A Data Authentication Method Based on Vector Projection for Industrial Edge Computing System

Yi CHEN\textsuperscript{1}, Ai-dong XU\textsuperscript{2}, Yi-xin JIANG\textsuperscript{2}, Yu-nan ZHANG\textsuperscript{2}, Hong WEN\textsuperscript{1,*}, Qian-ru WANG\textsuperscript{1} and Zhen WANG\textsuperscript{1}

\textsuperscript{1}National Key Lab of Comm., University of Elec. Sci., and Tech. of China, Chengdu 611731, China
\textsuperscript{2}EPRI, China Southern Power Grid Co. Ltd., Guangzhou 510080, China

*Corresponding author

Keywords: Vector projection, Authentication, Edge computing, CSI.

Abstract. In this paper, we consider a success rate of data authentication for industrial edge computing system. We propose a data authentication method based on vector projection, which is a novel secure authentication program. The proposed authentication method is divided into initial authentication, calculating the vector projection of channel state information (CSI), and checking the validity of data frames. Experimental results show that the proposed scheme can significantly achieve a high success rate of data authentication.

Introduction

With the rapid development of Internet of things (IoT) technology, various intelligent nodes will generate huge amounts of data. The same goes for industrial systems. As we know, traditional cloud computing system has some inherent limitations \cite{1} that it can’t satisfy the demand of real-time control. Especially, for a great quantity of intelligent nodes, it is not suitable for quickly verifying the validity of data in the industrial edge computing system due to the intensive computation involved in traditional complex cryptographic authentication schemes \cite{2-3}. Recently, the edge computing paradigm can also satisfy the key industrial requirements, such as real-time control, low cost, and energy consumption, by building small edge data centers \cite{4}. The industrial edge computing system consists of edge servers who are usually specific high-end servers, and various intelligent nodes who usually have limited resources \cite{5} due to cost constraints. Additionally, the authentication techniques of physical layer based on channel state information (CSI) have been proposed for information security in recent years \cite{6-13}. It is carried out via comparing the similarity of CSI \cite{14-15}, which has the physical-layer channel characteristics of spatial-temporal uniqueness and can be estimated from the received data frames. However, the authentication rates of these methods need to be improved for their applications, especially in mobile application scenarios. Therefore, it is necessary to design a brand-new efficient data authentication method for industrial edge computing system.

System Model

We consider a simplified industrial edge computing scenario as shown in Figure 1, where it consists of various industrial nodes (Alice), and industrial edge devices (Bob). Alice wants to send messages to Bob across a wireless link. Bob has to check the validity of the data packets from Alice. Compared to the nodes with limited resources, edge devices are usually specific high-end servers with powerful CPU, larger memory and storage. Bob can perform authentication of initial data frames from Alice via upper layer authentication.

![Figure 1. A simple scenario of industrial edge computing.](image)
Proposed Scheme

In this section, we will present the proposed data authentication method, which is divided into initial authentication, calculating the vector projection of CSI, and checking the validity of data frames. Figure 2 is the detailed processes of the proposed data authentication method.

Initial Authentication

When Alice transmits messages to Bob, the industrial edge computing server, Bob authenticates the initial data frame from Alice through the upper layer authentication and estimates the corresponding channel state information vector as the reference vector for data authentication.

Bob Authenticates the First Data Frame with the Upper Layer Authentication. If the upper layer authentication fails, Bob discards the first data frame and takes the next data frame as the first one, then, does the upper layer authentication again. If the upper layer authentication of the first data frame is successful, Bob accepts the packet and estimates the channel response $H_{1}^{TS}$. The CSI $H_{1}^{TS}$ can be estimated by ILS channel estimation method [16-18]. However, the upper layer authentication and the channel estimation method are not the essence of this article, thus we omit them here.

Bob Takes the Real Part of the Channel Response as a Reference Vector

$$\overline{H}_{1} = \text{Real}(H_{1}^{TS})$$,  \hspace{1cm} (1)

where $H_{1}^{TS}$ represents the CSI from the industrial node to the edge computing server, which is a complex matrix of $m$ rows and 1 column, and Real ($\cdot$) denotes the real part of the channel response.

Calculating the Vector Projection of CSI

When Bob receives a new data frame, he estimates the corresponding channel response and calculates the vector projection of the new data frame on the previous valid data frame. Figure 3 is the principle map of vector projection about channel information.

