DCA-KEAE: A Dynamic Context-Aware Key Exchange and Adaptive Encryption Scheme for Secure RFID Systems

[†]Bernard Amoah, [§]Xiangyu Wang, [‡]Jian Zhang, [†]Shiwen Mao, [§]Senthilkumar CG Periaswamy, [§]Justin Patton
[†]Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849-5201, USA
[‡]Department of Electrical and Computer Engineering, Kennesaw State University, Kennesaw, GA 30144, USA
[§]RFID Lab, Auburn University, Auburn, AL 36849, USA
Email: {bza0066, xzw0042}@auburn.edu, {jianzhang, smao}@ieee.org, {szc0089, jbp0033}@auburn.edu

***Abstract*—In dense RFID systems, where numerous readers and tags operate simultaneously in close proximity, securing reader-to-reader communication is essential to prevent attacks such as eavesdropping and spoofing. Existing protocols focus primarily on reader-to-tag communication and use static security mechanisms that may be inadequate in dynamic conditions. We propose DCA-KEAE, a Dynamic Context-Aware Key Exchange and Adaptive Encryption framework for RFID systems. DCA-KEAE adapts security protocols in real-time based on factors such as reader proximity, system load, and threat levels: it employs lightweight symmetric keys for low-risk scenarios and escalates to stronger protocols like ECDH and AES-256 in high-risk environments. Evaluations with up to 10,000 readers show that DCA-KEAE reduces latency, optimizes encryption, and improves system throughput, offering a scalable and efficient solution for RFID networks, with applications extending to the Internet of Things (IoT), industrial automation, and smart grids.**

***Index Terms*—Elliptic Curve Diffie-Hellman (ECDH), Adaptive encryption, Symmetric key exchange, Context-awareness, Internet of Things (IoT), Wireless Sensor Networks (WSNs).**

I. Introduction

In the era of smart cities, Industry 4.0, and the Internet of Things (IoT), Radio Frequency Identification (RFID) systems have become indispensable for real-time tracking, identification, and data collection [1], [2]. From supply chain management and inventory control to healthcare and transportation, RFID has been widely deployed in environments that require continuous monitoring and communication between readers and tags. However, as RFID systems scale and become more integrated into critical infrastructures, they face increasingly complex challenges in ensuring secure communications. In dense environments where numerous RFID readers operate simultaneously, protocols like RFIDNet [3] have enhanced multi-reader coordination, but the security of reader-to-reader communication (RRC), as illustrated in Fig. 1, remains a significant concern.

However, traditional RFID security mechanisms, designed primarily for reader-tag communication, rely on static key exchange and encryption protocols that could be inadequate for the dynamic, resource-constrained settings of dense RFID deployments [4]. These environments are particularly susceptible to security threats: eavesdropping, spoofing, replay, and man-in-the-middle attacks. Moreover, static security protocols often overcompensate, leading to high overhead in low-risk situations or leaving the system vulnerable in unpredictable environments.

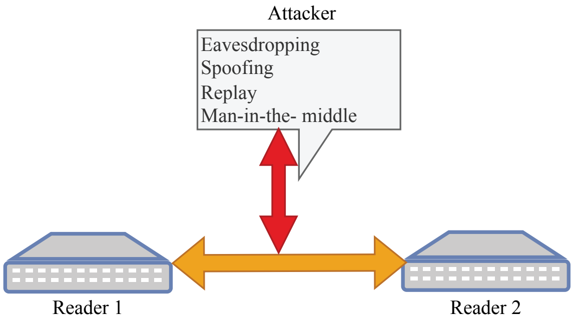


Fig. 1: Illustration of RRC and potential security threats.

Key exchange and encryption are fundamental to protecting communication within RFID systems, but they pose unique challenges in dense environments. RFID readers have limited computational power, and the need for real-time responsiveness requires security protocols that can adapt to varying environmental conditions without incurring excessive overhead. Static security protocols, e.g., AES-GCM-DH [5], ECC-AES-CCM [6], Hybrid PQC [7], and RSA-AES-CBC [8], often overcompensate for the worst-case scenario, leading to inefficiency, or underperform when faced with unexpected threats, leaving the system vulnerable and require high-performance platform. As RFID systems continue to be deployed in complex, dynamic environments, it is imperative to develop adaptive security frameworks that respond in real-time to contextual changes, such as reader density, location, proximity to sensitive assets, and communication patterns [9], [10].

