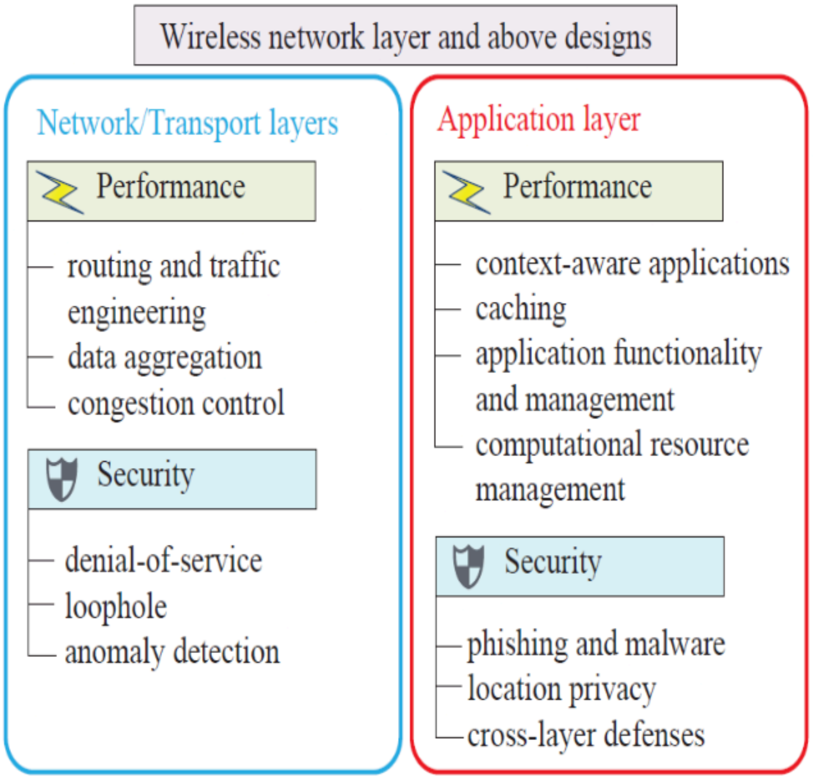
AI Technique Used	Reason and Benefits
Deep Reinforcement Learning (DRL)	Helps secondary users predict primary users' power allocation in cognitive radio networks, improving spectrum efficiency
Deep Q-Network (DQN)	Optimizes mobile network sleeping rules by learning traffic patterns, reducing energy consumption and improving adaptability

MAC Layer Performance

•**Spectrum and Access Management:**

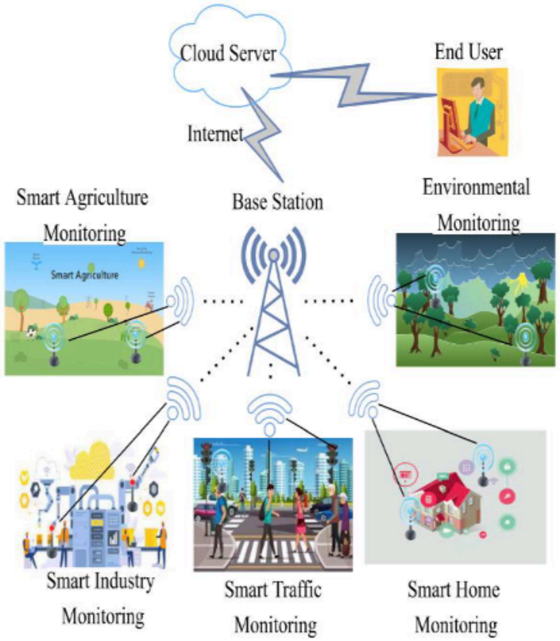
AI Technique Used	Reason and Benefits
Multi-Task Deep Learning for NOMA	Enhances non-orthogonal multiple access (NOMA) by modulating, spreading symbols, and detecting efficiently, enabling better signal decomposition in 5G/NextG networks
Multi-Agent Deep Reinforcement Learning (DRL)	Optimizes dynamic spectrum access by learning the best timeslots for transmission, maximizing data rates and improving overall network efficiency

AI in Network and Transport Layers



- In the context of next-generation wireless networks, the network layer plays a crucial role in providing connectivity, managing traffic, and ensuring efficient use of resources
- As these networks become more complex, AI (Artificial Intelligence) is expected to play an increasingly central role in automating, optimizing, and securing the network infrastructure
- AI can address the challenges posed by the dynamic nature of these networks, including high traffic volumes, mobility, ultra-low latency requirements, and the need for seamless integration of a diverse set of services

AI in Network and Transport Layers

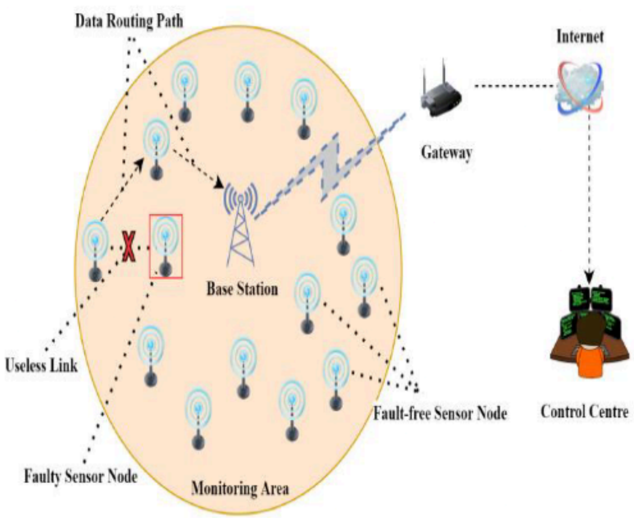


- How AI will be utilized in the network layer of next-generation wireless networks:
- **AI-based Routing:** AI can be used to manage traffic more efficiently in real-time
- For example, machine learning algorithms can predict congestion and reroute traffic dynamically to less congested paths
- This is particularly important in high-density environments like urban areas, where traffic can be unpredictable
- **Predictive Load Balancing:** AI can predict shifts in user demand and adjust network load balancing strategies to ensure smooth service delivery
- It can dynamically shift traffic across base stations, backhaul networks, and other resources to optimize overall performance
- **Fault Tolerance**
- **Localization and Positioning**
- **Quality of Service (QoS)**
- **Congestion Control**

AI for Performance at Network Layer

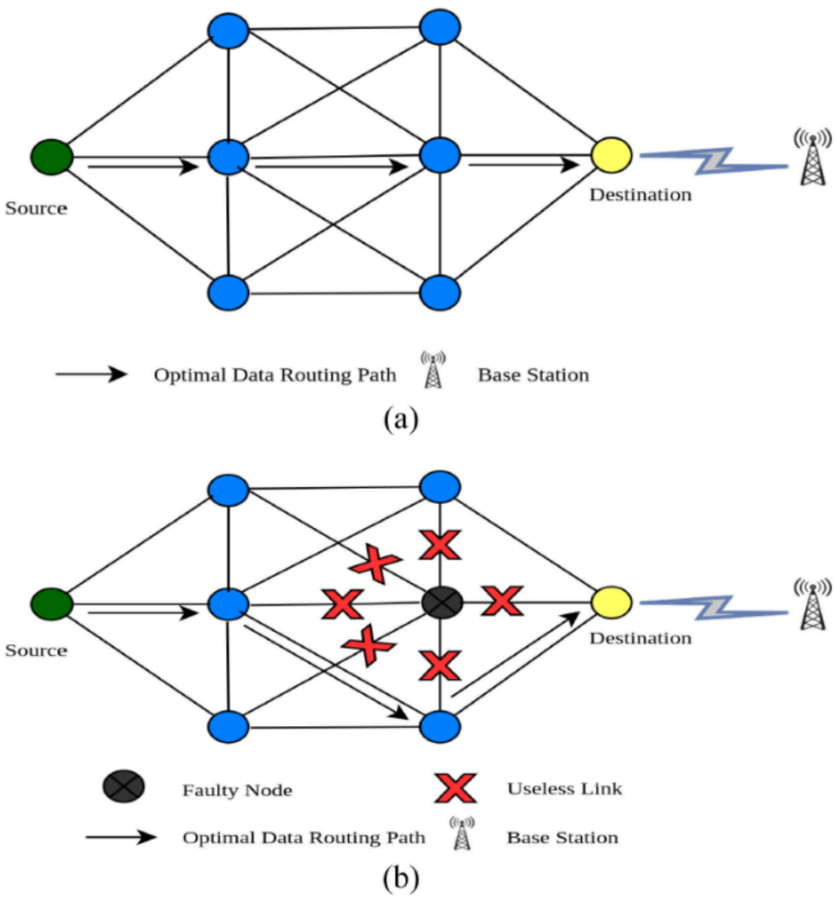
Scope	AI Technique Used	Advantages
Routing & Traffic Engineering (IoT/WSN Networks)	Deep Reinforcement Learning (DRL)	Efficiently schedules HVFT applications to avoid conflicts with time-sensitive applications, enabling 147% more data transmission without degradation
Congestion Control (Mobile/WSN Networks)	Reinforcement Learning	Optimizes congestion control by learning dynamic link bandwidth variations, using Kanerva coding to speed up learning and improve network throughput
Data Aggregation in Mobile Vehicular Networks (VANET)	Reinforcement Learning with Distributed Markov Decision Process (MDP)	Optimizes data aggregation by learning from nearby vehicles' actions, reducing redundant data while maintaining an efficient delay-redundancy

AI for Fault Tolerance Data Routing



- Wireless sensor networks (WSNs) have become one of the essential components of the Internet of Things (IoT)
- A high-performance intelligent WSNs is essential for any IoT-based application
- Faulty nodes and broken links affect the reliability of the IoT-enabled WSNs
- In this work, a Mult objective-deep reinforcement-learning (DRL)- based algorithm is proposed for fault tolerance in IoT-enabled WSNs
- The main objective of this work is to detect the faulty nodes with high accuracy and less overhead
- Furthermore, this work focuses on reliable data transmission after fault detection
- Finally, a mobile sink (MS) is used for energy-efficient data gathering that significantly improves the network lifetime

AI for Fault Tolerance Data Routing



- In WSNs, fault tolerance can be classified into four categories:

- **Energy management:** energy-management-based fault-tolerance mechanism deals with the energy consumption of smart SNs to prevent premature death of the networks

- It also prevents network partitioning and significantly improves the reliability of the networks

- **Flow management:** The flow-management-based fault-tolerance mechanism ensures continuous connectivity in case of any node/link failure

- It also governs the optimal flow of data within the networks that significantly improves the overall performance of the networks

AI for Fault Tolerance Data Routing

- **Data management:** Data-management-based fault-tolerance mechanism deals with collecting and aggregating data by the SN or cluster head (CH) to mitigate the effect of any fault within the networks

- CH is responsible for collecting and aggregating the data from their members and finally transmits it to the BS. It can also help to decrease the overall energy consumption of the networks

- **Coverage/connectivity-management-based fault tolerance:** coverage management- based fault-tolerance mechanism deals with the coverage issues where active SNs preserve the maximum number of alternative paths with maximum coverage

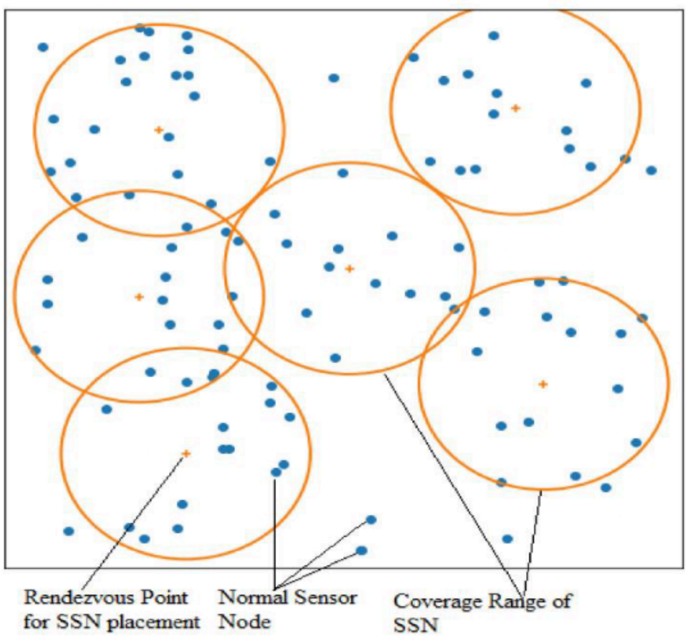
- In this mechanism, the maximum packet delivery to the BS is guided by selecting the alternative paths

AI for Fault Tolerance Data Routing

- **The proposed scheme is divided into four phases**
  - Optimal Rendezvous Points (RPs) selection
  - Cluster formation phase
  - Intelligent fault detection using Multi-Objective Deep Reinforcement Learning (MO-DRL)
  - Efficient data gathering using a Mobile Sink (MS)

- **Phase I: Optimal Rendezvous Points (RPs) selection**
  - The proposed work uses heterogeneous types of sensor nodes (Normal Sensor Nodes (NSNs) and Special Sensor Nodes (SSNs)) in terms of initial energy
  - Initially, the NSNs are deployed randomly in a square-shaped monitoring field
  - Maximum coverage location problem (MCLP) identifies the best optimal locations for SSNs placement

AI for Fault Tolerance Data Routing



- The MCLP aims to find p locations for n candidates by ensuring the maximum coverage of candidates by minimizing the distance between all the locations and candidates
- In the proposed work, this algorithm is used to identify the optimal position for SSNs placement based on the total number of SNs deployed in an environment
- These SSNs become the CH for each group

AI for Fault Tolerance Data Routing

- MCLP-based optimal RPs selection is described as follows:
- *Sets and Indices:*

  $i \in I$ = Set of sensors

  $j \in J$ = Set of RPs

  $Nj = \{i \in I | dij \leq r\}$
- *Parameters:*

  hj = total weight at RP j

  dij = distance between sensor i and RP j

  r = maximum range of RP

- *Decision Variables:*

$$y_i = \begin{cases} 1, & \text{a sensor is sited at location } i \\ 0, & \text{otherwise} \end{cases}$$

$$X_j = \begin{cases} 1, & \text{RP } j \text{ is assigned to a sensor} \\ 0, & \text{otherwise.} \end{cases}$$

AI for Fault Tolerance Data Routin

- Objective Function:

$$\text{Maximize} \sum_{j \in J} h_j X_j.$$

- Constraints:

$$\sum_{i \in I} y_i = p$$

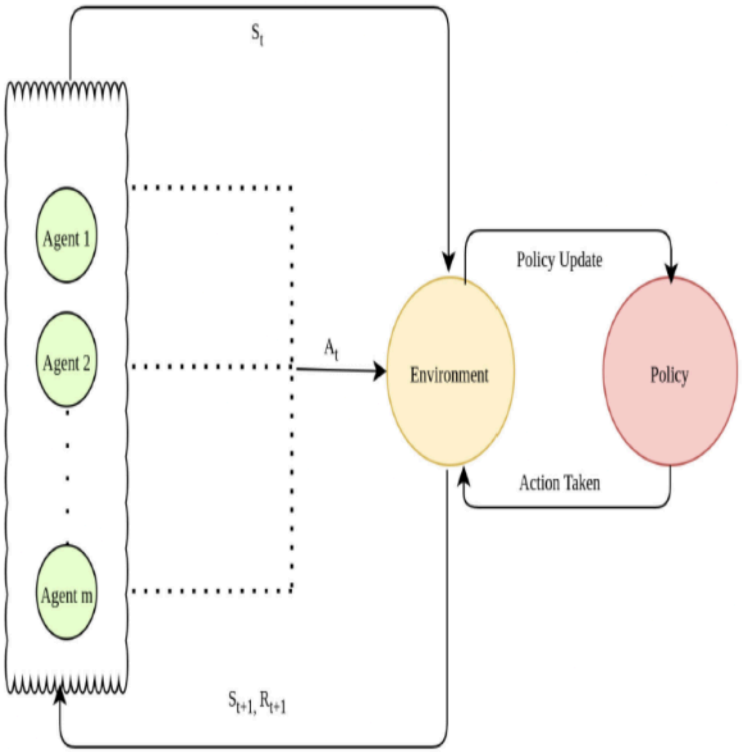
$$\sum_{i \in N_j} y_i \geq X_j \;\; \forall j \in J$$

