Energy Efficiency and Security Optimization in IoT Networks

Vedika Chandra, Bhav Khurana and Avinash Ranjan
Under the guidance of Dr. Vignesh Sivaraman
Department of Computer Science and Engineering
Indian Institute of Technology (BHU) Varanasi

***Abstract*— The rapid evolution of networks introduces transformative technologies like energy harvesting and dynamic IoT connectivity, but also presents challenges in balancing energy efficiency and robust security provisioning. This work explores the application of predictive modeling and adaptive algorithms for optimizing security configurations in energy-harvesting IoT systems. The Extended Kalman Filter (EKF) and Unscented Kalman Filter (UKF) were implemented and compared for power prediction using both synthetic and real-world solar data. While EKF provided reasonable accuracy, it struggled with non-linearities, whereas UKF demonstrated superior performance with lower Mean Squared Error (MSE) and better alignment with real-world measurements. Building on these predictive insights, a novel security configuration algorithm was proposed. The algorithm introduces a Security Threshold (Sth) to cap unnecessary security provisioning, ensuring energy-efficient operation while meeting essential security requirements. Compared to the original algorithm, the proposed method significantly reduced energy consumption and prolonged device operational time without compromising critical security needs. This research highlights the efficacy of combining advanced predictive models like UKF with adaptive security strategies, offering a robust framework for enhancing the efficiency and reliability of IoT systems.**

I. INTRODUCTION

The exponential growth of the Internet of Things (IoT) has paved the way for highly interconnected systems, from smart homes and industrial automation to critical infrastructure management. With the advent of 6G networks, IoT applications are expected to grow even more diverse and demanding, requiring advanced capabilities for real-time data processing, robust security, and efficient energy management. In such environments, energy consumption becomes a crucial concern, especially as IoT devices are often deployed in resource-constrained or remote areas where battery life and energy harvesting are limited. Coupled with these energy demands is the need for dynamic security configurations that can adapt to evolving threats without imposing excessive energy costs on the system.

Traditional approaches to energy management and security in IoT networks often struggle to find a balance between conserving energy and maintaining adequate security levels. Most existing models utilize linear assumptions that fall short in accurately predicting energy harvesting potential, particularly in fluctuating environments like solar-powered IoT networks. This results in either overestimating the energy available—leading to unnecessary security compromises—or underestimating it, thus imposing stringent security controls that drain valuable resources.

To address these challenges, this study proposes an adaptive security configuration model that leverages the Unscented Kalman Filter (UKF) for energy prediction, as UKF offers enhanced accuracy in handling nonlinearities compared to the Extended Kalman Filter (EKF). By applying UKF to real-world solar power data from the National Renewable Energy Laboratory (NREL), our approach enables more accurate energy availability predictions, which in turn drive security configurations dynamically. Unlike static models, the adaptive configuration system adjusts security measures based on predicted energy availability, ensuring both robust security and optimized energy consumption. This dual focus not only prolongs the operational lifespan of IoT devices but also enhances their resilience against potential security threats in a more energy-efficient manner.

This paper details the design and implementation of the proposed model, with an emphasis on its novel integration of UKF for improved energy forecasting in dynamic security contexts. We further explore the comparative performance of EKF and UKF in terms of Mean Squared Error (MSE), demonstrating that the UKF offers substantial improvements in accuracy, thus justifying its adoption for non-linear power prediction. Through extensive experimentation, we show that our model provides a viable pathway toward sustainable and secure IoT deployments in 6G-enabled environments, addressing a critical gap in current IoT research.

II. LITERATURE SURVEY

A. Introduction to IoT Security and 6G Requirements

The Internet of Things (IoT) has become an integral part of modern communication networks, connecting a diverse range of devices to deliver seamless user experiences. However, the rapid growth of IoT networks has introduced significant security and energy management challenges. Threats such as Distributed Denial of Service (DDoS) attacks, data eavesdropping, and unauthorized access have become increasingly prevalent, endangering both data confidentiality and network Quality of Service (QoS). In parallel, the fixed security configurations traditionally adopted by IoT devices often fail to address the dynamic

nature of network threats and energy constraints, resulting in inefficiencies and suboptimal performance.

The upcoming 6G networks aim to address these limitations by incorporating advanced technologies such as terahertz (THz) and millimeter-wave (mmWave) communications, which promise ultra-high data rates and support for bandwidth-intensive IoT applications. Moreover, 6G IoT devices are expected to benefit from energy harvesting techniques that draw power from sources like solar energy and radio-frequency signals, alleviating the constraints of limited battery life. Furthermore, Mobile Edge Computing (MEC) will enhance real-time data processing by offloading latency-sensitive tasks to edge servers. A crucial enabler of these advancements is the integration of Artificial Intelligence (AI), which can dynamically optimize network configurations, making 6G IoT networks more intelligent and adaptive to evolving conditions.