This paper presents Dynamic Context-Aware Key Exchange, and Adaptive Encryption (DCA-KEAE), the security layer of RFIDNet [3]—a practical framework designed specifically for secure reader-to-reader communication in dense RFID environments. The technical novelty of DCA-KEAE lies in its ability to dynamically adjust both key exchange protocols and encryption strength based on real-time contextual parameters, such as reader proximity, system load, and risk levels. Unlike static security mechanisms, DCA-KEAE ensures both low-latency communication and strong security, making it ideal for dense RFID deployments. However, implementing this dynamic system poses several challenges. First, RFID readers have limited computational capacity and operate under strict real-time constraints, necessitating lightweight yet effective security protocols. Second, dynamically adapting encryption strength and key exchange processes to the current operational context requires designing an optimization model that balances security overhead and system performance. Finally, scaling the system to support thousands of readers without compromising security or performance adds a layer of considerable complexity. This paper addresses these challenges with DCA-KEAE to provide a scalable, efficient, and secure solution for RFID systems. While this framework is designed for RFID systems, its scalability and adaptability make it applicable to other areas, such as IoT, industrial automation, and smart grids, where dynamic security adjustments are crucial.

The key innovations of DCA-KEAE are as follows:

- *Dynamic Context-Aware Key Exchange:* Unlike static protocols, our adaptive key exchange mechanism dynamically selects the optimal protocol in real time based on the RFID network states, such as reader proximity and system load.
- *Adaptive Encryption Mechanism:* We introduce an encryption framework that adjusts strength based on risk assessment, using AES-128 for low-risk interactions and escalating to AES-256 or ECC for high-risk communications.
- *Scalability and Flexibility:* Our experimental results demonstrate DCA-KEAE's ability to scale across varying network sizes and configurations, maintaining high security and achieving significant improvements in key exchange latency, encryption efficiency, and system throughput, particularly in dense deployment scenarios.

The remainder of this paper is organized as follows: Section II discusses related work. Section III presents the system model and assumptions, while Section IV describes the proposed DCA-KEAE framework. Section V is on our experimental evaluation, and Section VI concludes the paper.

II. Related Work

While existing literature on RFID security predominantly focuses on reader-to-tag communication, adaptive and context-aware security schemes have been explored in other areas, such as IoT, Wireless Sensor Networks (WSNs), and general wireless communication systems. For example, frameworks such as LEAP+ [11] and LSS [12] for WSNs and DSF [13] for IoT have introduced dynamic security mechanisms for resource-constrained devices. However, these approaches primarily focus on access control or lightweight encryption for tag-based communication and do not account for the unique challenges of RRC communication in RFID systems. In IoT systems, context-aware security frameworks like SEF (Secure Encryption Framework) [14] dynamically adapt encryption strength based on environmental parameters such as network density and data sensitivity. Similarly, in WSNs, CANS (Context-Aware Network Security) [15] optimizes security protocols based on real-time risk assessments. However, these frameworks do not directly translate to RFID systems due to the high density of readers and real-time data exchange required between readers. Furthermore, they often rely on centralized control mechanisms. RFID readers, in contrast to IoT nodes, have more stringent latency requirements and lower computational capacities, especially in dense deployments where coordination among readers is critical for good system performance [3].

The proposed DCA-KEAE is a dynamic, context-aware [16] security framework specifically designed for secure RRC in RFID systems. Unlike adaptive security systems in IoT or WSNs, DCA-KEAE is tailored to address the unique constraints of RFID readers, including real-time responsiveness, low computational overhead, and the need for scalability in environments with up to 10,000 readers by employing decentralized, real-time adjustment mechanisms. Our framework not only adjusts encryption strength based on contextual factors but also dynamically selects the key exchange mechanism according to real-time risk assessments. This dual adaptation approach ensures a good balance between performance and security, making DCA-KEAE particularly well-suited for dense RFID environments and other applications, such as the Internet of Things (IoT) and industrial systems.

III. System Model and Assumptions

RFID readers, constrained by limited computational resources and low power capacity, require lightweight security protocols [17], [18] that do not sacrifice real-time responsiveness. This introduces a challenge in balancing security with performance, especially in dense deployments with thousands of readers. DCA-KEAE addresses this by dynamically adjusting both the key exchange protocol and encryption strength based on real-time contextual data such as proximity and system load.