$$y_i, X_j \in \{0, 1\} \;\; \forall i \in I \;\; \forall j \in J.$$

AI for Fault Tolerance Data Routing

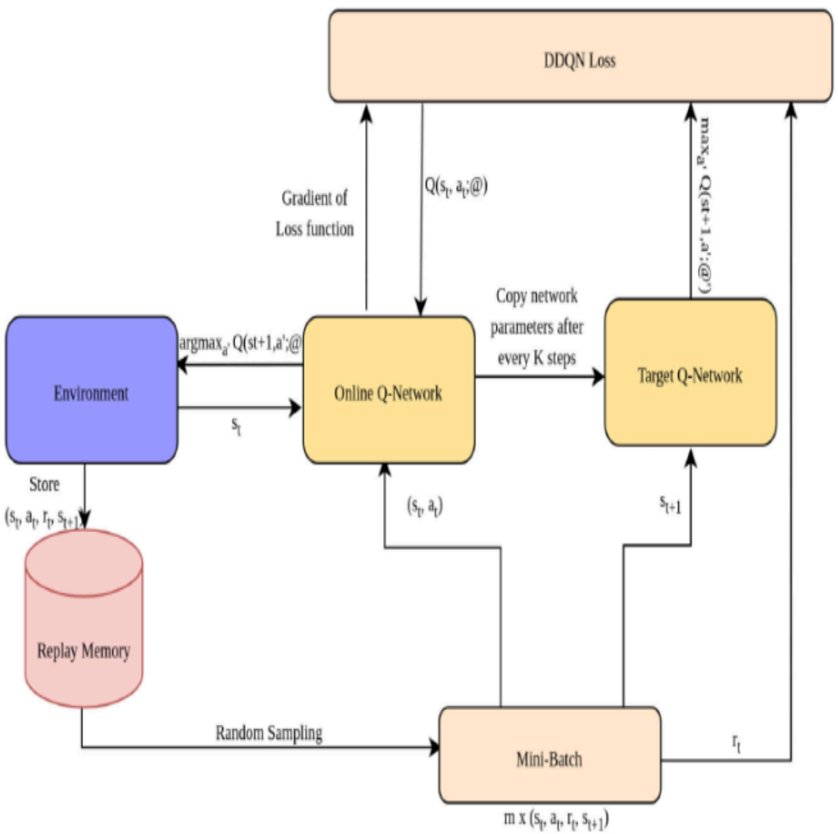
- **Phase II: Cluster formation phase**
  - After deploying the SSNs to their optimal positions, they broadcast a *REQTOJOIN* message with their IDs, location, and residual energy within its range
  - If any NSN receives a *REQTOJOIN* message, then it sends a *RESPONSESSN* message to the corresponding SSN
  - *RESPONSESSN* message contains the ID, location, and residual energy of NSN. After this process, all the NSNs are joined with their nearest SSNs
  - If some nodes will be left to join any SSN, these NSNs are treated as Isolated Sensor Nodes (ISNs)
  - Each ISN broadcasts a HELP message to all other NSNs in their communication range
  - If any NSN receives a help message, then NSNs reply with a *RESPONSENSN* message with their IDs, location, and residual energy
  - Finally, the ISN joins the nearest NSN with high residual energy and the least distance
  - The SSN aggregates the collected data from its members and transmits the data to the MS when it comes to data collection

AI for Fault Tolerance Data Routing



- **Phase III: Fault detection phase using Multi-Objective Deep Reinforcement Learning (MO-DRL)**
  - If a fault occurs in any SN, then an intelligent MO-DRL-based algorithm is used to detect the fault in the SNs
  - In the fault detection phase, the SNs act as agents to detect any fault in the network
  - The first objective is to minimize the message overhead during the fault detection phase
  - The second objective is to minimize the communication delay, and the third objective is set to maximize the network throughput
  - Since all the objectives are contradictory with each other thus, the problem is solved using MO-DRL based on the Pareto optimal policy set

AI for Fault Tolerance Data Routing



- Deployed SNs act as agents and maximize the overall performance by optimizing the multiple conflicting objectives
- The agent deals with multiple objectives, such as minimizing the message overhead and communication delay
- Furthermore, agents also maximize the throughput by timely detection of faulty nodes
- In the proposed work, many wireless SNs with large state space in the MDP framework are considered
- Therefore, a double deep Q-network (DDQN) is used in the MO-DRL algorithm for optimizing the Q-values, which gives the highest rewards by minimizing the over estimations
- The DDQN consists of two identical deep neural networks (DNNs)

AI for Fault Tolerance Data Routing

- The ISNs transmit their data via NSNs to the nearest SSN. After receiving the data, the NSN sends an acknowledgment message to the ISN
- The acknowledgment message contains node ID, location information, and residual energy
- If NSN did not respond within a threshold time, the ISN declares the non-responding NSN as a faulty node and immediately joins the new NSN
- The new NSN is selected based on the least distance and highest residual energy

- **Phase IV: Efficient data gathering using a Mobile Sink (MS)**
  - The MS uses the information stored by the BS during the data gathering process
  - Before starting the data-gathering tour, MS collects the optimal path information from the BS.
  - BS computes shortest data gathering path using TSP with christofides heuristics
  - The MS starts its journey from the BS, visits each SSN for data collection and finally offloads the collected data to the BS

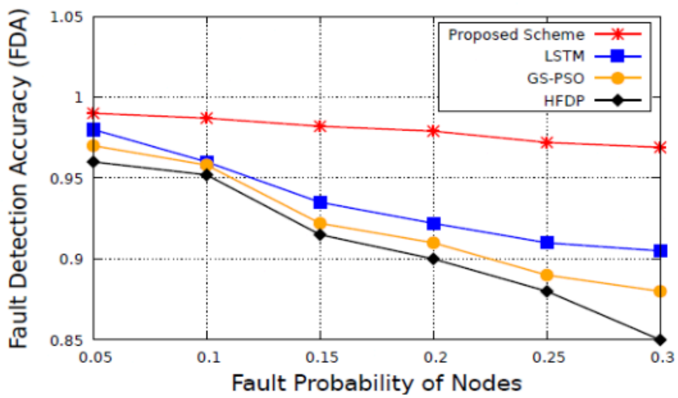
AI for Fault Tolerance Data Routing

Data gathering using a MS

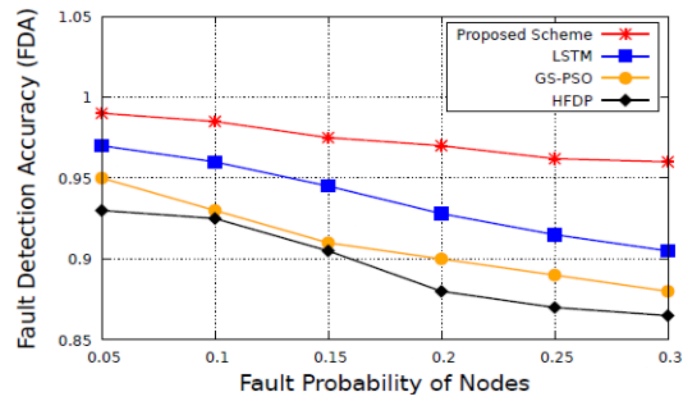
Validation and Evaluation

- The results of the proposed scheme are compared with existing state-of-the-art algorithms like LSTM, GS-PSO, and HFDP
- Extensive simulations have shown the effectiveness of the proposed scheme in terms of Fault Detection Accuracy (FDA), False Alarm Rate (FAR), False Positive Rate (FPR), Average Energy Consumption, and Throughput