(1) When the edge computing server receives the $(k+1)$-th data frame, where $k$ is the index of the message, an integer no less than 1, Bob estimates the corresponding channel response $H_{k}^{TS}$. Then, Bob makes the real part of $H_{k+1}^{TS}$ as a vector

$$\overline{H}_{k+1} = \text{Real}(H_{k+1}^{TS})$$,  \hspace{1cm} (2)

(2) Bob calculates the vector projection of the vector $\overline{H}_{k+1}$ on the vector $\overline{H}_{k}$

$$\psi_{k} = \frac{\overline{H}_{k} \cdot \overline{H}_{k+1}}{\|\overline{H}_{k}\|} \times \cos(\theta_{k}) = \frac{\overline{H}_{k} \cdot \overline{H}_{k+1}}{\|\overline{H}_{k}\|}$$,  \hspace{1cm} (3)

where, $\overline{H}_{k}$ is a channel information vector estimated from the $k$-th data frame, $\overline{H}_{k} \cdot \overline{H}_{k+1}$ denotes the dot product of the two vectors, $\|\overline{H}_{k}\|$ represents the length of the vector $\overline{H}_{k}$, $\cos(\cdot)$ indicates the trigonometric cosine function, and $\theta_{k}$ is the angle between the two vectors, $\overline{H}_{k+1}$ and $\overline{H}_{k}$, who also indicates the angular deviation of the channel state information $H_{k+1}^{TS}$ and $H_{k}^{TS}$.

Checking the Validity of Data Frames

After the vector projection is computed, Bob utilizes the hypothesis testing, as (4), to determine whether the data frames are valid or not, where $\eta$ indicates the threshold of projection.

$$\psi_{k} > \sqrt{H_{0}^{2}}$$ or $$\psi_{k} < \sqrt{H_{1}^{2}} \eta.$$  \hspace{1cm} (4)
Hypothesis testing is the task of deciding which of the two hypotheses, $\mathcal{H}_0$ or $\mathcal{H}_1$, is true, when one is given the value of a random variable [19]. In the null hypothesis, $\mathcal{H}_0$, the $(k+1)$-th data frame is valid. Bob accepts this hypothesis if the test statistic $\psi_k$, is below some projection threshold $\eta$. Bob accepts the $(k+1)$-th data frame, replaces the previous vector $\overline{H}_k$ with the new vector $\overline{H}_{k+1}$, and then calculates the next new vector projection. Otherwise, in the alternative hypothesis, $\mathcal{H}_1$, the data frame is invalid. Bob accepts this hypothesis if the test statistic $\psi_k$, is above some projection threshold $\eta$. Bob discards the $(k+1)$-th data frame, and returns to the initial authentication.

Bob receives the first data frame sent by Alice.

Is the initial authentication successful?

N

Y

Bob estimates the channel response $H_i^{TS}$ and takes the real part of the channel response as a reference vector $\overline{H}_1 = \text{Real}(H_i^{TS})$

Bob calculates the vector projection $\psi_i$

$\psi_i < \eta$?

Y

Data frame is valid.

N

Bob receives the second data frame sent by Alice and gets $H_2^{TS}$ and $\overline{H}_2 = \text{Real}(H_2^{TS})$

Bob calculates the vector projection of channel information.

$\psi_1 < \eta$?

Y

Data frame is valid.

N

Bob receives the $k$-th data frame sent by Alice and gets $H_k^{TS}$ and $\overline{H}_k = \text{Real}(H_k^{TS})$

Bob calculates the vector projection of channel information.

$\psi_k < \eta$?

Y

Data frame is valid.

N

Bob receives the $(k+1)$-th data frame sent by Alice and gets $H_{k+1}^{TS}$ and $\overline{H}_{k+1} = \text{Real}(H_{k+1}^{TS})$

Bob calculates the vector projection $\psi_k$

Figure 2. Process flowchart of the proposed data authentication method.

Figure 3. Principle map of vector projection about channel information.

Performance Assessment and Analyses

To examine the performance of the proposed scheme, we employ the data of channel impulse responses provided by NIST (National Institute of Standards and Technology) [20] to simulate the data transmission authentication performance. The channel impulse responses measured in different typical industrial sites are adopted as the CSI. We use the channel impulse responses of moving scenarios to do the test. The transmitting equipment always stayed stationary and the transmitting central frequency is 5 GHz with Omni-antennas, hence the wavelength of the transmission signal is 0.06 meter. The receiving equipment walked from one acquisition point towards the next one, hence each record of channel impulse responses corresponded to a different position. It is worth to notice that the wireless channel is reciprocal. Therefore, the CSI results of the simulated receiver to the transmitting equipment are not influenced. Each experiment includes multiple acquisitions and each acquisition includes multiple records. The data collected by NIST provide an 8188 samples long channels impulse response for each position of the receiving equipment in each scenario. Since an
FFT size of 8188 is used for the channel measurements, the channel impulse response in each record is an 8188×1 complex vector in the time domain.

Fig. 4 plots the success rate of data frames authentication for varying threshold values of vector projection $\psi$ in different industrial moving scenarios. The success rates of data frames authentication gradually increases with the increasing threshold values of projection $\psi$. When the threshold value of projection $\psi$ is high, greater than $5\times10^{-4}$, the proposed scheme contributes to high success rates of data frames authentication in different scenarios. The key features of data transmission by wireless nodes are intermittence and continuance for a short time. In the coherent time, the channel information carried by the data frame is approximately the same. When the wireless node moves from one acquisition point towards the next one, the channel state information from the sender to the receiver changes accordingly. Thus, even if the difference of vector projection is very small, the proposed scheme can achieve a high success rate of data authentication. Therefore, it is feasible to satisfy the requirement of massive data authentication for the industrial edge computing scenario.

![Figure 4. Success rate of data frames authentication versus threshold value of projection.](image)

Conclusions

In this paper, a data authentication method based on vector projection of channel state information is proposed for industrial edge computing scenario. The novel method employs vector projection of channel state information to authenticate the validity of the data frames from industrial nodes. It contributes to high success rates of data frames authentication in different industrial environment. Therefore, the proposed scheme is suitable for users in the industrial edge computing scenario to achieve data authentication rapidly.

Acknowledgement

This research is supported by the National Key R&D Program of China (2018YFB0904900, 2018YFB0904905).

References

[1] Y. Kawamoto, N. Yamada, H. Nishiyama, N. Kato, Y. Shimizu, and Y. Zheng, A Feedback Control-Based Crowd Dynamics Management in IoT System, IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1466-1476, Oct. 2017.

[2] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. X. Lu, and X. M. Shen, A Lightweight Message Authentication Scheme for Smart Grid Communications, IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Dec. 2011.

[3] A. R. Metke and R. L. Ekl, Security Technology for Smart Grid Networks, IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 99-107, Jun. 2010.
[4] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, A Survey on Network Methodologies for Real-Time Analytics of Massive IoT Data and Open Research Issues, IEEE Communications Surveys and Tutorials, vol. 19, no. 3, pp. 1457-1477, Apr. 2017.

[5] T. G. Rodrigues, K. Suto, H. Nishiyama, and N. Kato, Hybrid Method for Minimizing Service Delay in Edge Cloud Computing Through VM Migration and Transmission Power Control, IEEE Transactions on Computers, vol. 66, no. 5, pp. 810-819, May 2017.

[6] H. Wen, S. Li, X. Zhu, and L. Zhou, A framework of the PHY-layer approach to defense against security threats in cognitive radio networks, IEEE Network, 27(3): 34-39, May 2013.

[7] H. Wen, P. H. Ho, B. Wu, Achieving Secure Communications over Wiretap Channels via Security Codes from Resilient Functions, IEEE Wireless Communication Letter, 3(3): 273-276, 2014.

[8] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. H. Song, J. T. ang, X. Wang, Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things, IEEE Internet of Things Journal, 5(1): 219-228, 2018.

[9] J. Tang, D. Monireh, K. Zeng, H. Wen, Impact of Mobility on Physical Layer Security Over Wireless Fading Channels, IEEE Transactions on Wireless Communications, 17(12): 7849-7864, Dec. 2018.

[10] Y. Chen, H. Wen, H. H. Song, et al., Lightweight one-time password authentication scheme based on radio frequency fingerprinting, IET Communications, 12(12): 1477-1484, Jul. 2018

[11] F. Pan, Z. B. Pang, M. Luvisotto, et al. Physical-layer security for industrial wireless control systems: basics and future directions, IEEE Industrial Electronics Magazine, 12(4): 18-27, 2018.

[12] Y. P. Xie, H. Wen, B. Wu, Y. X. Jiang, J. X. Meng, A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing, IEEE Transaction on Cloud Computing, 7(2): 383-391, Apr. 2019.

[13] Y. Chen, H. Wen, J. Wu, et al., Clustering Based Physical-Layer Authentication in Edge Computing Systems with Asymmetric Resources, Sensors, 19(8): 1926, Apr. 2019.

[14] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Transactions on Wireless Communications, vol.7, no.7, pp. 2571-2579, Jul. 2008.

[15] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, A Physical-Layer Technique to Enhance Authentication for Mobile Terminals. 2008 IEEE International Conference on Communications, 2008, pp. 1520-1524.

[16] Y. Li, L.J. Cimini, N.R. Sollenberger, Robust channel estimation for OFDM systems with rapid dispersive fading channels. IEEE Transactions on Communications, 46(7): 902-915, Jul. 1998.

[17] E.G. Larsson, G.Q. Liu, J. Li, G.B. Giannakis, Joint symbol timing and channel estimation for OFDM based WLANs. IEEE Communications Letters, 5(8): 325-327, Aug. 2001.

[18] S. Wei, Z.W. Pan. Iterative LS channel estimation for OFDM systems based on transform-domain processing. 2007 International Conference on Wireless Communications, Networking and Mobile Computing, 2007, pp. 416-419.

[19] H. Wen, Y. F. Wang, X. P. Zhu, J. Q. Li, and L. Zhou, Physical layer assist authentication technique for smart meter system, IET Communications, vol. 7, no. 3, pp. 189-197, Feb 2013.

[20] R. Candell, K. A. Remley, and N. Moayeri, “Radio frequency measurements for selected manufacturing and industrial environments,” NIST, Tech. Rep. 1951, 2016. [Online]. Available: http://doi.org/10.18434/T44S3N.