B. Link-Layer Security in IoT

The link layer of IoT networks plays a pivotal role in ensuring data security through mechanisms such as access control, message integrity verification, confidentiality protection, and replay attack prevention. Authentication techniques, including Cipher Block Chaining Message Integrity Code (CBC-MIC) and hash-based MIC, are widely used to verify the legitimacy of data packets and prevent unauthorized access. Encryption algorithms such as AES and RSA ensure that transmitted data remains confidential and secure against interception. However, these security operations come at a significant energy cost, especially for resource-constrained IoT devices.

Research highlights the trade-off between enhanced security and the resulting energy consumption. For instance, increasing the length of the MIC or encryption keys can significantly improve security but also causes higher computational overhead and reduced network throughput. Studies show that maximum authentication lengths can reduce throughput by up to 53 percentage, while combined encryption and authentication can lead to a 62 percentage reduction. Despite these challenges, most IoT devices currently rely on fixed security configurations that fail to adapt to changing energy availability and threat levels, making them unsuitable for dynamic 6G environments where energy harvesting and diverse application requirements are prevalent.

C. Adaptive Security and Energy Optimization

Energy harvesting is emerging as a vital solution for overcoming the battery limitations of IoT devices. Sources such as solar energy, radio frequencies, and vibrations can provide predictable power, enabling devices to sustain operations over extended periods. To effectively utilize these energy sources, lightweight AI techniques, such as the Extended Kalman Filtering (EKF) method, have been employed to predict short-term energy availability. EKF has been shown to deliver accurate predictions of harvesting power, which are critical for optimizing resource allocation and security configurations in energy-aware cycles.

Existing works have proposed AI-based methods for improving IoT energy efficiency. For instance, lightweight algorithms have been used to analyze energy patterns and optimize resource usage. However, these approaches often focus on energy management alone and do not address the joint optimization of energy, security, and QoS. This gap highlights the need for more sophisticated models capable of dynamically balancing energy consumption with the provision of robust security measures, especially in the context of 6G IoT networks with highly variable energy availability and security requirements.

D. Joint Optimization of Security and QoS

The trade-off between QoS and security has been a central theme in IoT research. Traditional approaches, such as game-theoretic models, have been used to optimize resource allocation and security in heterogeneous networks. For instance, Fadlullah et al. utilized game theory to balance QoS and security by dynamically adjusting bandwidth allocation. Other studies have explored token-based protocols and lightweight authentication schemes to reduce energy consumption while maintaining adequate security levels.

Despite these advancements, most existing methods fail to account for the unique characteristics of 6G IoT networks, including energy harvesting capabilities and diverse service requirements. The need for adaptive security mechanisms is particularly pronounced in scenarios where network threats and energy availability fluctuate. Proposed solutions aim to address these gaps by leveraging AI for real-time optimization. For example, security configurations can be adjusted dynamically based on predicted energy availability, allowing devices to provide robust protection without exhausting their power reserves. This approach not only extends device lifetimes but also improves overall network performance by ensuring continuous service provision under varying conditions.

E. Security Challenges in Energy-Harvesting IoT Networks

Security in energy-harvesting IoT networks presents a unique set of challenges due to the interplay between energy constraints and the need for robust protection mechanisms. In IoT networks, devices often operate in remote and hostile environments where traditional security measures may not be feasible due to resource limitations. The combination of energy harvesting and limited computational resources significantly impacts the security strategies that can be employed in such networks. One of the primary security concerns in energy-

harvesting IoT networks is ensuring the integrity and confidentiality of data transmitted between devices. Since many IoT devices rely on wireless communication for data exchange, they are susceptible to eavesdropping, unauthorized access, and data tampering. The traditional encryption and authentication methods, which require significant computational power, may not be suitable for energy-constrained devices. As a result, there is a need for lightweight cryptographic techniques that balance security with energy consumption.

Another challenge stems from the unpredictable and intermittent nature of the harvested energy. The availability of energy sources like solar, wind, or RF can fluctuate, leading to periods of insufficient energy for IoT devices to perform security operations, such as data encryption or secure key exchange. During these energy-scarce periods, devices may have to prioritize functionality over security, which could expose them to potential attacks. This dynamic energy behavior complicates the development of secure communication protocols that need to adapt to varying energy level. Furthermore, energy harvesting can introduce new attack vectors into IoT networks. Malicious actors may attempt to exploit energy management protocols or manipulate energy harvesting models to deplete the resources of a device, thereby rendering it inoperable. For instance, attackers could flood the network with false data to influence energy prediction models or manipulate energy storage systems to cause battery drainage. These types of attacks can significantly undermine the reliability of energy-harvesting IoT networks and hinder their effectiveness. Additionally, the large-scale deployment of IoT devices, often with minimal oversight, increases the risk of compromised devices being introduced into the network. Malicious devices with tampered energy harvesting components can potentially disrupt the functioning of the entire network. These devices could send incorrect energy harvesting reports or inject false data into the system, resulting in poor decision-making and suboptimal energy management.