Comparison of Performance Metrics

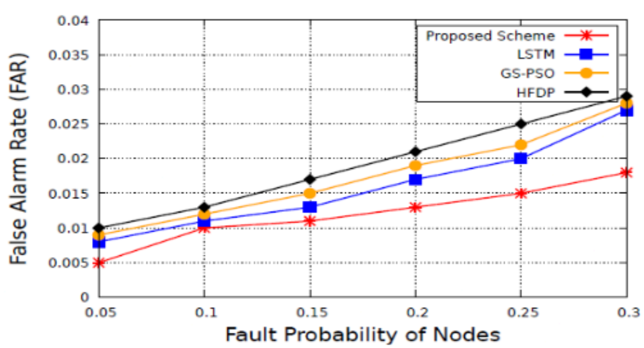


(a) FDA with 100 Nodes

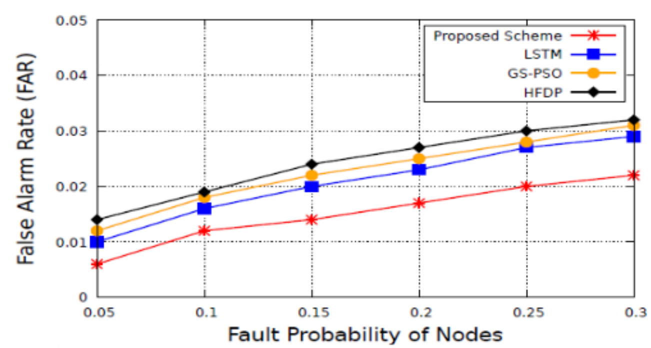


(b) FDA with 200 Nodes

Figure: Fault Detection Accuracy



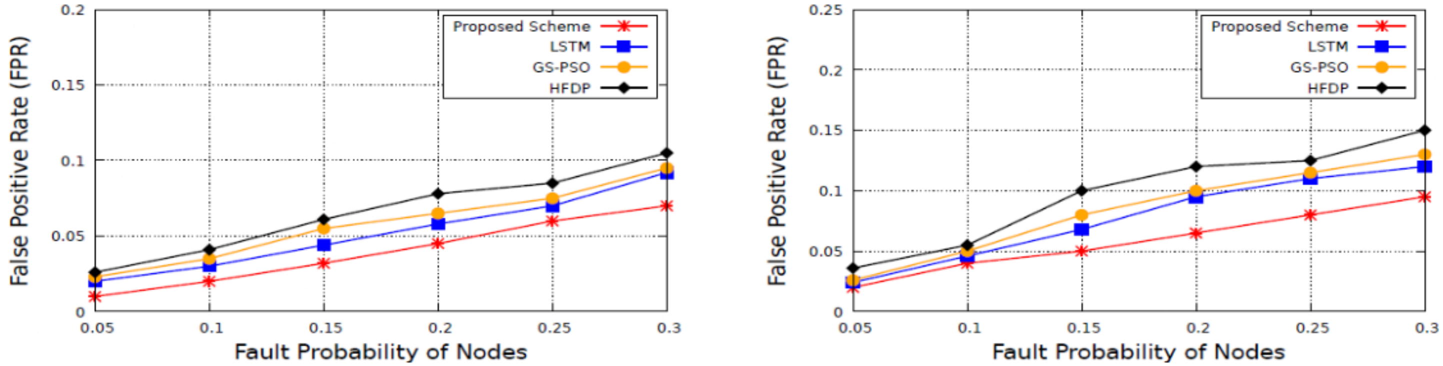
(a) FAR with 100 Nodes



(b) FAR with 200 Nodes

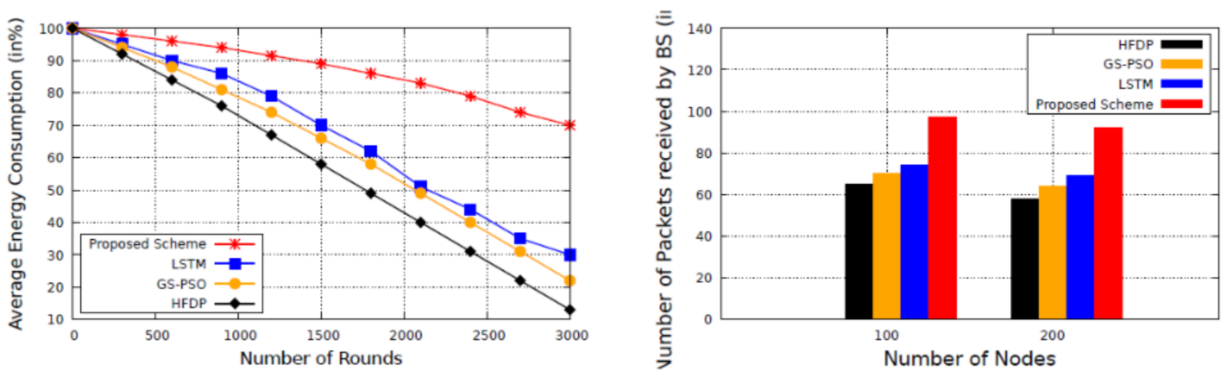
Figure: False Alarm Rate

Comparison of Performance Metrics



(a) FPR with 100 Nodes (b) FPR with 200 Nodes

Figure: False Positive Rate



(a) Avg Energy Consumption (b) Network Throughput

Figure: Average Energy Consumption and Throughput

Comparison of Performance Metrics

- Performance comparison of Proposed Scheme with LSTM, GS-PSO, and HFDP

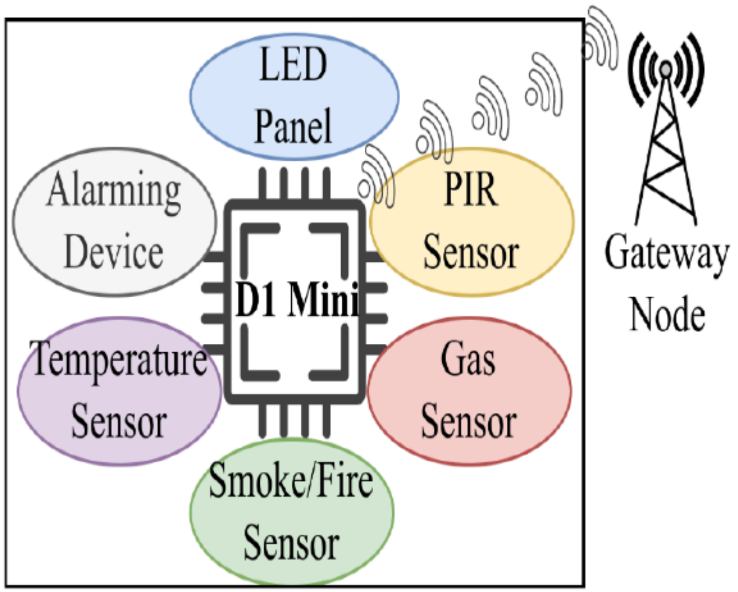
Number of Nodes	Performance metrics	Improvement over LSTM	Improvement over GS-PSO	Improvement over HFDP
100 Nodes	FDA	increased by 16.5%	increased by 22.4%	increased by 31.5%
	FAR	decreased by 17.40%	decreased by 24.5%	decreased by 29.3%
	FPR	decreased by 15.4%	decreased by 23.7%	decreased by 32.5%
	Average Energy Consumption	reduced by 24.03%	reduced by 32.70%	reduced by 41.74%
	Throughput	increased by 22.16%	increased by 31.04%	increased by 43.65%
200 Nodes	FDA	increased by 18.4%	increased by 24.9%	increased by 34.1%
	FAR	decreased by 16.50%	decreased by 23.5%	decreased by 27.3%
	FPR	decreased by 18.4%	decreased by 22.5%	decreased by 34.7%
	Average Energy Consumption	reduced by 22.3%	reduced by 29.70%	reduced by 39.24%
	Throughput	increased by 21.5%	increased by 33.6%	increased by 44.6%

