Wenli SHANG, Xudong WEN, Zhuo CHEN, Wenze XIONG, Zhiwei CHANG, Zhong CAO, 2024. Lightweight authentication scheme for edge control systems in Industrial Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 25(11):1466-1478. https://doi.org/10.1631/FITEE.2400497

Lightweight authentication scheme for edge control systems in Industrial Internet of Things

Key words: Edge intelligent controller (EIC); Edge control systems (ECSs); Terminal devices (TDs); Anonymous authentication; Lightweight authentication

Corresponding author: Zhong CAO
E-mail: zhongc@gzhu.edu.cn
ORCID: https://orcid.org/0000-0002-2301-8030

Motivation

1. Terminal devices (TDs) in edge control systems (ECSs), such as intelligent instruments and industrial robots, need to communicate sensitive information with the edge intelligent controller (EIC). Therefore, authentication between the EIC and TDs is one of the most fundamental security issues and an integral part of the security defense of ECSs.

2. Since the TDs that need to access the EIC have constrained computing and storage resources and traditional asymmetric cryptography based authentication schemes have high computational cost, a lightweight authentication scheme is needed to protect ECSs.

Main idea

1. We propose a lightweight authentication scheme that enables bidirectional anonymous authentication between EICs and TDs.

2. Due to the limited resources of ECS devices, our scheme uses only hash functions and XOR operations for mutual authentication. This effectively reduces the burden of computation and storage while providing adequate protection measures.

3. We prove the security and effectiveness of our authentication scheme through security and performance analysis, and demonstrate its advantages in terms of security properties and computational cost by comparison with other authentication schemes.

Framework

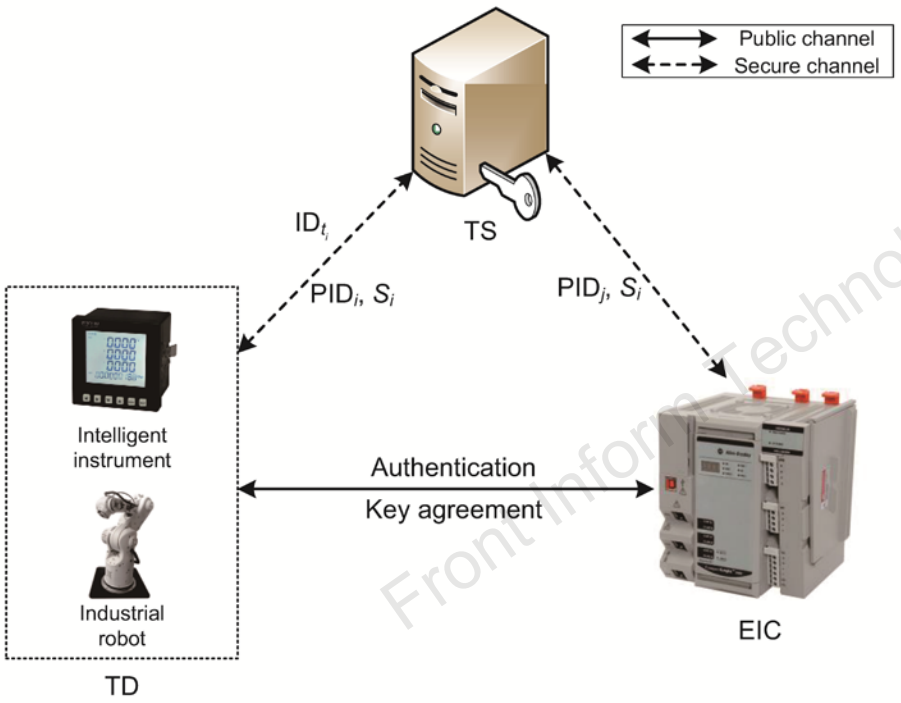


Fig. 1 System architecture

TDs are resource-constrained devices, which are responsible for collecting data and executing commands. The EIC can receive data collected by TDs, process and analyze these data, and control TDs to execute commands. The TS is an entity with high security and independence; at the same time, it has powerful storage and computing capabilities to generate the security parameters required by the system in the ECSs and send them to the corresponding entities.

Method

1. Registration phase: The TD registers with the TS to obtain the secret, which will be used for mutual authentication with the EIC, while the TS generates its pseudo-identity for the EIC and sends the secret value and its pseudo-identity to the EIC.

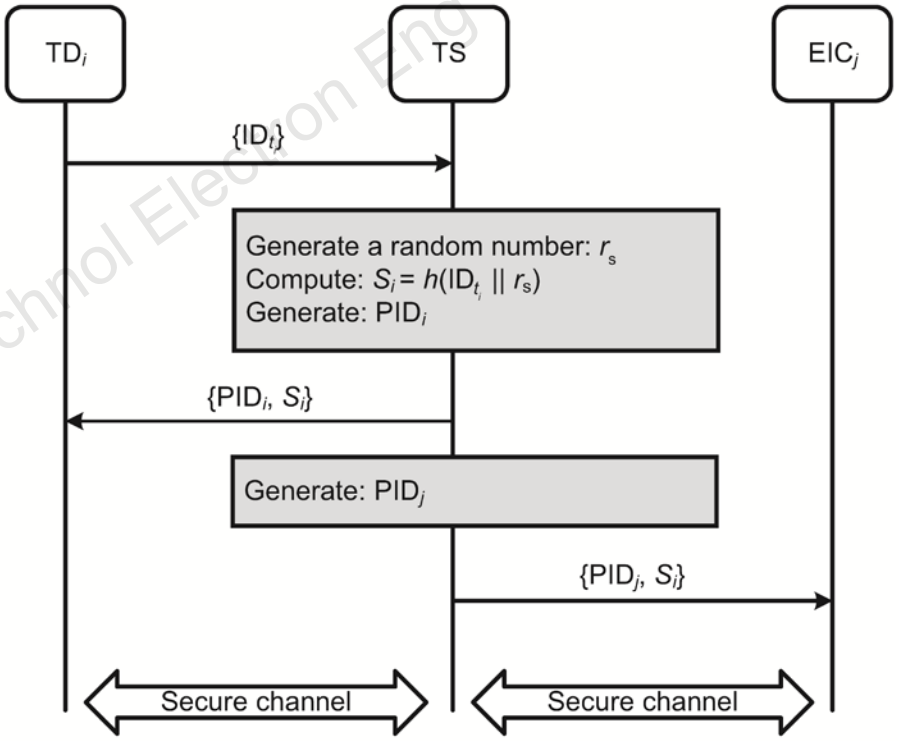


Fig. 2 Registration phase

Method

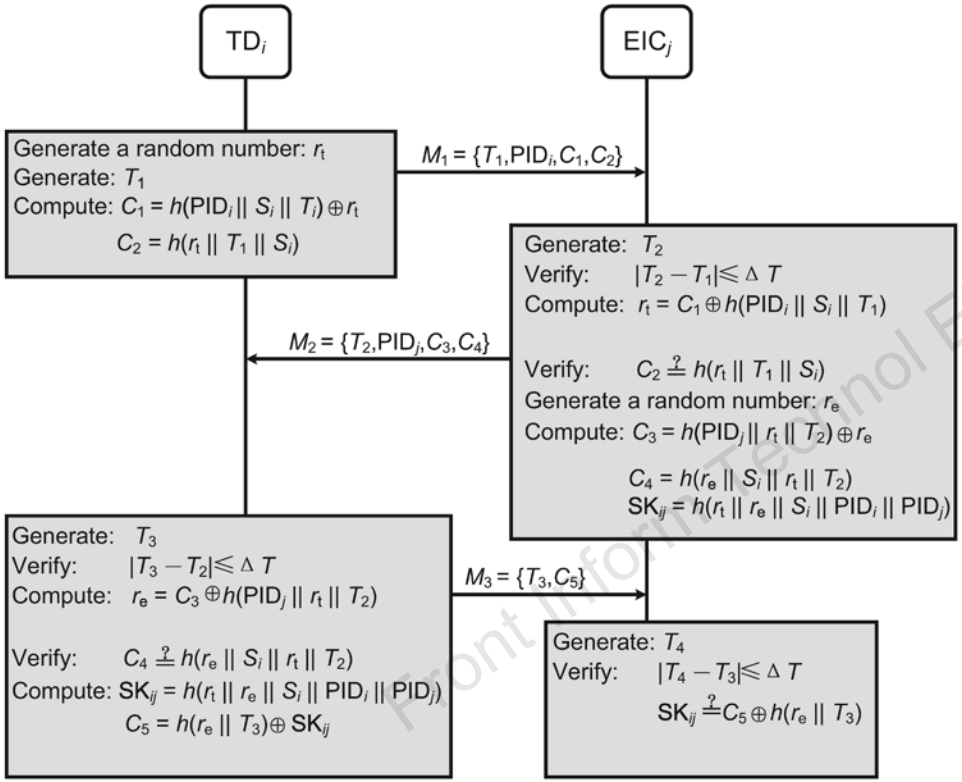


Fig. 3 Mutual authentication phase

2. Mutual authentication phase: The TD and EIC authenticate each other and generate the session key.

Major results

Table 2 Comparison of security properties among different authentication schemes

SP	Sun et al. (2015)'s	Esfahani et al. (2019)'s	Zhang LP et al. (2019)'s	Jan et al. (2021)'s	Ehui et al. (2022)'s	Ours
SP1	Yes	Yes	Yes	Yes	Yes	Yes
SP2	Yes	Yes	Yes	Yes	Yes	Yes
SP3	Yes	Yes	Yes	Yes	Yes	Yes
SP4	No	Yes	Yes	Yes	Yes	Yes
SP5	Yes	No	Yes	No	No	Yes
SP6	Yes	Yes	Yes	Yes	Yes	Yes
SP7	No	No	Yes	Yes	No	Yes
SP8	Yes	Yes	Yes	Yes	Yes	Yes
SP9	No	Yes	Yes	No	Yes	Yes
SP10	Yes	Yes	Yes	Yes	Yes	Yes
SP11	No	No	No	Yes	No	Yes
SP12	No	No	Yes	Yes	No	Yes
SP13	Yes	No	Yes	No	No	Yes

DoS: denial-of-service; MITM: man-in-the-middle; SP: security property; SP1: confidentiality; SP2: integrity; SP3: mutual authentication; SP4: anonymity; SP5: forward secrecy; SP6: known session key security; SP7: resistance to tracking attacks; SP8: resistance to impersonation attacks; SP9: resistance to MITM attacks; SP10: resistance to replay attacks; SP11: resistance to DoS attacks; SP12: resistance to desynchronization attacks; SP13: resistance to stolen-verifier attacks

Major results

Table 5 Comparison of computational cost

Scheme	Computational cost	
	Registration phase	Authentication phase
Sun et al. (2015)'s	User: – Server: $T_h + T_e$	User: $4T_h + T_e$ Server: $5T_h + 2T_d$
Esfahani et al. (2019)'s	Smart sensor: – Authentication server: $2T_h$	Smart sensor: $7T_h$ Router: $7T_h$
Zhang LP et al. (2019)'s	Smart sensor: – Service provider: $2T_h + T_e$	Smart sensor: $7T_h + T_d$ Service provider: $9T_h + 2T_e + T_d$
Jan et al. (2021)'s	Client: $2T_h$ Remote server: $3T_h$	Client and gateway: $9T_h$ Remote server: $8T_h$
Ehui et al. (2022)'s	Sensor: – Gateway: –	Sensor: $4T_e + 4T_d + 3T_h + 4T_{hmac}$ Gateway: $4T_e + 4T_d + 2T_h + 4T_{hmac}$
Ours	TD: – TS: T_h	TD: $6T_h$ EIC: $6T_h$

EIC: edge intelligent controller; TD: terminal device; TS: trusted server. T_{hmac}: execution time of the hash-based message authentication code (HMAC); T_h: execution time of the hash function; T_e: execution time of advanced encryption standard (AES) encryption; T_d: execution time of AES decryption

Major results

Table 7 Comparison of computation time

Scheme	Computation time (μs)		Total (μs)
	TD	EIC	
Sun et al. (2015)'s	134.333	53.232	187.565
Esfahani et al. (2019)'s	168.000	37.800	205.800
Zhang LP et al. (2019)'s	208.000	83.700	291.700
Jan et al. (2021)'s	216.000	43.200	259.200
Ehui et al. (2022)'s	2113.332	801.232	2914.564
Ours	144.000	32.400	176.400

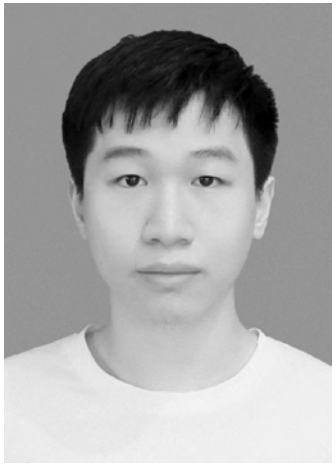
EIC: edge intelligent controller; TD: terminal device

Conclusions

1. In this paper, we propose a lightweight authentication scheme for ECSs that enables bidirectional anonymous authentication and key agreement between the EIC and TDs, and the negotiated session key can be used for subsequent secure communication between the two parties.

2. Security analysis shows that the authentication scheme can provide necessary security properties. In addition, performance analysis demonstrates the benefits of the authentication scheme in terms of security properties, communication overhead, and computational cost.

Wenli SHANG received the MS degree from School of Mechanical and Automation Engineering, Northeastern University, in 2002, and the PhD degree from Laboratory of Industrial Control Network and System, Shenyang Institute of Automation, Chinese Academy of Sciences, in 2005. From 2005 to 2019, he served as an assistant researcher, associate researcher, and researcher successively in Shenyang Institute of Automation, Chinese Academy of Sciences. Since 2020, he has been a professor with Guangzhou University. His research interests include industrial control system information security, computational intelligence and machine learning, and edge computing.



Xudong WEN is pursuing a graduate degree in electronic information with the School of Electronics and Communication Engineering, Guangzhou University, Guangzhou, China. His research focuses on the security of Industrial Internet of Things.

Zhuo CHEN received the MS degree from the School of Electronics and Communication Engineering, Guangzhou University, Guangzhou, China, in 2023. His research includes industrial control system information security, computational intelligence, and machine learning.

Wenze XIONG received the MS degree from the School of Electronic Engineering, Beijing University of Posts and Telecommunications, in 2018. He is now a senior engineer in the Instrumentation Technology and Economy Institute (ITEI). His research interests include industrial control systems, industry security, functional safety, and reliability of complex systems.

Zhiwei CHANG received the PhD degree from the School of Electronic Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2020. He is currently with the School of Electronics and Communication Engineering, Guangzhou University. His research interests include the extended interaction devices, plasma physics, and high-power microwave technology and its applications.

Zhong CAO received the MS degree from the School of Computer Science and Educational Software, Guangzhou University, in 2005, and the PhD degree from the School of Energy Science and Engineering, UESTC, in 2015. From Dec. 2016 to Dec. 2017, he was a visiting scholar at the Department of Civil and Environmental Engineering, University of North Carolina at Charlotte, Charlotte, NC, USA. He is currently an associate professor with the School of Electronics and Communication Engineering, Guangzhou University. His research interests include industrial control system, information security, machine learning, and intelligence control.