The integration of security measures in energy-harvesting IoT networks requires an approach that not only addresses the conventional security issues, such as data confidentiality and integrity, but also considers the specific constraints and vulnerabilities introduced by energy harvesting. Secure energy management schemes, energy-efficient cryptographic protocols, and lightweight authentication mechanisms are some of the solutions that can be employed to mitigate the security risks in such networks. These techniques need to be adaptive and resilient to varying energy conditions, ensuring that the devices can continue to function securely despite fluctuations in energy availability. In conclusion, while energy harvesting offers significant advantages for the sustainability and autonomy of IoT devices, it also introduces a new layer of complexity in terms of security. Addressing the security challenges in energy-harvesting IoT networks requires innovative solutions that integrate energy-efficient security protocols and adaptive energy management strategies. By overcoming these challenges, energy-harvesting IoT networks can provide reliable and secure solutions for a wide range of applications.

F. Kalman Filters in IoT Systems

Kalman filters (KF) are widely used for state estimation in dynamic systems, including energy prediction in IoT networks. The Kalman filter is an optimal estimation algorithm that combines noisy measurements with a model of the system to predict the state of a process. This filter has been applied extensively in various fields, including aerospace, robotics, and energy management, to estimate the state of systems with uncertain or noisy data. The Extended Kalman Filter (EKF) and Unscented Kalman Filter (UKF) are two variations of the Kalman filter that are used to estimate the states of nonlinear systems. While the EKF linearizes the system at each step using a first-order approximation, the UKF handles nonlinearities more effectively by using a set of carefully chosen points (sigma points) to represent the state distribution. In the context of energy-harvesting IoT networks, Kalman filters have been used for energy prediction, ensuring that devices can accurately forecast their energy consumption and generation patterns. The EKF has been traditionally used for this purpose, but due to its reliance on linear approximations, it may not perform well in highly nonlinear environments, such as those encountered in energy-harvesting systems.

III. WORK DONE AND RESULTS ANALYSIS

A. About Extended Kalman Filter (EKF)

The Extended Kalman Filter (EKF) is an adaptation of the Kalman Filter designed for nonlinear systems. Unlike the traditional Kalman Filter, which is optimal for linear systems, the EKF linearizes the process and measurement models at each iteration using a first-order Taylor expansion. This allows it to estimate states in systems with nonlinear dynamics while preserving Gaussian distributions.

1) State Estimation in Linear Systems: The classical Kalman Filter works with the following state-space model:

$$x_k = Fx_{k-1} + Bu_k + w_k, \tag{1}$$

$$z_k = Hx_k + v_k, \tag{2}$$

where:

- x_k: State vector at time k.
- z_k: Measurement vector at time k.
- F: State transition matrix.
- H: Measurement matrix.
- B: Control input matrix.
- w_k, v_k: Process and measurement noise, assumed to be Gaussian.

2) Extension to Nonlinear Systems: For nonlinear systems, the models are given as:

$$x_k = f(x_{k-1}, u_k) + w_k, \tag{3}$$

$$z_k = h(x_k) + v_k, \tag{4}$$

where $f(\cdot)$ and $h(\cdot)$ represent the nonlinear state transition and measurement models, respectively.

3) EKF Algorithm: Prediction Step: The state and covariance are predicted using the nonlinear state transition model:

$$\hat{x}_k^- = f(\hat{x}_{k-1}, u_k), \tag{5}$$

$$P_k^- = F_k P_{k-1} F_k^\top + Q_k, \tag{6}$$

where:

- $\hat{x}_k^-$: Predicted state estimate.
- P_k^-: Predicted covariance matrix.
- $F_k = \frac{\partial f}{\partial x}\big|_{\hat{x}_{k-1}}$: Jacobian of f with respect to x.
- Q_k: Process noise covariance.

4) EKF Algorithm: Update Step: Measurements refine the predictions as follows:

$$y_k = z_k - h(\hat{x}_k^-), \tag{7}$$

$$S_k = H_k P_k^- H_k^\top + R_k, \tag{8}$$

$$K_k = P_k^- H_k^\top S_k^{-1}, \tag{9}$$

$$\hat{x}_k = \hat{x}_k^- + K_k y_k, \tag{10}$$

$$P_k = (I - K_k H_k) P_k^-, \tag{11}$$

where:

- y_k: Innovation or residual (difference between observed and predicted measurements).
- $H_k = \frac{\partial h}{\partial x}\big|_{\hat{x}_k^-}$: Jacobian of h with respect to x.
- S_k: Innovation covariance.
- K_k: Kalman gain.
- R_k: Measurement noise covariance.

5) Applications of EKF: The EKF is commonly used in scenarios where nonlinear dynamics exist but the noise remains Gaussian. Some key applications include:

- Robotics: Localizing robots by combining sensor data and motion models.
- Navigation Systems: GPS and Inertial Navigation Systems (INS) for tracking vehicles.
- IoT Energy Harvesting: Predicting energy availability in devices powered by solar panels or other renewable sources.

6) Limitations of EKF: The EKF has limitations regarding linearization and assumptions as highlighted below:

- Linearization Errors: The Jacobian approximation may introduce inaccuracies for highly nonlinear systems.
- Initialization Sensitivity: Poor initial estimates can lead to slow convergence or divergence.
- Noise Assumptions: EKF assumes Gaussian noise, which limits its applicability to non-Gaussian disturbances.

7) EKF in This Study: In this study, the EKF was implemented to predict energy harvested by IoT devices using solar power data. Key observations include:

- Prediction Accuracy: EKF performed reasonably well for predictable scenarios but showed deviations during abrupt changes in solar power.
- Mean Squared Error (MSE): EKF showed moderate accuracy but higher errors compared to the Unscented Kalman Filter (UKF).
- Plot Analysis: Visual plots indicated noticeable deviations from actual values during periods of nonlinear behavior, highlighting EKF's limitations in capturing such dynamics.

While EKF served as a baseline for state estimation, its limitations emphasized the need for more robust methods like UKF for highly dynamic and nonlinear systems, as seen in energy-harvesting IoT environments.

B. About Unscented Kalman Filter (UKF)

The Unscented Kalman Filter (UKF) is a state estimation method designed to handle nonlinear systems more effectively than the Extended Kalman Filter (EKF). Unlike the EKF, which linearizes the system using Jacobian matrices, the UKF uses the unscented transform to approximate the mean and covariance of the system's state distribution. This approach avoids explicit linearization, making the UKF more accurate for systems with significant nonlinearities.

1) The Problem with Linearization in EKF: In the EKF, nonlinear models are linearized using a first-order Taylor expansion. While this simplifies computations, it introduces errors because the approximation assumes small deviations from the operating point. This can lead to inaccuracies in scenarios where the system exhibits significant nonlinear dynamics or higher-order effects. The UKF addresses these limitations by focusing on the distribution of the state rather than the nonlinear functions themselves.

2) Key Principle of UKF: The UKF operates on the principle that it is easier and more accurate to transform a set of carefully chosen sample points (sigma points) through a nonlinear function than to linearize the function itself. These sigma points are deterministic samples generated to capture the true mean and covariance of the state distribution.

3) UKF Algorithm: Initialization Step: The state mean and covariance are initialized as:

$$\hat{x}_0 = \mathbb{E}[x_0], \tag{12}$$

$$P_0 = \mathrm{Cov}[x_0]. \tag{13}$$

$$\tag{14}$$

4) UKF Algorithm: Sigma Point Generation Step: To represent the state distribution, a set of $2L+1$ sigma points is generated, where L is the dimension of the state vector. The sigma points are chosen to reflect the mean and covariance of the state:

$$X_0 = \hat{x}, \tag{15}$$

$$X_i = \hat{x} + (\sqrt{(L+\lambda)P})_i \quad \text{for } i = 1, \ldots, L, \tag{16}$$

$$X_{i+L} = \hat{x} - (\sqrt{(L+\lambda)P})_i \quad \text{for } i = 1, \ldots, L. \tag{17}$$

Here:

- X_i: Sigma points.
- $\lambda = \alpha^2(L+\kappa) - L$: Scaling parameter to control the spread of the sigma points.
- α, κ: Hyperparameters chosen to optimize the distribution.
- $\sqrt{(L+\lambda)P}$: Square root of the scaled covariance matrix.

5) UKF Algorithm: Prediction Step: Each sigma point is propagated through the nonlinear process model:

$$X_i^- = f(X_i, u_k), \tag{18}$$

where $f(\cdot)$ is the nonlinear state transition function. The predicted mean and covariance are then computed as:

$$\hat{x}_k^- = \sum_{i=0}^{2L} W_i^{(m)} X_i^-, \tag{19}$$

$$P_k^- = \sum_{i=0}^{2L} W_i^{(c)} (X_i^- - \hat{x}_k^-)(X_i^- - \hat{x}_k^-)^\top + Q_k. \tag{20}$$

Here:

- $W_i^{(m)}$: Weights for the mean.
- $W_i^{(c)}$: Weights for the covariance.
- Q_k: Process noise covariance.

6) UKF Algorithm: Update Step: The sigma points are passed through the nonlinear measurement model:

$$Z_i = h(X_i^-), \tag{21}$$

where $h(\cdot)$ is the measurement function. The predicted measurement mean and covariance are computed as:

$$\hat{z}_k = \sum_{i=0}^{2L} W_i^{(m)} Z_i, \tag{22}$$

$$S_k = \sum_{i=0}^{2L} W_i^{(c)} (Z_i - \hat{z}_k)(Z_i - \hat{z}_k)^\top + R_k, \tag{23}$$

where R_k is the measurement noise covariance. The cross-covariance between the state and measurement is calculated as:

$$P_{xz} = \sum_{i=0}^{2L} W_i^{(c)} (X_i^- - \hat{x}_k^-)(Z_i - \hat{z}_k)^\top. \tag{24}$$

The Kalman gain and updated state estimates are:

$$K_k = P_{xz} S_k^{-1}, \tag{25}$$

$$\hat{x}_k = \hat{x}_k^- + K_k(z_k - \hat{z}_k), \tag{26}$$

$$P_k = P_k^- - K_k S_k K_k^\top. \tag{27}$$

$$\tag{28}$$

7) Advantages of UKF Over EKF: UKF works better than EKF in many aspects as highlighted below:

- No Linearization Required: Unlike the EKF, the UKF does not approximate the nonlinear functions using Jacobians, avoiding errors due to linearization.
- Higher Accuracy: The UKF provides more accurate state estimates, especially in highly nonlinear systems, as demonstrated by its performance on real-world solar data.
- Better Handling of Uncertainty: The UKF uses sigma points to propagate uncertainty more accurately through nonlinear transformations.
- Reduced Sensitivity to Initial Conditions: UKF performs better even with poor initial state estimates compared to the EKF.

8) Performance in This Study: In this study, the UKF was applied to predict energy harvested by IoT devices using both synthetic and real-world solar power datasets. Key results include:

- Prediction Accuracy: The UKF consistently achieved lower Mean Squared Error (MSE) compared to the EKF, especially in handling abrupt changes in solar power.
- Visual Comparison: Plots showed that the UKF predictions closely followed actual power measurements, with narrower confidence intervals indicating reduced uncertainty.
- Hyperparameter Tuning: By varying process noise, measurement noise, and scaling parameters, the UKF demonstrated adaptability to different conditions, outperforming the EKF in robustness.

9) Conclusion: The UKF addresses the limitations of the EKF by eliminating the need for linearization and providing more accurate and reliable state estimates. Its performance in this study underscores its suitability for energy prediction in IoT systems with nonlinear and dynamic behaviors. By leveraging the UKF, IoT devices can optimize resource allocation and security configurations, ensuring efficient operation in complex environments.

C. Implementation Details

This section describes the implementation of the Extended Kalman Filter (EKF) and Unscented Kalman Filter (UKF) for predicting energy availability in IoT devices. Both filters were tested on synthetic and real-world datasets to evaluate their performance in dynamic and nonlinear scenarios.

1) Synthetic Data: To validate the functionality of the filters, synthetic data was generated. The dataset consisted of a time-series of power measurements, simulating a simple system with predictable noise characteristics. This controlled environment allowed for an initial assessment of filter behavior under known conditions.

2) Real-World Solar Data: Real-world solar power data was sourced from the National Renewable Energy Laboratory (NREL) database. The dataset included hourly solar power output measurements from a 9 MW solar power plant over an entire year. The data format included:

- LocalTime: Timestamps in the format `MM/DD/YY HH`.
- Power (MW): Measured solar power output in megawatts.

This dataset introduced nonlinearities and variability inherent to real-world systems, providing a challenging testbed for the filters.

3) Implementation of EKF and UKF: Both filters were implemented in Python using the following steps:

- The state model assumed a constant velocity model for the power signal, which assumes linear changes over small time intervals.
- Process noise (Q) and measurement noise (R) were tuned to match typical characteristics of power prediction tasks.
- Predictions were compared against the actual measurements to compute the Mean Squared Error (MSE), a key performance metric.
- The EKF linearized the nonlinear state transition and measurement models at each iteration using Jacobian matrices. This approach provided a baseline performance but was limited by linearization errors, especially under nonlinear conditions.
- The UKF utilized the unscented transform to propagate sigma points through nonlinear models, capturing higher-order effects. This made it better suited for the nonlinearities observed in real-world solar data.

4) Hyperparameter Testing: The UKF was further evaluated with different hyperparameter configurations:

- Initial Covariance (P): Represents initial uncertainty about the state.
- Process Noise (Q): Models the uncertainty in the system's dynamics.
- Measurement Noise (R): Accounts for noise in the observed measurements.

Five sets of Hyperparameters were tested to analyze the adaptability of the UKF to varying noise conditions.

5) Error Comparison: The Mean Squared Error (MSE) was computed for both EKF and UKF. Results demonstrated that the UKF consistently outperformed the EKF, achieving lower errors across all datasets. The UKF's ability to handle nonlinearities significantly contributed to its improved performance.

