An Attack-Resilient and Energy-Adaptive Monitoring System for Smart Farms

Qisheng Zhang (presenter) [1] Yash Mahajan [2]
Ing-Ray Chen [3] Dong Sam Ha [4] Jin-Hee Cho [5]

[1,2,3,5]Department of Computer Science, Virginia Tech

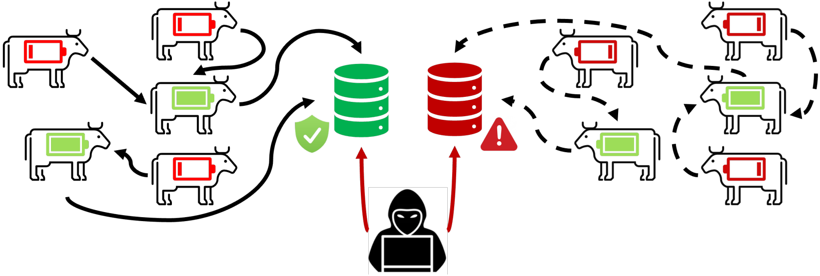
[4]Bradley Department of Electrical and Computer Engineering, Virginia Tech

IEEE GLOBECOM 2022, December 2022

Outline

- **Introduction**
- **Related Work**
- **Problem Statement**
- **System Model**
  - Network Model
  - Node Model
  - Attack Model
- **DRL-based Animal Monitoring**
  - Uncertainty-Aware Animal Monitoring
  - DRL-based Monitoring Update
  - Data Aggregation at LoRa Gateways
- **Experimental Setup**
- **Experimental Results and Analyses**
- **Conclusions and Future Work**

Motivation



- Lack of security-aware smart farm technologies under resource constraints
- Introducing serious, possible food contamination when animal conditions are not properly monitored (The World Health Organization, 2020)
- Potential high revenue loss of farmers due to the failure of protecting farms from cyberattacks, such as false information injection

Key Contributions

- Propose an energy-adaptive monitoring smart farm system to ensure high monitoring quality under network dynamics and cyberattacks.
- Leverage deep reinforcement learning and belief model (i.e., Subjective Logic) to achieve autonomous decision-making under uncertainty.
- Demonstrate the effectiveness of the proposed DRL-based monitoring system in monitoring quality, system overload, and energy consumption.
- Observe the robustness of the proposed smart farm monitoring system against both inside and outside attackers.

Related Work

- **Applications in wireless sensor networks**
  - Rule-based
    - Energy management system (Qi et al., 2019)
  - DRL-based
    - Sleep scheduling system (Chen et al., 2016)
    - Communication routing protocol (Kiani, 2017)
    - Power control scheme (Chen et al., 2018)
    - Access control scheme (Chen et al., 2019)
- **Limitations**
  - Limited number of DRL agents
  - Limited adversarial attack behaviors
  - No data uncertainty considered

Problem Statement

- **Objective function** : Minimize monitoring error ($\mathcal{ME}$) and system overload ($\mathcal{OL}$))

$$\underset{P=\{p_1,p_2,\ldots,p_T\}}{\arg\max} \sum_{i=1}^{T} f(g_i(p_1, p_2, \ldots, p_i)), \quad s.t. \quad \forall i \in [1, T], p_i \in \mathcal{P},$$

$$T : \text{total monitoring step}$$
$$P : \text{update policy}$$
$$p_i : \text{monitoring action at time step } i$$
$$\mathcal{P} : \text{action space}$$
$$g_i : \text{sensor network at time step } i$$
$$f : g \mapsto -\mathcal{ME}(g) - \mathcal{OL}(g)$$

System Model

- **Network Model**: A wireless solar sensor network-based smart farm environment
  - Bluetooth Low Energy (BLE) protocol
    - $100m$ coverage
    - $2Mbps$ data rate
  - Long Range (LoRa) protocol
    - $> 1km$ coverage
    - $27kbps$ data rate
- **Node Model**
  - Temperature: temp_t^i
  - Heart beat: hb_t^i
  - Velocity: ma_t^i
  - Battery level: bl_t^i

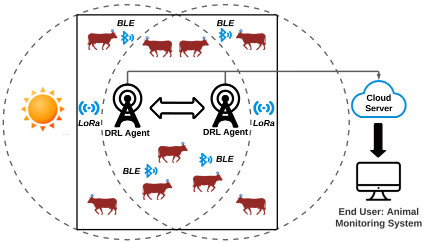
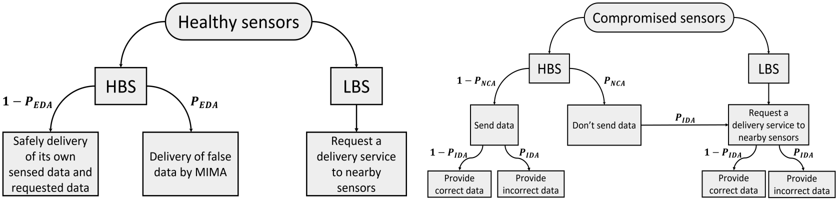


Figure 1: Wireless Solar Sensor Node-based Smart Farm Environment.