A. RFID System Components

Let $\mathcal{R} = \{R_1, R_2, ..., R_N\}$ represent the set of N RFID readers, where each reader R_i can communicate with other readers $R_{j \neq i} \in \mathcal{R}$ over a wireless channel, exchanging control information (e.g., read rates, system status, and coordination signals). The communication between readers R_i and R_j at time t is denoted as $C_{i,j}(t)$. The communication process is subject to attacks (see Fig. 1) and, therefore, must be secured using appropriate encryption and key exchange protocols.

B. Assumptions

The system operates under the following assumptions:

- *Readers are Context-Aware*: Each reader R_i can gather real-time contextual information $\mathcal{C}(R_i, t)$ based on proximity sensors, location tracking, and system monitoring.
- *Communication Channels are Unsecured*: RRC is considered unsecured, requiring adaptive security mechanisms to ensure confidentiality and integrity.
- *Resource Is Constrained*: RFID readers can perform lightweight cryptographic operations in real-time, while RFID tags remain resource-constrained and offload cryptographic tasks to readers.

- *Adversary Capabilities*: Adversaries can attempt eavesdropping, spoofing, replay attacks, and MITM attacks, but cannot break modern cryptographic standards (e.g., AES-256, ECC) in real time.

C. Contextual Parameters

The system adapts its security protocols based on a set of *contextual parameters* defined for each reader R_i as:

$$\mathcal{C}(R_i, t) = \{L_i(t), P_i(t), S_i(t)\}, \tag{1}$$

where $L_i(t)$ is the *location* of reader R_i at time t (obtained using available sensors or localization techniques), $P_i(t)$ is the *proximity* or distance of reader R_i to the sensitive tag or neighboring reader that it is communicating with, which is modeled as an inverse square function of the signal strength received from neighboring readers, and $S_i(t)$ is the *system load* on reader R_i, representing the number of active communication sessions or the volume of data being processed. Each of these parameters is used to assess the *risk level* $\rho_i(t)$ of reader R_i, which is defined as:

$$\rho_i(t) = f(L_i(t), P_i(t), S_i(t)), \tag{2}$$

where $f(\cdot)$ is a risk function that maps the contextual parameters to a risk value, $\rho_i(t) \in [0, 1]$, where 0 represents the lowest risk and 1 represents the highest risk.

D. Security Threats

The DCA-KEAE framework addresses four main security threats in RFID systems: eavesdropping, spoofing, replay attacks, and man-in-the-middle (MITM) attacks. Each of these threats is modeled as a probabilistic event, where the likelihood of an attack depends on the risk level and the network environmental conditions.

1) Eavesdropping Probability: The probability that communication $C_{i,j}(t)$ between readers R_i and R_j is eavesdropped is given by:

$$P_{\text{eav}}(C_{i,j}(t)) = g(\rho_i(t), \text{dist}(R_i, R_j)), \tag{3}$$

where $\text{dist}(R_i, R_j)$ is the distance between R_i and R_j, and $g(\cdot)$ is a function that increases as $\rho_i(t)$ or the distance increases.

2) Spoofing Probability: The probability of a spoofing attack on reader R_i is modeled as:

$$P_{\text{spoof}}(R_i, t) = h(\rho_i(t), S_i(t)), \tag{4}$$

where $h(\cdot)$ increases with the load $S_i(t)$ and risk level $\rho_i(t)$.

3) Replay Attack Probability: The probability of a replay attack on the communication between readers is modeled as:

$$P_{\text{replay}}(C_{i,j}(t)) = r(\rho_i(t), \Delta t), \tag{5}$$

where Δt is the time delay between the original message and the replayed message. The function $r(\cdot)$ increases with larger Δt and higher risk levels $\rho_i(t)$.

4) Man-in-the-Middle Attack Probability: The probability of a man-in-the-middle (MITM) attack on communication $C_{i,j}(t)$ between readers R_i and R_j is given by:

$$P_{\text{mitm}}(C_{i,j}(t)) = k(\rho_i(t), \text{dist}(R_i, R_j)), \tag{6}$$

where $\text{dist}(R_i, R_j)$ is the distance between readers R_i and R_j, and $k(\cdot)$ is a function that increases with risk level $\rho_i(t)$ as well as the distance between the communicating readers.

E. Encryption and Key Exchange

Let $K_{i,j}(t)$ denote the *encryption key* used for communication between reader R_i and R_j at time t. The *key exchange protocol* is dynamically selected based on the context $\mathcal{C}(R_i, t)$. We define the *encryption strength* $E_{i,j}(t)$ as a function of the risk level using two threshold values α and β as:

$$E_{i,j}(t) = \begin{cases} \text{AES-128}, & \text{if } \rho_i(t) \le \alpha \\ \text{AES-256}, & \text{if } \alpha < \rho_i(t) \le \beta \\ \text{ECC}, & \text{if } \rho_i(t) > \beta. \end{cases} \tag{7}$$

These threshold values (typically $\alpha = 0.4$ and $\beta = 0.7$) are chosen based on empirical observations in typical RFID environments, allowing the system to maintain an effective balance between performance and security under varying risk conditions. For encryption strength, AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptography) are the widely used encryption methods. The system uses lightweight encryption (AES-128) when the risk level is low and stronger encryption (*ECC*) when the risk level is high.

For key exchange, we define the key exchange protocol $\mathcal{K}(R_i, t)$ as:

$$\mathcal{K}(R_i, t) = \begin{cases} \text{Symmetric Key}, & \text{if } \rho_i(t) \le \alpha \\ \text{Elliptic Curve Diffie-} & \\ \text{Hellman (ECDH)}, & \text{if } \rho_i(t) > \alpha. \end{cases} \tag{8}$$

Such an adaptive scheme ensures that a stronger key exchange protocol is employed in higher-risk scenarios, while a lightweight symmetric key exchange is used in low-risk settings to optimize performance.

F. Performance Optimization

The DCA-KEAE framework is designed to balance the trade-offs between security, computational overhead, and system performance. Thus, we formulated the optimization problem to minimize the overall cost function $\phi(x)$ as follows:

$$\begin{aligned} \min \quad & \phi(x) = w_1 \cdot O_E + w_2 \cdot S^{-1} + w_3 \cdot E^{-1} + w_4 \cdot C && (9) \\ \text{s.t.:} \quad & S_i \ge S_{\text{min}} \quad (\textit{Security constraint}) && (10) \\ & E_i \le E_{\text{max}} \quad (\textit{Resource constraint}) && (11) \\ & C_i \ge C_{\text{min}} \quad (\textit{Context constraint}) && (12) \\ & K_i \le K_{\text{max}}, \quad (\textit{Key Exchange Constraint}) && (13) \end{aligned}$$

where O_E represents the encryption overhead, S is the security strength, E is the resource consumption (e.g., CPU cycles, memory, etc.), and C represents the context-awareness of the system. The weights $\{w_1, w_2, w_3, w_4\}$ were determined based on an empirical study conducted across several real-world RFID deployments. For example, in critical infrastructure scenarios (e.g., medical facilities), we prioritize security strength by assigning $\{w_1 = 0.2, w_2 = 0.5\}$, and reducing the emphasis on overhead minimization. In contrast, for retail environments, overhead reduction is prioritized with $\{w_1 = 0.4, w_2 = 0.2\}$, ensuring low latency with adequate security.

IV. The Proposed DCA-KEAE Framework

A. *System Overview*

The DCA-KEAE system is designed to ensure secure communication between RFID readers by continuously evaluating the surrounding context and dynamically adjusting both the key exchange protocol and encryption strength. The system operates in the following phases as depicted in Fig. 2.

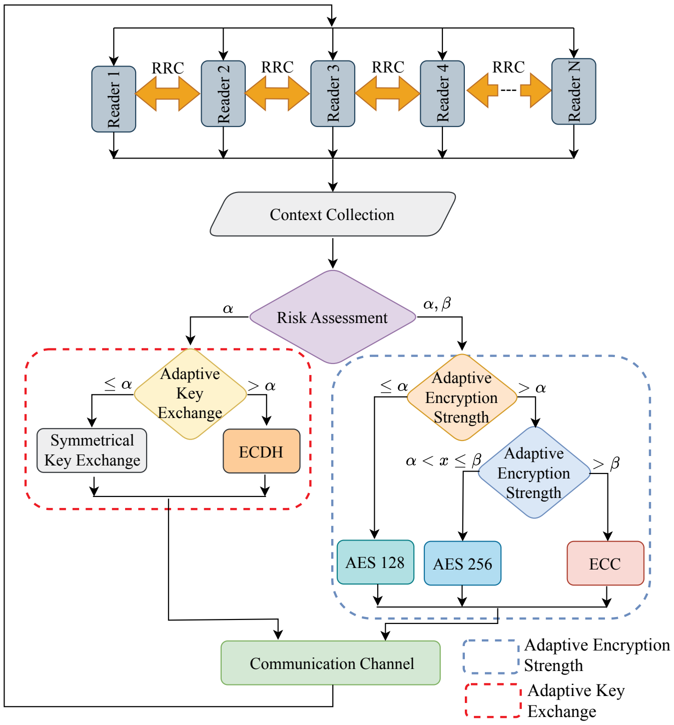


Fig. 2: DCA-KEAE System Architecture — This illustrates the adaptive key exchange and encryption mechanisms, risk assessment, and context-aware security adjustments for secure communication between RFID readers.

1) *Context Collection and Risk Analysis*: Each RFID reader periodically gathers *contextual information* about its operational environment, including its location, proximity to other readers, network load, and the current security threat level and computes the risk value $\rho_i(t)$.
2) *Adaptive Key Exchange*: Based on the contextual analysis, the system dynamically selects the appropriate *key exchange protocol*, such as lightweight (e.g., symmetric key) and more secure (e.g., ECDH) options as needed.
3) *Encryption Strength Adjustment*: Once a secure communication session is established, the encryption algorithm is chosen based on the *real-time risk level*, ensuring that higher-risk scenarios receive stronger encryption, while low-risk environments maintain minimal overhead.

B. *Context Collection and Risk Assessment*

In DCA-KEAE, each RFID reader R_i continuously collects *contextual information* $\mathcal{C}(R_i, t)$, which influences its security decisions. The contextual parameters $\mathcal{C}(R_i, t)$ are defined by (1). The risk level $\rho_i(t)$ is computed using (2), which then guides the selection of the key exchange protocol and encryption strength. For instance, in a scenario where reader proximity $P_i(t)$ increases due to a crowded deployment (e.g., in a warehouse), the risk function $\rho_i(t)$ rapidly approaches 0.75, causing the system to switch from symmetric key encryption to ECDH and AES-256. In contrast, when proximity is low and the system load remains within thresholds, $\rho_i(t)$ remains below 0.4, allowing the system to use lightweight AES-128 encryption for efficiency.

C. *Adaptive Key Exchange Mechanism*

Once the risk level $\rho_i(t)$ is computed, the system dynamically selects the appropriate key exchange protocol. The key exchange selection algorithm follows (8). Here, α is the threshold risk level that determines when a more secure (but resource-intensive) key exchange protocol, such as ECDH, is needed. This adaptive key exchange mechanism allows DCA-KEAE to adjust its security protocols without over-burdening the system in low-risk scenarios. The flexibility in switching between symmetric key exchange and ECDH ensures that the protocol can scale to different network sizes and configurations while maintaining optimal performance and security.

D. *Encryption Strength Adaptation*

Following the key exchange, DCA-KEAE adjusts the encryption strength based on the real-time context. The encryption strength $E_{i,j}(t)$ is selected from a set of available algorithms defined in (7). One of the key design challenges is to ensure that the system could adapt its security protocols in real time without introducing latency that could degrade system performance. The lightweight encryption algorithm, AES-128, is chosen to balance security and computational overhead in low-risk situations, while ECC is employed for high- and critical-risk environments despite its higher computational demands. The dynamic nature of the DCA-KEAE framework ensures that such balance is achieved without overloading the RFID readers.

In extreme, high-risk scenarios, such as targeted MITM attacks on sensitive tags, DCA-KEAE escalates to ECC and AES-256 encryption. However, even with these measures, some scenarios may require additional layers of security. For example, in high-security environments like military installations, where the likelihood of sophisticated attacks is elevated, DCA-KEAE can be combined with Intrusion Detection Systems (IDS) that detect anomalous behavior in the communication channels and multi-factor authentication protocols for reader access control. This hybrid approach ensures that even in extremely high-risk conditions, the RFID system maintains high security without compromising performance.

V. Experimental Study and Discussions

A. *Simulation Setup*

Simulations are carried out using MATLAB, chosen for its robust capabilities in modeling and analyzing communication systems. The RFID network is simulated under different configurations of readers and tags, as well as varying levels of system load, reader density, and proximity to sensitive assets. The simulation environment is configured to model real-time RFID system behavior, including communication between readers and dynamic adjustments in security protocols based on context-aware data. The setup is focused on evaluating DCA-KEAE's ability to: (i) dynamically adjust key exchange protocols and encryption strength; (ii) balance system performance (throughput, latency, overhead) and security robustness; and (iii) scale efficiently across a range of network sizes.

To evaluate the scalability and performance of DCA-KEAE, we simulated networks with varying numbers of RFID readers (from 100 to 10,000) and tags (up to 1,000,000). These parameters are chosen to reflect both small-scale and large-scale RFID deployments in real-world scenarios. The number of readers per square meter is varied to create low-density (5 readers/m²), medium-density (10 readers/m²), and high-density (20 readers/m²) environments. The Poisson distribution is used to model tag reads as it reflects real-world traffic patterns, where read requests occur sporadically and unpredictably. There are two types of tags: normal and sensitive. Sensitive tags ($\sigma_T = 1$), such as medical devices or critical infrastructure components, require stronger encryption due to the higher risk of eavesdropping or tampering. Normal tags ($\sigma_T = 0$) are assigned lightweight encryption to reduce computational overhead, reflecting the lower security requirements of less critical assets. Such classification allows us to evaluate DCA-KEAE's ability to dynamically adjust encryption strength based on the contextual importance of tags.

B. Performance Metrics

We evaluate DCA-KEAE based on the following metrics: *(i) Key Exchange Latency ($T_{KE}(R_i, R_j)$)*, the time taken to establish a secure communication channel between readers R_i and R_j; *(ii) Encryption Overhead (O_E)* is the computational cost of encryption relative to no encryption. For a given encryption strength E, overhead is defined as:

$$O_E = \text{Time with encryption}/\text{Time without encryption}. \quad (14)$$

We measure overhead for three encryption levels: AES-128, AES-256, and ECC. *(iii) Throughput (τ)* is defined as the number of successful RRCs per second:

$$\tau = N_{\text{successful reads}}/T_{\text{experiment}}. \quad (15)$$

Throughput measures the system's ability to maintain performance as reader density and system load increase. *(iv) Security Strength ($\mathcal{S}$)* measures the system's resilience to attacks. We simulate *eavesdropping, spoofing, replay*, and *man-in-the-middle* attacks and measure the percentage of attacks successfully thwarted by each protocol.

$$\mathcal{S} = N_{\text{attacks thwarted}}/N_{\text{total attacks}}. \quad (16)$$

(v) Energy efficiency (η) is the amount of useful work done per unit of energy consumed per communication E_{comm}, as

$$\eta = \tau/E_{\text{comm}}. \quad (17)$$

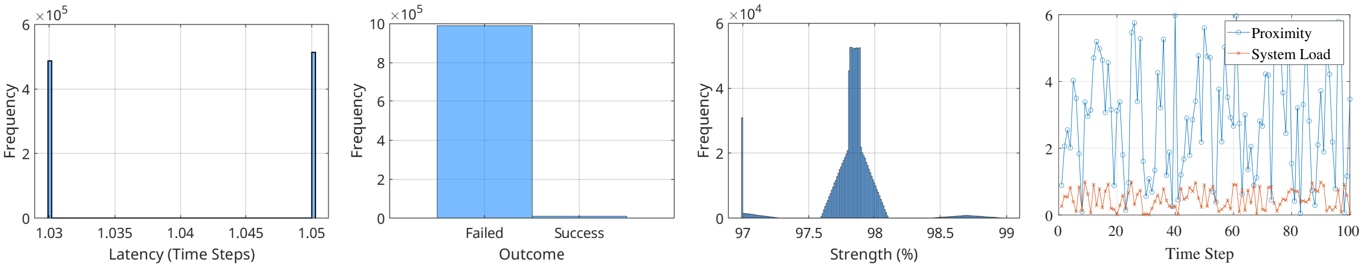
C. Experimental Results and Discussions

As shown in Fig. 3, DCA-KEAE consistently demonstrates low key exchange latency, $T_{KE}(R_i, R_j)$, across various risk levels (Fig. 3(a)), with values staying below 1.05×-time steps (averaging 1.0423×) even in high-risk scenarios, indicating the framework is well-optimized to balance security without introducing significant delays. Fig. 3(b) illustrates the success rate of attacks over time as the system adjusts to higher-risk conditions. Only 0.14271% of the attacks are successful. Fig. 3(c) affirms that DCA-KEAE not only scales efficiently but also maintains strong security, thwarting nearly 98% of attacks while preserving low latency and high throughput. Fig. 3(d) shows the fluctuations in proximity and system load (within 1 unit per reader) over time. DCA-KEAE dynamically adjusts encryption and key exchange protocols based on these varying conditions, ensuring minimal latency and maintaining strong security even as environmental factors shift. This dynamic adjustment allows the system to maintain optimal performance despite high variability in real-time conditions.

When compared to static security protocols such as AES-GCM-DH, RSA-AES-CBC, ECC-AES-CCM, and Hybrid PQC in real time avalanche of unexpected threat conditions as shown in Table I, DCA-KEAE outperforms them across key performance metrics: DCA-KEAE achieves the lowest latency (1.0299 time steps), highest security strength (98.11%), and lowest attack success rate (1.03%), while maintaining the highest throughput (97,973.48 reads/s) and low energy consumption (0.60 mJ). DCA-KEAE's energy efficiency is primarily due to its ability to scale encryption strength down to AES-128 in low-risk scenarios, where less resources are required. This contrasts with static protocols like RSA-AES-CBC, which maintain a higher baseline energy consumption regardless of the risk level. DCA-KEAE also minimizes encryption overhead (2.99%) while offering superior anomaly detection capabilities, particularly in critical risk scenarios, thanks to its adaptive risk assessment framework.

As shown in Table II, DCA-KEAE marginally outperforms Hybrid PQC in detecting abnormalities across varying risk scenarios. This is attributed to DCA-KEAE's dynamic adjustment of key exchange and encryption protocols in real time, allowing it to respond more effectively to sudden changes in proximity, system load, or potential security threats. Hybrid PQC, while being robust, uses static mechanisms and lacks such real-time adaptability, leading to slightly lower detection rates in high-risk scenarios.

Discussions: The experimental results verify that DCA-KEAE provides significant improvements in key exchange latency, encryption overhead, and system throughput compared to fixed-security systems. The adaptive nature of DCA-KEAE enables it to adjust security level based on real-time risk assessment, balancing the trade-off between security and performance. The results show that DCA-KEAE is well-suited for dense RFID deployments with varying system loads and tag sensitivities. The framework effectively reduces computational costs while maintaining robust security, making it a scalable and efficient



(a) Key exchange latency

(b) Attack success rate

(c) Security strength

(d) Proximity and system load over time

Fig. 3: Mean Key Performance Metrics for DCA-KEAE Framework across risk levels for 10,000 readers and 1,000,000 tags for 1000 time steps. (a) Key exchange latency remains low even in high-risk scenarios (which required ECDH), maintaining sub-1.05 time steps and sub-1.03 time steps for low- and medium-risk scenarios (which used symmetric keys) (b) Attack success rate decreases as the system adapts, with a maximum rate ($< 1\%$) even in high-risk conditions. (c) Security strength, indicating the average percentage of attacks thwarted, approaches 98%: for high-risk scenarios, the security strength averaged approx. 97% and an average of nearly 98.75% for low- and medium-risk scenarios. (d) Proximity and system load fluctuate over time (100 time steps shown for readability), but DCA-KEAE dynamically adjusts security protocols to maintain system load within 1 unit under varying environmental conditions.

TABLE I: Performance comparison (Mean) of DCA-KEAE with other static security protocols under real-time avalanche of abnormal conditions (unexpected threats) for 10,000 readers and 1,000,000 tags over 100,000 time steps.

Protocol	**Avg Latency (time steps)**	**Avg Security Strength (%)**	**Attack Success Rate (%)**	**Throughput (reads/s)**	**Energy Consumption per communication (mJ)**	**Encryption Overhead (%)**
AES-GCM-DH [5]	1.0350	94.00	1.11	97,893.08	0.60	2.01
ECC-AES-CCM [6]	1.0550	96.00	1.07	97,933.78	1.50	5.10
Hybrid PQC [7]	1.0299	98.11	1.03	97,968.58	0.60	2.99
RSA-AES-CBC [8]	1.0450	89.00	1.21	97,807.16	0.70	3.03
DCA-KEAE [Ours]	**1.0299**	**98.11**	**1.03**	**97,973.48**	**0.60**	**2.99**

TABLE II: Comparison of abnormality detection in various risk scenarios for DCA-KEAE and HYBRID PQC over 100,000 time steps.

	Risk Scenario			
Protocol	**CRITICAL**	**HIGH**	**MEDIUM**	**LOW**
DCA_KEAE [proposed]	**116770**	**120916**	**124349**	**140960**
HYBRID_PQC	116216	120230	123858	140740

solution for real-world RFID applications.