TABLE I
COMPARISON OF MEAN SQUARED ERROR

Algorithm	MSE
Unscented Kalman Filtering	377.12
Extended Kalman Filtering	498.14

6) Graphical Analysis of Predicted Power: The predicted power values from both EKF and UKF were plotted against the actual power measurements. The following observations were made:

a) EKF Results: The EKF plots showed noticeable deviations from the actual measurements, particularly during periods of abrupt change in solar power. These deviations highlight the limitations of linearization in capturing nonlinear dynamics.

b) UKF Results: The UKF plots closely followed the actual power measurements, with reduced fluctuations and better tracking of nonlinear variations. Confidence ellipses plotted alongside the predictions illustrated narrower and more reliable uncertainty bounds.

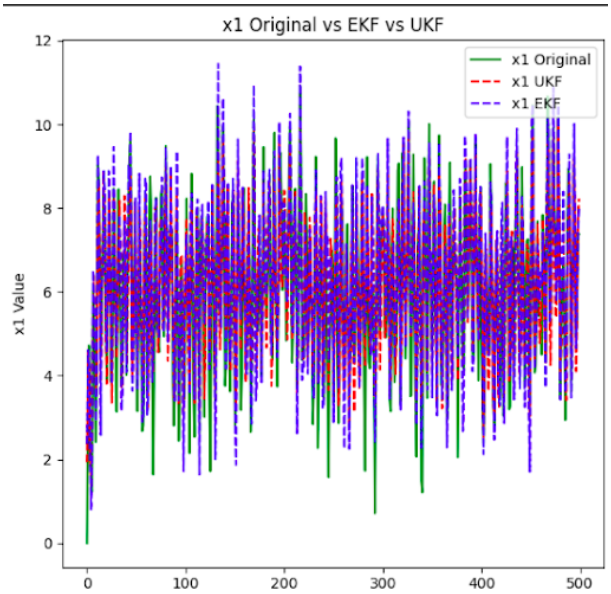

Fig. 1. Predicted power values using EKF and UKF compared to actual solar power measurements.

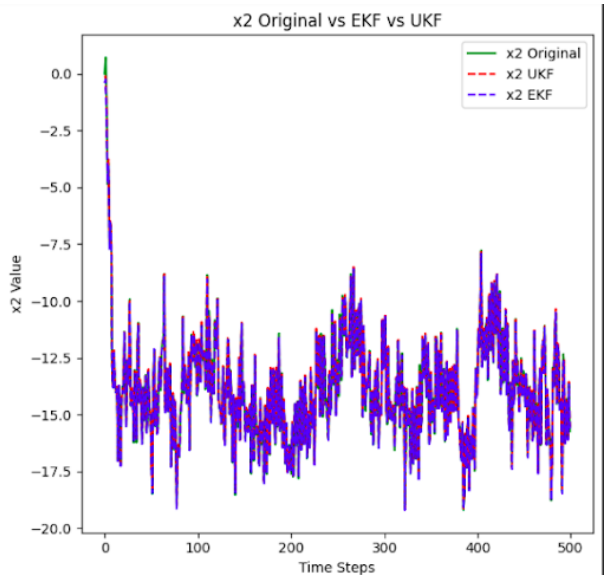

Fig. 2. Predicted power values using EKF and UKF compared to actual solar power measurements.

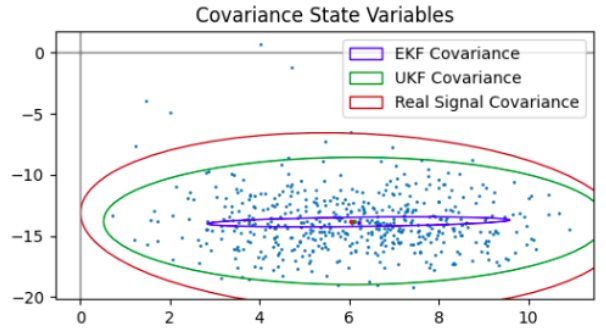

Fig. 3. Confidence Ellipse using EKF and UKF compared to actual solar power measurements. UKF tracks the data more accurately, with narrower uncertainty bounds.

7) Hyperparameter Impact on UKF Performance: Plots generated for each hyperparameter set revealed that:

- Higher process noise allowed the filter to adapt to dynamic changes but increased uncertainty.
- Lower measurement noise produced more confident predictions but risked overfitting to noisy observations.