System Model

Attack Model

- Non-compliance to the protocol: P_{NCA}
  - Reject the data request
- False data injection
  - Inject from internal/external attacker: P_{IDA}/P_{EDA}
- Denial-of-Service (DoS): P_{IDA}
  - Send redundant data requests



HBS: high battery sensors; LBS: low battery sensors; MIMA: man-in-the-middle attackers

Uncertainty-Aware Animal Monitoring

- SL-based Formulation of a Multinomial Opinion
  - A multinomial opinion X: $\omega_X = (\boldsymbol{b}_X, u_X, \boldsymbol{a}_X)$
  - $\sum_{x \in \mathbb{X}} \boldsymbol{b}_X(x) + u_X = 1$

$\boldsymbol{b}_X$: *belief mass distribution* over $\mathbb{X}$

u_X: *uncertainty mass* representing *vacuity of evidence*

$\boldsymbol{a}_X$: *base rate distribution* over $\mathbb{X}$

  - The dissonance $\boldsymbol{b}_X^{\mathrm{Diss}}$ of an opinion X:

$$\boldsymbol{b}_X^{\mathrm{Diss}} = \sum_{x_i \in \mathbb{X}} \left(\frac{\boldsymbol{b}_X(x_i) \sum_{x_j \in \mathbb{X} \setminus x_i} \boldsymbol{b}_X(x_j) \mathrm{Bal}(x_j, x_i)}{\sum_{x_j \in \mathbb{X} \setminus x_i} \boldsymbol{b}_X(x_j)} \right)$$

relative mass balance:

$$\mathrm{Bal}(x_j, x_i) = 1 - \frac{|\boldsymbol{b}_X(x_j) - \boldsymbol{b}_X(x_i)|}{\boldsymbol{b}_X(x_j) + \boldsymbol{b}_X(x_i)}$$

DRL-based Monitoring Update

- **States**:
  - Global critic state: $s_t^i = g_t(k_1, k_2, \ldots, k_t)$
  - Local actor state: $s_t^i = g_t^i(k_1, k_2, \ldots, k_t)$
  - g_t/g_t^i is represented by the history action sequence
- **Actions**:
  - n_t^i: the total number of LBS
  - Action space: $\mathbf{a}_t^i = \{0, \lfloor \frac{n_t^i}{2} \rfloor, n_t^i\}$
- **Rewards**:
  - $r_t^i = f(g_t(k_1, k_2, \ldots, k_t))$ based on $f(g_t) = -\mathcal{ME}(g_t) - \mathcal{OL}(g_t)$ given in Eq. (6) where k_i is an action taken in step i

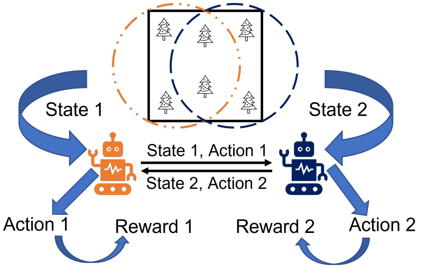


Figure 2: The proposed Multi-Agent Deep Reinforcement Learning (MADRL) framework.

Data Aggregation at LoRa Gateways

- Uncertainty (vacuity) Maximization
  - Move belief mass $\boldsymbol{b}_X$ to uncertainty mass u_X
  - Update uncertainty based on recent data

$$\omega_X = (\boldsymbol{b}_X, u_X, \boldsymbol{a}_X) \longrightarrow \ddot{\omega}_X = (\ddot{\boldsymbol{b}}_X, \ddot{u}_X, \boldsymbol{a}_X)$$

$$\ddot{u}_X = \min_i \left[\frac{\boldsymbol{P}_X(x_i)}{\boldsymbol{a}_X(x_i)} \right],$$

$$\ddot{\boldsymbol{b}}_X(x_i) = \boldsymbol{P}_X(x_i) - \boldsymbol{a}_X(x_i) \cdot \ddot{u}, \quad \text{for} \quad x_i \in \mathbb{X}$$

$$\text{Trigger condition: } u_X < \rho$$

Experimental Setup

- **Dataset**: EmbediVet Devices (EVD)