Indoor Emergency Evacuation System

- Emergency Evacuation System for Dynamic Fire Regions
- Over the years, various evacuation techniques have been proposed for a fire emergency
- Many existing techniques consider only the current fire hazard situation during evacuation path design
- They do not consider the dynamic spread of fire with time while designing an evacuation path
- It may cause severe detours and even trap individuals in hazardous regions
- Hence, it is important to consider the dynamic fire spread while designing an evacuation path

Indoor Emergency Evacuation System

- **The proposed scheme is divided into five phases:**
  - Real-time data collection phase
  - Optimal path initialization using reinforcement learning
  - Formation of safety layers around the danger zone
  - Optimal path planning mechanism using a multi-objective grey wolf optimization algorithm
  - Guiding evacuees to the nearest exit
- **Phase I: Real-time data collection phase**
  - Initially, the hardware modules are uniformly deployed in the industrial environment
  - Each hardware module is equipped with different sensors like smoke, gas, temperature, fire, and Passive InfraRed (PIR), an alarm device, a microcontroller, and LEDs



Indoor Emergency Evacuation System

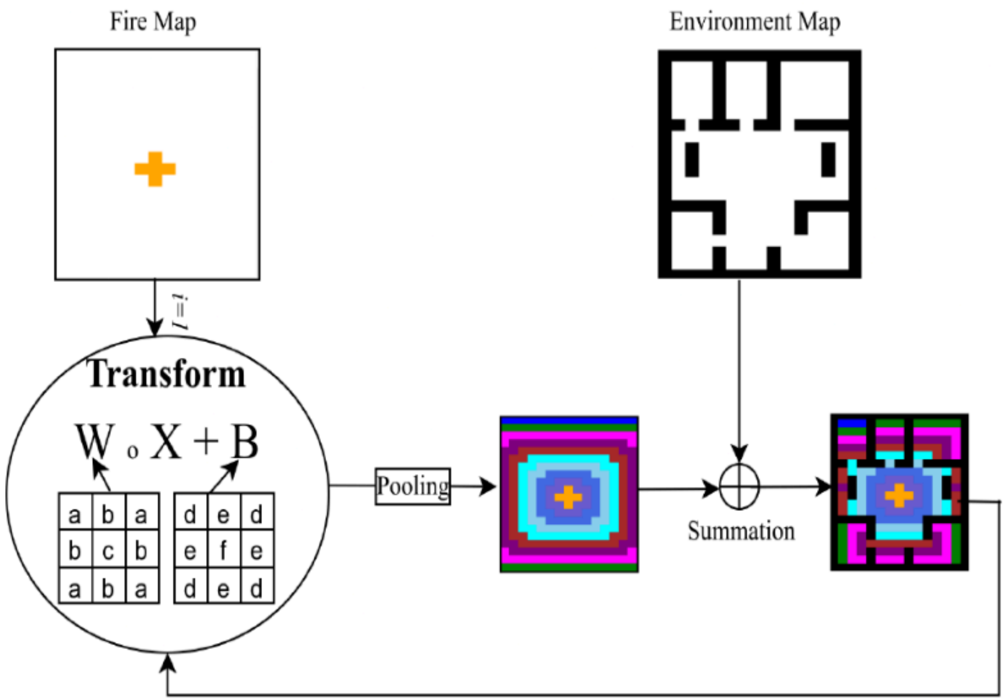
- The sensors equipped in the hardware module sense the monitoring environment periodically
- During an emergency, the hardware modules collect real-time data and transmit it to the BS for further processing