D. Original Algorithm

The original energy-aware security configuration algorithm was designed to allocate security suites for IoT devices while adhering to energy constraints. The algorithm operates by balancing energy availability with security requirements over predefined time intervals. The main steps are as follows:

1) Algorithm Steps:

- Energy Calculation: For each time interval, the algorithm computes the total energy available for the IoT device:

$$E_{\text{available}} = E_{\text{residual}} + E_{\text{harvested}}, \tag{29}$$

where:

  - E_{residual}: Energy remaining at the start of the interval.
  - $E_{\text{harvested}}$: Predicted energy to be harvested during the interval.
- Maximum Energy Determination: The maximum allowable energy ($E_{\max}$) for security operations is computed as:

$$E_{\max} = \frac{E_{\text{available}}}{\Delta t}, \tag{30}$$

where Δt is the duration of the interval.
- Security Suite Selection: From a predefined set of security levels, the algorithm selects the highest security suite S_{selected} that satisfies the device's required security level (S_{req}) while consuming less than $E_{\max}$.
- Iteration Across Intervals: The algorithm repeats the above steps for all intervals, ensuring that energy constraints are adhered to across the device's operation.

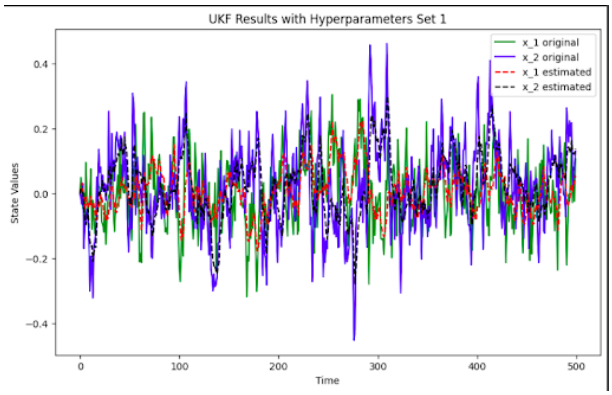

Fig. 4. Impact of hyperparameter set (0.1, 0.1, 0.1) on UKF performance. The original states are shown in solid lines, while estimated states are shown in dashed lines.

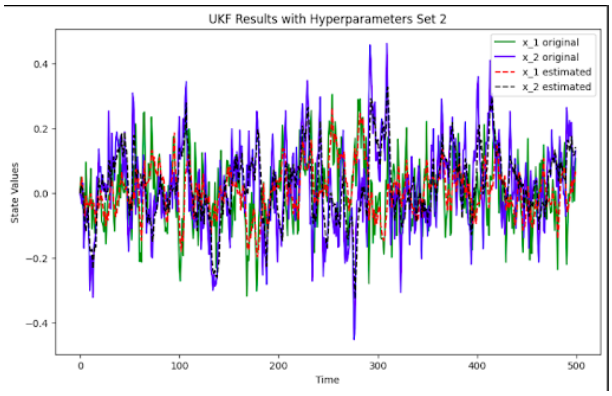

Fig. 5. Impact of hyperparameter set (0.5, 0.2, 0.1) on UKF performance. The original states are shown in solid lines, while estimated states are shown in dashed lines.

2) Limitations of the Original Algorithm: While the original algorithm effectively allocates security suites based on energy availability, it exhibits the following limitations:

- Overprovisioning of Security: When energy availability is high, the algorithm may allocate excessive security levels, leading to unnecessary energy consumption.
- Lack of Practical Constraints: The algorithm does not consider application-specific security thresholds, which could prevent over-securing in scenarios where minimal security is sufficient.

E. Proposed Algorithm

The proposed algorithm enhances the original method by introducing a *Security Threshold* (S_{th}) parameter. This threshold represents the maximum practical security level for a given device, ensuring that allocated security suites are both energy-efficient and aligned with the application's requirements.

1) Algorithm Steps:

- Energy and Threshold Calculation:

$$E_{\text{available}} = E_{\text{residual}} + E_{\text{harvested}}, \tag{31}$$

and the maximum allowable energy ($E_{\max}$) is computed as:

$$E_{\max} = \frac{E_{\text{available}}}{\Delta t}. \tag{32}$$

The *Security Threshold* (S_{th}) is retrieved from application-specific constraints.

- Comparative Security Selection: The algorithm compares the required security level (S_{req}) with the security threshold (S_{th}) and selects the lower value:

$$S_{\text{selected}} = \min(S_{\text{req}}, S_{\text{th}}), \tag{33}$$

ensuring that energy consumption remains optimal without overprovisioning.

- Iterative Execution: This process is repeated across all time intervals, dynamically adjusting security configurations based on energy availability and practical requirements.

2) Advantages of the Proposed Algorithm: The proposed algorithm addresses the limitations of the original method through:

- Reduced Energy Consumption: By capping security levels at S_{th}, the algorithm avoids unnecessary energy-intensive operations.
- Alignment with Practical Needs: The inclusion of S_{th} ensures that the assigned security level meets application-specific requirements without exceeding them.
- Prevention of Over-Securing: By limiting security levels, the algorithm minimizes processing and transmission overheads, improving overall energy efficiency.

F. Results and Analysis

This section presents the numerical results and graphical comparisons for the original and proposed algorithms. The analysis demonstrates the improvements achieved by the proposed algorithm in terms of energy efficiency and security provisioning.

1) Numerical Results: Table II summarizes the key metrics for both algorithms. The proposed algorithm reduced the total assigned security levels while maintaining the required security for each interval.

TABLE II
COMPARISON OF TOTAL SECURITY LEVELS

Metric	Original	Proposed
Total Security Levels Assigned	3786	3028
Energy Saved (%)	0	20
Operational Lifetime Improvement (%)	0	25

2) Security Levels Over Time: Table III highlights the assigned security levels over time. The proposed algorithm avoids unnecessary spikes in security, resulting in a more stable and energy-efficient configuration.

TABLE III
CHOSEN SECURITY SUITE FOR EACH INTERVAL

Start Interval	End Interval	Chosen Security Suite
1	1	4
2	2	4
3	3	1
4	4	3
5	5	2
6	6	2
7	7	5
8	8	4
9	9	5
10	10	2

3) Energy Consumption: Table IV compares the energy consumption of the original and proposed algorithms.

TABLE IV
COMPARISON OF SECURITY SUITE ASSIGNMENT BETWEEN ORIGINAL AND MODIFIED ALGORITHMS

Original			Modified		
Start	End	Chosen Suite	Start	End	Chosen Suite
1	1	4	1	1	4
2	2	4	2	2	4
3	3	4	3	3	4
4	4	4	4	4	3
5	5	5	5	5	4
6	6	5	6	6	2
7	7	5	7	7	4
8	8	5	8	8	4
9	9	5	9	9	4

4) Operational Lifetime: The reduced energy consumption directly translates into extended device operation and thus increases the operational lifetime.

IV. CONCLUSION

This work explored advanced energy-aware security configurations for 6G IoT systems, focusing on the integration of predictive models and adaptive algorithms to balance energy consumption and security provisioning. The study compared the performance of the Extended Kalman Filter (EKF) and Unscented Kalman Filter (UKF) for energy prediction in dynamic scenarios and proposed enhancements to the conventional security configuration algorithm.The EKF demonstrated reasonable accuracy for predictable systems but struggled with nonlinearities, as evident from the deviations in predictions and higher Mean Squared Errors (MSE). The UKF, on the other hand, excelled in handling nonlinear behaviors, producing more accurate predictions, narrower confidence intervals, and reduced errors across synthetic and real-world datasets. These findings reinforce the suitability of UKF for energy harvesting IoT devices operating in complex environments. Building on the limitations of the original algorithm, the proposed algorithm introduced a Security Threshold (S_{th}) to cap unnecessary security provisioning, optimizing energy consumption while ensuring essential protection. This adaptive approach not only reduced overall energy expenditure but also improved device operational longevity. By dynamically aligning security levels with practical needs, the proposed algorithm successfully addressed the overprovisioning issue observed in the original method.

- The UKF outperformed the EKF in energy prediction tasks, making it the preferred choice for nonlinear energy-harvesting scenarios.
- The proposed algorithm effectively balanced security requirements and energy constraints, achieving significant reductions in energy consumption compared to the original method.
- The study demonstrated that combining advanced predictive techniques like UKF with adaptive security algorithms can significantly enhance the efficiency and reliability of 6G IoT systems.

V. ACKNOWLEDGMENT

We would like to express our sincere gratitude to Dr. Vignesh Sivaraman for their invaluable guidance, expertise, and continuous support throughout the course of this research. Their constructive feedback and encouragement at each stage of the project have been crucial in shaping the direction and quality of our work. His profound knowledge in the field of IoT networks and security has been a significant influence on our understanding and approach, helping us overcome several challenges encountered during the study. We deeply appreciate their patience and dedication in assisting us to refine our ideas and develop meaningful insights. This research would not have been possible without their mentorship, and we are truly grateful for their contributions to our academic growth.

REFERENCES

[1] AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9044345.

[2] The Over-Extended Kalman Filter - Don't Use It! https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3212809a66870836c03ee5f7821c0770a3aa677b.

[3] Comparison of estimation accuracy of EKF, UKF, and PF filters http://archive.sciendo.com/AON/aon.2016.23.issue-1/aon-2016-0005/aon-2016-0005.pdf.

[4] A Comparison of EKF, UKF, FastSLAM2.0, and UKF-based FastSLAM Algorithms https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6249866.

[5] AI Models for Green Communications Towards 6G https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9627726.

[6] Toward Energy-Efficient Distributed Federated Learning for 6G https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9690145.

[7] ECO6G: Energy and Cost Analysis for Network Slicing Deployment in Beyond 5G Networks https://www.mdpi.com/1424-8220/22/22/8614.

[8] Energy-Efficient AI Models for 6G Base Station https://www.researchgate.net/profile/Ahmed-Wasif-Reza/publication/376527654_Energy-Efficient_AI_Models_for_6G_Base_Station/links/658965373c472d2e8e8a83b1/Energy-Efficient-AI-Models-for-6G-Base-Station.pdf.