Metric	Description
Serial	A unique animal identifier
Heart rate	Heart bits per min.
Average-temperature	Average body temperature in Celsius
Min-temperature	Minimum temperature in Celsius
Max-temperature	Maximum temperature in Celsius
Average-activity	Average activity recorded by the number of steps taken
Battery-level	Residual battery life
Timestamp	Date and time of transmission

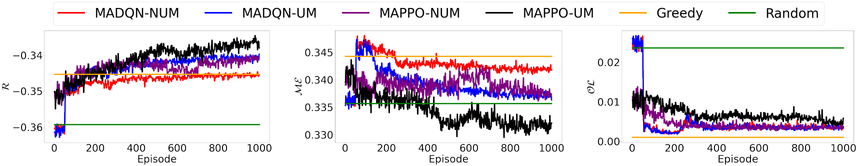
- **Environmental Setup**
  - Modeling sun's movement in a day
  - Consensus agreement: ensuring maximum number of requests executed in the consolidated priority list based on Hopcroft–Karp algorithm [1]
  - Gateway locations: covering the whole farm with same coverage of each gateway

[1] Hopcroft et al., 1973

Experimental Setup

Param.	Meaning	Value
T_M	A minimum battery level to transmit sensed data by a sensor	30%
P_i^{mv}	Cow i's probability to move	$[0.3, 0.7]$
P_A	Probability for an attacker or a compromised node to perform a certain attack (e.g., P_{NCA}, P_{IDA}, P_{EDA})	0.1
n	Total number of cows (sensors)	20
A	Area of a given smart farm	40 acres
a	length of a given smart farm	402 m
ρ	Uncertainty maximization threshold	0.05
t_0	Hyper-parameter used in sun model	0.2
T_u	Time interval for a sensor to send sensed data	30 s
T_a	Time interval for a gateway to take an action to adjust k	60 s
ϕ	A constant factor to normalize freshness of a received sensed data	0.01

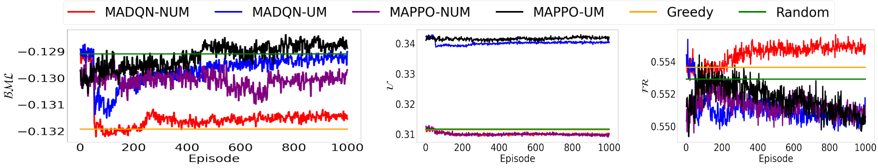
Performance Comparison $(\mathcal{R}, \mathcal{ME}, \mathcal{OL})$



(a) Accum. reward $(\mathcal{R})$ (b) Monitoring error $(\mathcal{ME})$ (c) Overload $(\mathcal{OL})$

- MAPPO-UM has a stationary decision process and achieves the best performance among all comparing schemes.
- DRL algorithms with uncertainty maximization perform better than their counterparts without uncertainty maximization.
- Uncertainty maximization (UM) can update the uncertainty information from time to time, which reflects the sensor network status in a timely manner.

Performance Comparison ($\mathcal{BML}, \mathcal{U}, \mathcal{FR}$)



(d) Batt. maintenance level ($\mathcal{BML}$) (e) Uncertainty ($\mathcal{U}$) (f) Freshness ($\mathcal{FR}$)

- MAPPO-UM achieves the best battery maintenance level ($\mathcal{BML}$) compared to other schemes.
- Different schemes could have very different policies due to two conflict goals our multi-objective function.
- The overall performance order of the considered schemes is: MAPPO-UM $\geq$ MADQN-UM $\approx$ MAPPO-NUM $\geq$ MADQN-NUM$\geq$ Greedy $\geq$ Random.

Conclusions and Future Work

Conclusions: Our proposed MAPPO-UM achieves

- A strong resilience against attacks by achieving the best monitoring quality and minimum system overload.
- Intelligently leveraging the uncertainty information and achieves the best energy maintenance level.
- Enhancing further monitoring quality and energy-adaptive operation with the uncertainty maximization (UM) technique using more recent evidence.

Future Work:

- Use more gateways to use more DRL agents to achieve high scalability of the proposed smart farm system.
- Leverage *transfer learning* algorithms to further expedite the speed of learning convergence by the DRL agents.
- Identify an optimal energy level that can be used for low-energy solar sensors to request data transmission to nearby high-energy sensors.

Any Questions?

Thank you!

Qisheng Zhang at
qishengz19@vt.edu

National Capital Region Campus
7054 Haycock Rd., Office 314
Falls Church, VA 22043

Project website: Google scholar: