Lightweight Authentication For Resource-Constrained IoT Devices

Adrian Necaj[1], Ryan Cheevers-Brown[2], Kenneth Anderson[3], and Cipriana Sorenson[4]

[1]Department Of Cybersecurity, Rochester Institute of Technology

April 29, 2024

Abstract

The rapid proliferation of Internet of Things (IoT) devices in various sectors, including smart homes, healthcare, and industrial automation, underscores the importance of robust security mechanisms. Among these, authentication is critical, as it ensures that only authorized devices and users can access the network and its data. However, many IoT devices face significant constraints in terms of processing power, memory, and energy availability, which complicates the implementation of traditional, resource-intensive authentication protocols. This paper explores the development and optimization of lightweight authentication protocols tailored for resource-constrained IoT devices.

We commence with a comparative analysis of existing authentication solutions, examining their applicability and limitations in the context of IoT. We particularly assess the protocols presented by Lara et al. (2020) [1] , who propose a lightweight authentication mechanism suitable for low-cost IoT devices, and Athanere and Thakur (2023) [2], who introduce a hierarchical multi-authority access control scheme for distributed IoT environments. Both approaches reflect a shift towards minimizing computational and communication overhead, which is critical in IoT settings.

Our methodology involves both theoretical evaluation and empirical testing within simulated IoT environments to gauge the performance, security, and resource consumption of proposed authentication schemes. We specifically look into dynamic key management and streamlined public key infrastructures as potential solutions to enhance IoT security without imposing significant resource burdens.

Preliminary findings suggest that dynamic key management significantly mitigates the risk of key compromise while reducing resource usage, echoing the benefits noted in recent studies by King and Awad (2015). Additionally, the adaptation of lightweight cryptographic algorithms, as discussed by Fang, Ruan, and Zuo (unknown publication year), indicates potential for further reducing power consumption without compromising security integrity.

The paper concludes with a discussion on the practical implications of these lightweight authentication protocols, recommending strategies for integration into existing and future IoT frameworks. The ultimate aim is to foster a more secure IoT ecosystem that accommodates the limitations of resource-constrained devices while maintaining high security standards.

Keywords

IoT Security, Lightweight Authentication, Resource-Constrained Devices, Dynamic Key Management, Public Key Infrastructure

1 Introduction

The ever so increasing adoption of the Internet of Thing (IoT) devices across diverse sectors underscores a pivotal shift in how digital systems interact with the physical world, driving efficiency and innovation in areas ranging from smart homes to industrial automation. Yet, as IoT devices increasingly permeate critical infrastructures, the necessity for robust and efficient security protocols, particularly authentication mechanisms, becomes paramount. Authentication in IoT ensures that interactions and data exchanges are conducted between verified devices and users, safeguarding sensitive information and system operations against unauthorized access.

Research Problem

Despite the critical role of authentication, many IoT devices operate under significant constraints including limited processing power, memory capacity, and energy resources. These limitations pose unique challenges for

implementing traditional security protocols, which often require substantial computational overhead. Existing solutions, as demonstrated in the work by Xue Li et al. [3], reveal that conventional authentication methods—reliant on complex cryptographic processes—are impractical for such resource-constrained environments. These methods expose devices to various security risks, including offline password guessing and impersonation attacks, which can severely compromise the integrity of IoT systems.

Current Authentication Challenges

Traditional authentication schemes are typically designed for environments with abundant computational and energy resources. For IoT devices, however, these schemes become untenable, leading to inefficiencies and increased vulnerability to attacks. The study by Xue Li et al [3]. highlights the inefficacy of elliptic curve cryptography and bilinear pairing in constrained environments, underpinning the urgent need for tailored authentication solutions that align with the operational realities of IoT devices.

Proposed Solution

Addressing these challenges, this paper proposes an innovative lightweight authentication protocol tailored specifically for resource-constrained IoT devices in cyber-physical systems. This protocol leverages hash functions and XOR operations to provide a secure, efficient authentication process. Compared to traditional methods, this new protocol minimizes computational demands and power consumption, thereby enhancing the feasibility of robust security measures in constrained environments. The protocol's design not only mitigates common security threats but also supports user anonymity and traceability, crucial for maintaining privacy and security in IoT interactions.

Significance and Impact

The development of lightweight, scalable, and secure authentication protocols is crucial for the widespread adoption and safe operation of IoT technologies. This research contributes significantly to cybersecurity by providing a practical solution that respects the inherent limitations of IoT devices while fortifying them against sophisticated cyber threats. By enabling secure and efficient authentication, the proposed protocol ensures the sustainable and safe expansion of IoT networks, particularly in critical infrastructures where security and operational efficiency are paramount.

2 Background & Significance

Core Research Problem

The rapid integration of Internet of Things (IoT) devices into critical and everyday environments poses significant security challenges, primarily in authentication—the process of validating device and user identities within a network. Traditional authentication methods, developed for systems with substantial computational resources, are largely inapplicable to IoT devices. These devices often operate under severe constraints in processing power, memory, and energy. This discrepancy introduces vulnerabilities that could be exploited to compromise device functionality and data integrity. The core problem, therefore, is developing an authentication protocol that is both secure and efficient enough to operate within these constraints.

Purpose and Rationale of the Study

This study addresses the urgent need for authentication protocols that can secure IoT devices without exceeding their limited computational capabilities. The importance of this research lies in its potential to significantly enhance the security of IoT networks, crucial for their safe and effective operation in environments ranging from healthcare to industrial control systems. Without secure and efficient authentication protocols, these devices are at risk of security breaches that can lead to data theft, device manipulation, and broader network compromises.

Major Issues and Research Questions

The major issues addressed by this research include:

1. The inefficacy of traditional cryptographic methods in resource-constrained IoT environments due to their high computational and energy demands.
2. The vulnerability of current lightweight authentication methods to various security threats, including impersonation and replay attacks.
3. The lack of scalable and revocable authentication solutions that can be dynamically adapted as network configurations and security requirements evolve.

The research questions this study aims to answer are:

- How can authentication protocols be optimized to minimize computational and energy demands while maintaining high security?
- What methods can ensure the scalability and revocability of authentication schemes in dynamic IoT environments?

Methodology and Sources

Our methodology will include a comparative analysis of existing authentication protocols, both traditional and IoT-specific, to identify their strengths and limitations. This analysis will be supplemented by empirical testing of proposed lightweight authentication schemes in simulated IoT environments. Key sources will include recent

studies and benchmarks within the field, such as those by Lara et al. (2020) [1] and Xue Li et al. [3], which provide foundational insights into current practices and emerging needs in IoT security.

Boundaries of the Research

The proposed research will focus on the development and testing of authentication protocols specifically designed for low-power IoT devices. It will not cover the broader aspects of network security such as intrusion detection systems or data encryption methods beyond their relation to authentication. Additionally, while the study will consider the scalability of authentication solutions, it will primarily concentrate on scenarios typical to small and medium-scale IoT implementations.

Definitions of Key Concepts

- **IoT (Internet of Things):** A network of physical objects—devices, vehicles, appliances—that use sensors and APIs to connect and exchange data over the Internet.
- **Authentication:** The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in that system.
- **Resource-Constrained Devices:** Devices with limited computing power, memory, and energy resources, often used in the context of IoT.

3 Related Work

The field of IoT security, and in more particular, authentication for resource-constrained devices, has seen significant scholarly attention, highlighting a range of approaches and identifying persistent challenges and gaps. This section reviews seminal works and recent studies that lay the groundwork for our proposed research, examining their methodologies, findings, and the questions they leave unanswered.

Review of Existing Authentication Schemes

Lara et al. (2020) [1] and Athanere and Thakur (2023) [2] provide comprehensive reviews of current lightweight authentication mechanisms tailored to IoT devices. Lara et al [1]. focus on protocols that minimize computational requirements and enhance power efficiency, suitable for devices with limited battery life and processing power. Athanere and Thakur [2], on the other hand, explore multi-authority access control schemes that offer scalability and revocability, crucial for dynamic IoT environments. Both studies, however, primarily concentrate on static environments and do not fully address the challenges posed by highly dynamic networks where device configurations and connectivity statuses frequently change.

Xue Li et al [3]. delve into the specifics of a revocable lightweight authentication scheme designed for cyber-physical systems, emphasizing the balance between security and computational efficiency. Their work demonstrates improved resistance to common IoT security threats, such as impersonation and replay attacks, through the use of hash functions and XOR operations. While their protocol marks a significant advancement in terms of security features, it requires a secure initial setup environment, which may not always be feasible in practical, large-scale deployments.

Gaps in Current Research

A recurrent theme in these studies is the need for authentication protocols that are not only efficient and secure but also adaptable to varying operational demands and scalable across different IoT ecosystems. Most existing research, including the aforementioned studies, provides solutions that are somewhat rigid, lacking the flexibility to adjust as network parameters and security requirements evolve. Additionally, there is a noticeable gap in addressing the integration of new and legacy devices within the same network, a common scenario in industrial IoT applications.

Methodological Insights

The methodological approaches in these works often involve empirical testing and simulation models to evaluate the performance and security of proposed solutions. However, there is a need for more comprehensive real-world testing scenarios that can better mimic the unpredictable and heterogeneous nature of IoT networks. Furthermore, there is limited discussion on the user and administrative aspects of authentication, such as ease of deployment and management, which are critical for the adoption and sustainability of any security solution.

Open Questions and Research Opportunities

The review of related literature underscores several open questions:

- How can authentication protocols dynamically adapt to changes within IoT networks without requiring complete reconfiguration?
- What strategies can be employed to seamlessly integrate new authentication protocols with existing infrastructure, particularly in mixed environments of old and new IoT devices?
- How can the user and administrative burden of managing IoT authentication be minimized to promote wider acceptance and use?

Conclusion of Related Work

The related work highlights the progress made in developing lightweight authentication protocols for IoT devices and underscores the complexities and limitations

of current approaches. By identifying these gaps and questions, our study aims to contribute a novel solution that addresses not only the technical challenges but also the practical deployment and management concerns that have been somewhat neglected in previous research.

Algorithm 1: Setup

Input: λ

Output: $F_p, E/F_p, G, P, \kappa_{pub}, H_x(\cdot), \varpi$

1 Given a security parameter 1^{λ}

2 KGC selects a λ-bit prime p and generates $\{F_p, E/F_p, G, P\}$ according to the elliptic curve related contents

3 KGC selects a random number $\varpi \in Z_q^*$, and calculates the system public key $\kappa_{pub} = \varpi P$

4 Maintains an identity time list $Table_{time-ID}$

5 Defines one-way hash function $H_x(\cdot), x = 0, \cdots, 5$

6 **Return** system parameters $F_p, E/F_p, G, P, \kappa_{pub}, H_x(\cdot)$ and system master key ϖ

Figure 1: Algorithm 1 : Set Up

4 Research Problems and Design Goals

Targeted Research Problem

The primary research problem addressed by this study is the development of a secure, efficient, and scalable authentication protocol for IoT devices that are severely constrained in terms of computational resources, power, and memory. Current authentication methods either compromise security to save resources or require capabilities beyond what these devices can provide, leading to increased vulnerability to cyber threats.

Design Goals

To address this problem, the research will focus on several key design goals:

1. **Efficiency:** Develop a protocol that minimizes computational and power requirements to suit the limited capabilities of IoT devices.

2. **Security:** Ensure that the protocol provides top of the line security measures, including resistance to reoccurring attacks such as impersonation, replay, and man-in-the-middle attacks.

3. **Scalability:** The solution should be applicable to a wide range of IoT environments, from small home networks to large industrial systems, and be able to manage the dynamics of device addition and removal seamlessly.

4. **User and Administrative Simplicity:** Aim for a design that is easy to implement and manage, reducing the burden on users and administrators, which can further promote more widespread adoption.

5. **Generalization of Application:** The solution should be adaptable to varying types of IoT devices, networks, and environments, each with differing needs and restrictions.

5 Research Method

The primary methodological approach of this study is a comprehensive literature review aimed at understanding and addressing the core issue of developing secure, efficient, and scalable authentication protocols for resource-constrained IoT devices. This review is designed to synthesize existing knowledge, identify gaps, and set the foundation for developing new insights into lightweight authentication methods.

Literature Review Design

The literature review aims to analyze current authentication protocols applicable to IoT devices with limited resources. The focus is on identifying protocols that balance security with minimal computational overhead. By analyzing recent advancements and comparing their effectiveness, this review will address the critical question: How can authentication protocols be optimized for IoT devices to enhance security without compromising operational efficiency?