VI. Conclusions

This paper presented DCA-KEAE, a dynamic context-aware security framework for securing RRC in dense RFID systems. By dynamically adjusting key exchange and encryption strength based on real-time factors such as proximity and system load, DCA-KEAE improves key exchange latency, reduces encryption overhead, and scales efficiently in large networks. Beyond RFID, the framework has broader applications in IoT, industrial automation, and smart grids, where real-time security adjustments are essential. Future work will focus on energy optimization, machine learning integration for enhanced risk assessment, and applying the framework to critical infrastructure sectors.

Acknowledgments: This work is supported in part by the NSF under Grants CCSS-2245607 and CCSS-2245608.

References

[1] Y. Xiao, et al., “Radio frequency identification: Technologies, applications, and research issues,” *Wiley Wireless Commun. Mobile Comput.*, vol. 7, no. 4, pp. 457–472, July 2007.

[2] X. Wang, J. Zhang, Z. Yu, S. Mao, S. Periaswamy, and J. Patton, “On remote temperature sensing using commercial UHF RFID tags,” *IEEE Internet of Things J.*, vol. 6, no. 6, pp. 10 715–10 727, Dec. 2019.

[3] B. Amoah, X. Wang, J. Zhang, S. Mao, S. C. Periaswamy, and J. Patton, “RFIDNet: Protocol for effective multiple RFID readers collaboration,” in *Proc. IEEE ICC 2025*, Montreal, Canada, June 2025.

[4] M. A. Iqbal, “Distributed security paradigm for resource-constrained wireless sensors in the context of internet of things (IoT),” Ph.D. dissertation, University of Louisiana at Lafayette, Lafayette, LA, 2017.

[5] D. A. McGrew and S. D. Frankel, “AES Galois Counter Mode (GCM) Cipher Suites for TLS,” IETF RFC 5288, 2008.

[6] D. McGrew, J. Salowey, and A. Choudhury, “AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS,” IETF RFC 7251, 2014.

[7] E. Crockett, C. Paquin, and D. Stebila, “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH,” in *Proc. NIST 2nd PQC Standardization Conf.*, Santa Barbara, CA, Aug. 2019.

[8] S. Frankel, H. Herbert, P. Kelly, and R. Glenn, “The AES-CBC Cipher Algorithm and Its Use with IPsec,” IETF RFC 3602, 2003.

[9] O. Vermesan, *et al.*, “Internet of things beyond the hype: Research, innovation and deployment,” in *Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets*. River Publishers, 2022, pp. 15–118.

[10] E. Batista, et al., “Sensors for context-aware smart healthcare: A security perspective,” *MDPI Sensors*, vol. 21, no. 20, p. 6886, Oct. 2021.

[11] S. Zhu, S. Setia, and S. Jajodia, “LEAP+: Efficient security mechanisms for large-scale distributed sensor networks,” *ACM Trans. Sen. Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[12] G. T. Amariucai, C. Bergman, and Y. Guan, “An automatic, time-based, secure pairing protocol for passive RFID,” in *Proc. RFIDSec 2011*, Amherst, MA, June 2012, pp. 108–126.

[13] H. Saxena, et al., “DSF–a distributed security framework for heterogeneous wireless sensor networks,” in *Proc. IEEE MILCOM’10*, San Jose, CA, Oct.-Nov. 2010, pp. 1836–1843.

[14] Y. Bharadwaj and S. Chakraverty, “A design pattern for symmetric encryption,” in *Proc. 2013 Int. Conf. Control, Computing, Communication and Materials (ICCCCM)*, Allahabad, India, Aug. 2013, pp. 1–6.

[15] J. Pieprzyk, A.-R. Sadeghi, and M. Manulis, Eds., *Proc. Cryptology and Network Security: 11th Int. Conf., CANS 2012, Darmstadt, Germany, Dec. 2012*. Springer Science & Business Media, 2012, vol. 7712.

[16] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, and L. Khoukhi, “A secure multipath reactive protocol for routing in iot and hanets,” *Ad Hoc Networks*, vol. 103, p. 102118, 2020.

[17] X. Zhu, et al., “Enabling intelligent connectivity: A survey of secure ISAC in 6G networks,” *IEEE Commun. Surv. Tutor.*, pp. 1–1, 2024.

[18] T. Liu, et al., “Blockchain and trusted hardware-enabled data scheduling for edge learning in wireless iiot,” *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34 229–34 242, 2024.