- **Phase II: Optimal path initialization using reinforcement learning**
  - After the deployment of the hardware modules and connection with the gateway node, the optimal paths are identified using Reinforcement Learning (RL)
  - This work uses Q-Learning, which is a value-based RL algorithm. The basic principle of any RL algorithm is to maximize the reward by taking a series of actions at various states
  - In the proposed scheme, the hardware modules are considered as agents, and exit locations are their rewards
  - During an emergency, the optimal paths are identified based on the current input scenario
  - If there is any change in the network topology, then the optimal paths are updated accordingly

Indoor Emergency Evacuation System

- **Phase III: Formation of safety layers around the danger zone**
  - After receiving the data from the hardware modules, safety layers are formed around the danger zone using the Transferred POOling Layers with Breadth-First Search (TPOOL-BFS) emulations
  - The BS converted the data into a source matrix of size $r \times c$
  - Each cell of the source matrix contains different values like danger zone value, human presence value, and exit values
  - The BS also has a monitoring environment map in the form of an environment matrix of size $r \times c$, which contains walls/obstacles and free space
  - Both these maps are combined to form safety layers near the danger zone using TPOOL-BFS
  - TPOOL-BFS takes both the matrices as input and transforms them to form the safety layers around the danger zone
  - The process of forming safety layers based on the hazardous input scenario using TPOOL-BFS

Indoor Emergency Evacuation System



Formation of safety layers using TPOOL-BFS

Indoor Emergency Evacuation System

- **Phase IV: Optimal path planning mechanism using a multi-objective grey wolf optimization algorithm**
    - After forming the safety layers around the danger zone, the proposed scheme identifies the optimal path for each individual from their location to the nearest and safest exit
    - The proposed scheme uses the Multi-Objective Grey Wolf Optimization (MO-GWO) algorithm for optimal path planning
    - In the proposed scheme, the evacuees play the role of grey wolves, and the exit locations are their prey
    - The primary objective is to find the shortest and safest path for each evacuee to the nearest exit
    - For this purpose, multiple objectives have been considered, such as safety layers, load balancing, and distance to the nearest exit

Indoor Emergency Evacuation System

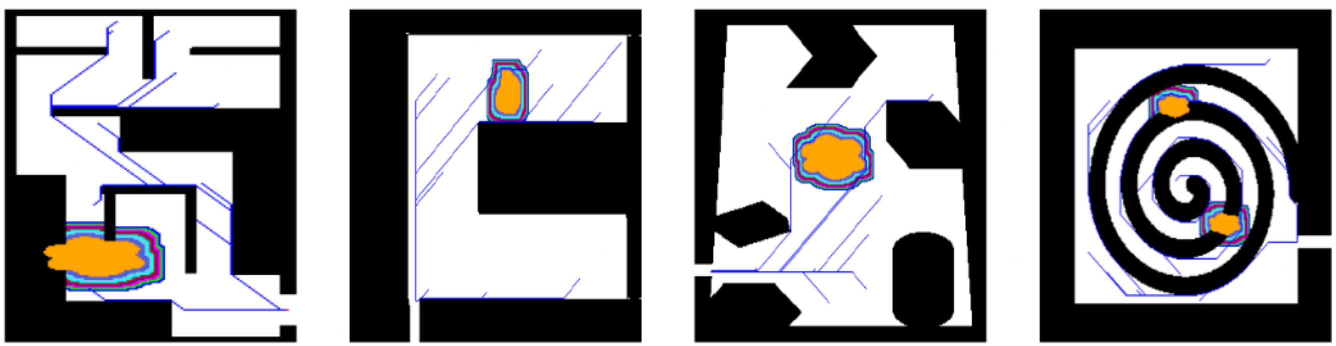
- **Phase V: Guiding evacuees to the nearest exit**
    - After the identification of the optimal path for each individual by the BS, the details of optimal paths for various people are sent back to the hardware module to guide them to the nearest exit
    - The LEDs equipped in each hardware module guides the evacuees by showing the correct direction to follow
    - In case of a power cut or a smoky environment, the LED helps to show the direction clearly
    - The people follow the direction shown by the LEDs and finally reach the nearest safe exit

Validation and Evaluation

- The performance of the proposed scheme is compared with the existing state-of-the-art algorithms like EESBIM, CISM, and ESAIoT
- Extensive simulations have shown the effectiveness of the proposed scheme in terms of average distance travelled and the average time required during evacuation

Simulations Performed

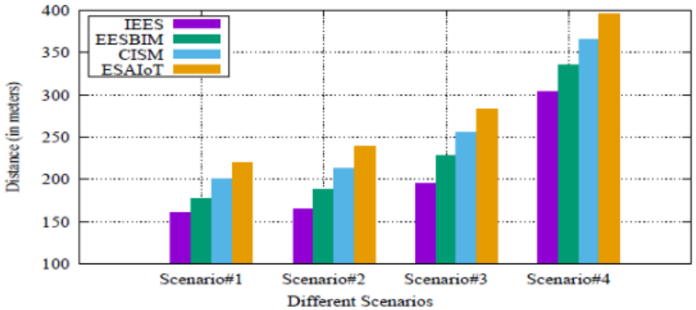
(a) Simulation scenario1 (b) Simulation scenario2 (c) Simulation scenario3 (d) Simulation scenario4



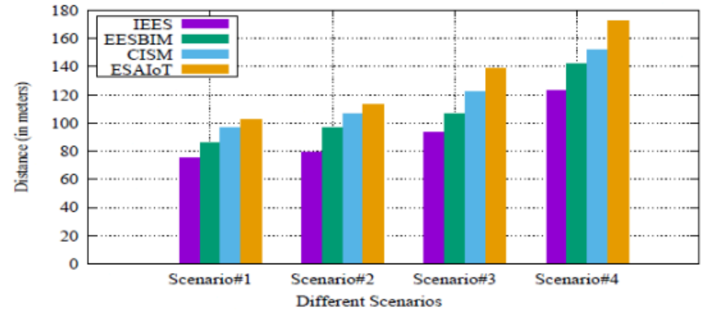
(e) O/P of Simulation scenario1 (f) O/P of Simulation scenario2 (g) O/P of Simulation scenario3 (h) O/P of Simulation scenario4

Figure: Simulation Screenshots of different scenarios

Result Analysis

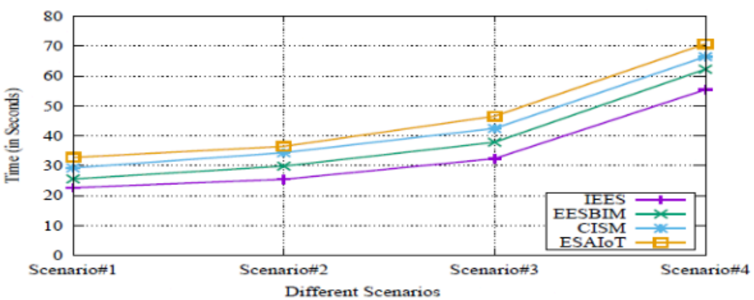


(a) Average distance covered with 1 exit

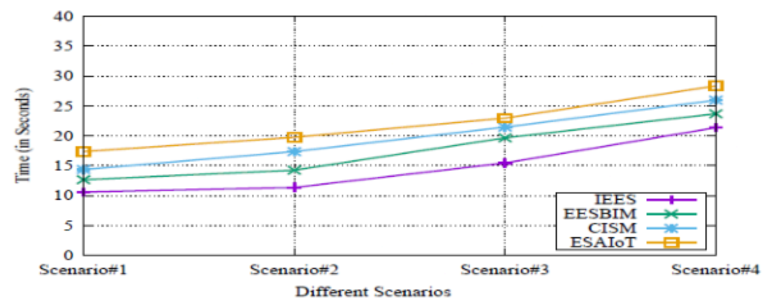


(b) Average distance covered with 2 exits

Figure: Average distance covered with different scenarios



(a) Average evacuation time with 1 exit



(b) Average evacuation time with 2 exits

Figure: Average evacuation time with different scenarios

Comparison of Performance Metrics

- Performance comparison of Proposed Scheme with EESBIM, CISM, and ESAIoT

Different Scenarios	Performance metrics	Improvement over EESBIM	Improvement over CISM	Improvement over ESAIoT
Scenario 1	Average Distance	reduced by 12.65%	reduced by 25.25%	reduced by 37.9%
	Average Evacuation Time	reduced by 15.25%%	reduced by 28.70%	reduced by 38.45%
Scenario 2	Average Distance	reduced by 12.35%	reduced by 24.75%	reduced by 36.5%
	Average Evacuation Time	reduced by 15.75%%	reduced by 27.50%	reduced by 36.25%
Scenario 3	Average Distance	reduced by 13.45%	reduced by 25.85%	reduced by 37.4%
	Average Evacuation Time	reduced by 14.65%%	reduced by 28.50%	reduced by 38.25%
Scenario 4	Average Distance	reduced by 14.25%	reduced by 26.45%	reduced by 37.2%
	Average Evacuation Time	reduced by 14.75%%	reduced by 27.80%	reduced by 37.45%

AI for Performance at Application Layer

- **Caching:**
  - **Intelligent Base Station Caching**: Uses a double-coded caching technique to optimize delay and power consumption
  - **Deep Reinforcement Learning for Optimization**: Models the network as an MDP with unknown transitions, optimizing scheduling and transmission efficiency

- **Application Functionality and Management:**
  - **AI for Traffic Classification (Atlas System):** Uses mobile agents to collect network logs, solving the challenge of training dataset scarcity in traffic classification
  - **AI-Driven Network Function Virtualization (NFV) in SDN:** Multi-agent deep reinforcement learning optimizes device selection, routing, and power allocation in IoT networks
  - **SDN for Mobile Edge Cloud Management:** Uses deep reinforcement learning to optimize video quality, transcoding, caching, bandwidth allocation, and power consumption in SDN-based video streaming

AI for Security at Network Layer

- **DoS Attacks**

  •**Deep Learning for DoS Attack Detection in 5G:** Identifies DoS attacks by analyzing packet features (flow duration, IP addresses, ports etc) while managing traffic

- **Loophole Attacks:**

  - **Deep Learning for Detection:** Uses traffic features (rank, topology inconsistency, rerouting procedures) to train a deep learning model, achieving 90%+ accuracy in detecting loophole attacks

•**Anomaly Detection:**

- Support Vector Machine (SVM)
- Decision Tree
- Random Forest
- K-Means Clustering

AI for Security at Application Layer

- **Phishing and Malware:**
  - A neural network-based fuzzy detector analyzes URL and web features for phishing detection, while Q-learning is used for malware detection in mobile and IoT networks
- **DDoS Detection:**
  - A deep learning framework analyzes network traffic features to detect silent call attacks, message spamming, and signaling attacks across the PHY and application layers
- **Location Privacy**
  - K-means clustering anonymizes spatiotemporal trajectory data, protecting user location privacy while minimizing information loss

Challenges moving forward

- AI models in wireless networks lack interpretability; selecting key features for better accuracy needs more research
- Neural networks are complex and costly for IoT; balancing AI with conventional methods ensures efficiency
- AI in wireless networks faces security risks from adversarial attacks; robust defenses are needed

References

- Vaibhav Agarwal, S. Tapaswi, **Prasenjit Chanak**, “Intelligent fault-tolerance data routing scheme for IoT- enabled WSNs”, ***IEEE Internet of Things Journal***
- Vaibhav Agarwal, Shashikala Tapaswi, **Prasenjit Chanak**, Neeraj Kumar, “Intelligent Emergency Evacuation System for Industrial Environments using IoT-enabled WSNs,” ***IEEE Transactions on Instrumentation and Measurement***

Thank You

Email: prasenjit.cse@iitbhu.ac.in