Sources Used

The literature review incorporates a range of sources to ensure a well-rounded understanding of the topic. Key academic papers, industry reports, and white papers have been sourced from databases such as IEEE Xplore, ScienceDirect, and specific IoT security journals. Additionally, the review includes practical insights from security standards published by organizations like the IoT Security Foundation and the National Institute of Standards and Technology (NIST) [4]. Sources from the provided Excel sheet, such as the works by Lara et al. (2020) [1] and Xue Li et al. [3], have been instrumental in framing the discussion around existing methods and their limitations.

5.1 Limitations and Risks

The rapidly evolving nature of IoT and its security technologies presents a significant challenge, as literature can quickly become outdated. Additionally, many studies do not provide extensive real-world testing data, which can limit the applicability of their conclusions.

To mitigate these limitations, the review focuses on the most recent publications and includes insights from experts currently active in the field. Engagements with IoT security professionals through interviews have supplemented published data, providing up-to-date perspec-

tives on the effectiveness of various authentication protocols.

5.2 Procedures

Systematic Analysis

The review process involved:

1. **Identification of Relevant Literature:** Keywords such as "IoT authentication," "lightweight security protocols," and "resource-constrained authentication" were used to search databases.
2. **Selection Criteria:** Papers were selected based on their relevance to resource constraints in IoT devices, the novelty of the authentication method proposed, and their citation count to ensure the inclusion of influential studies.
3. **Data Extraction:** Key information regarding each protocol's method, efficiency, security level, and scalability was extracted and tabulated for comparison.
4. **Critical Analysis:** Each study's methodology, findings, and conclusions were critically analyzed to assess their strengths, weaknesses, and applicability to resource-constrained environments.

5.3 Novel Techniques

Use of Meta-Analysis Tools

To enhance the depth of our literature review, meta-analysis software was employed to quantitatively analyze trends in research outcomes, particularly focusing on performance metrics such as latency, power consumption, and attack resilience. This approach allowed for a statistically significant comparison of different authentication methods, highlighting those that perform best under stringent resource constraints.

Integration of Expert Consultations

Another novel aspect of our methodology was the incorporation of consultations with cybersecurity experts specializing in IoT. These discussions provided practical insights that are often not available in academic literature, helping to bridge the gap between theoretical research and real-world application.

6 Findings

The majority of papers that we read for this survey had strong security levels and good performance on resource-constrained hardware. They were primarily limited in scope or had stringent setup requirements, such as a pre-existing secure channel or significant amounts of compute required at initial setup time. Many of the protocols surveyed are excellent choices for their respective designed application, but we are looking for a more generalized protocol.

6.1 Theme One: Cryptographic Security/Attack Resistance

The first theme is cryptographic security and resistance to various types of cryptographic attacks. Many of the papers we read for this audit include significant improvements to cryptographic security over the Rajaram et al. [5] paper, published in 2019. This paper provides a benchmark for attack resistance that is referenced in multiple other papers as they make improvements. The Rajawam et al. paper uses bilinear pairing to provide various authentication services. However, peer review [3] has come to the conclusion that the scheme can't guarantee user anonymity and is vulnerable to offline password attacks, impersonation, and privileged insider attacks.

The paper by Seunghwan et al. [6] proposes some significant improvements to Rajaram's proposed authentication protocol. Seunghwan's protocol provides provable anonymity and much stronger authentication protocols that are not vulnerable to the same kinds of cryptographic attacks. Additionally, the hardware-based protocol proposed by Vijaykumar et al. [7] provides a similar level of security, with large improvements over Rajaram's protocol. As such, we believe that these other protocols are much better options for large IoT networks.

6.2 Theme Two: Scope Limits

The second theme is protocols that are limited in scope. The protocol proposed by Li et al. [3] provides strong security, attack prevention, relative power and compute efficiency, and on-the-fly revocability. However, it has been created and proposed in such a way that it is only really applicable to cyber-physical power systems which include smart meters, generating stations, power companies, and subscribers. The protocol isn't generalizable, though it is highly robust and efficient. It makes use of elliptic-curve cryptography running on the authentication server and only simple operations, such as XOR and hashing, needed on the resource-constrained devices.

6.3 Theme Three: Setup Requirements

A third major theme that we observed in this literature analysis is stringent setup requirements. These appeared as additional hardware or requirements for a pre-existing secure channel. In Vijaykumar et al. [7], their algorithms are highly efficient only due to their use of single-use hardware. This increases the complexity and cost of a newly engineered IoT device, and can be cost-prohibitive in certain environments. The algorithms, run on a gen-

eral purpose CPU such as an Intel Core i9 or a Raspberry Pi are very slow and inefficient.

In the paper by Li, et al. [3], the protocol is highly secure without requiring dedicated hardware. However, this is achieved by using a pre-existing secure channel for key and parameter transmission between the IoT device and centralized authentication server. This secure channel requirement means that the protocol can't be securely set up without significant up-front configuration and cost, making it difficult to recommend.

7 Implications and Considerations for Future Work

This literature review is designed to challenge only one assumption: our current IoT security is good enough. Our research has thoroughly shown that the low-power IoT authentication protocols currently on the market do not meet the security needs of manufacturers and users. Even newly-proposed protocols often do not meet these needs. Our literature review was designed to find a newly created authentication protocol within the body of existing research that could be widely useful to businesses, industry, and users alike.

Our study is primarily limited in what it is looking for in a new standard IoT authentication protocol. It misses many protocols that are ideal for one workload or another, but are not meant to be generalized protocols. We are specifically targeting a protocol that will work reasonably well on highly resource-constrained hardware in most any situation.

The primary recommendation for future research that comes out of this paper is specialization. We feel that it would be useful to branch this paper and research authentication protocols specific to different workloads within the IoT space. These could include industrial sensors, home devices, adult toys, power grid controls, medical devices, and RFID/NFC tokens. Each of these spaces within IoT have unique requirements and need strong protection from outside tampering.

8 Conclusions

This study was conducted with the intention of examining authentication methodologies that improve on the current practical art of resource constrained IoT and other embedded devices. The landscape of IoT devices is ever growing and increasingly present in sensitive applications such as healthcare and transportation. To that end, our comparative examination of optimization strategies, scalability design, and revocability in authentication protocols demonstrates that the current operational baseline for IoT devices has much room for improvement. This strategy enabled our research team to conclude that existing authentication protocols improve on those currently in use, and merging the characteristics of said protocols would result in even higher security for IoT devices.

References

[1] Lara E, Aguilar L, Sanchez MA. Lightweight Authentication Protocol for M2M Communications in Industrial IoT Environments. Sensors. 2020;20(2):501.

[2] Athanere S, Thakur R. A Hierarchical Multi-Authority Access Control Scheme in IoT. Journal of Strategic Security. 2023;15. Available from: https://www.jstor.org/stable/48652014.

[3] Li X, Jiang C, Du D, Fei M, Wu L. A Novel Revocable Lightweight Authentication Scheme for Resource-Constrained Devices in Cyber–Physical Power Systems. Journal of Cybersecurity and Mobility. 2022;11(1):77-92.

[4] Best Practice Guidelines for Secure IoT; 2023. Available from: https://iotsecurityfoundation.org/best-practice-guidelines/.

[5] Rajaram S, Maitra T, Vollala S, Ramasubramanian N, Amin R. eUASBP: enhanced user authentication scheme based on bilinear Pairing. Journal of Ambient Intelligence and Humanized Computing. 2019.

[6] Son S, Park Y, Park Y. A Secure, Lightweight, and Anonymous User Authentication Protocol for IoT Environments. MDPI Sustainability. 2021.

[7] Vijaykumar VR, Sekar SR, Jothin R, Dinesh VC, Elango S, Ramakrishnan S. Novel Light Weight Hardware Authentication Protocol for Resource Constrained IoT Based Devices. IEEE Journal of Radio Frequency Identification. 2024;8 pp. 31-42.

9 Workload and Contributions

In this section, you specify the workload and contributions made by each team member towards the final product of this paper. Please modify each member's contributions and percentage numbers

Adrian Necaj: total percentage of workload **25%**

- Actively participated in brainstorming discussions
- Contributed to the literature review
- Contributed to the writing of the final paper

Ryan Cheevers-Brown: total percentage of workload **25%**

- Actively participated in brainstorming discussions
- Contributed to the literature review
- Contributed to the writing of the final paper

Kenneth Anderson: total percentage of workload **25%**

- Actively participated in brainstorming discussions
- Contributed to the literature review
- Contributed to the writing of the final paper

Cipriana Sorenson: total percentage of workload **25%**

- Actively participated in brainstorming discussions
- Contributed to the literature review
- Contributed to the writing of the final paper