氏　　名	趙　国柱
学　位　名	博士（システム情報科学）
学位記番号	第６７号
学位授与年月日	令和５年３月２２日
学位論文題目	Passive User Authentication in Industrial Internet of Things
論文審査委員	主査　姜　暁鴻
	副査　稲村　浩
	副査　藤野　雄一
	副査　和田　雅昭
	副査　石田　繁巳

論　文　要　旨

Industrial Internet of Things (IIoT) serves as an important network architecture for information collection, exchange and analysis in the industrial platform. An IIoT system usually consists of a vast number of users with highly diverse authority rights and constantly generates/stores huge amounts of confidential information, so how to design flexible and cost-effective authentication approaches to ensure the security of IIoT systems becomes an increasingly urgent demand. Specially, the passive user authentication is of great importance for IIoT systems to implement continuous and non-intrusive user identity verification. The IIoT can be roughly divided into three layers according to the functions of IIoT, i.e., the Manufacturing Execution (ME) layer, Monitoring and Control (MC) layer, and Decision and Optimization (DO) layer. This dissertation develops user authentication schemes corresponding to these three layers to ensure the secure operation of IIoT systems. First, for user authentication of the ME layer, this dissertation explores the common behavioral biometrics from user sequential operation actions in IIoT systems to propose a passive authentication framework, which provides continuous/non-intrusive user authentication and poses good anti-interference capability in the interference-intensive environment of the ME layer. Second, for user authentication of the MC layer, we explore the user consecutive screen-touch actions during routine work processes and propose a passive authentication method based on both the time-varying characteristics and spatial

image characteristics of the user touch trajectory sequences, which provides implicit / non-intrusive user identity verification and can meet the real-time authentication requirement of the MC layer. Finally, for user authentication of the DO layer, we develop a novel two-dimensional passive authentication framework by jointly utilizing both the time-varying characteristics of the user sequential operation actions and spatial variation characteristics of Channel State Information (CSI) caused by these actions, which applies to the authentication of the DO layer with high security requirement. It is expected that the new authentication methods proposed in this dissertation can significantly facilitate the applications of IIoT systems.

審査結果の要旨

This dissertation develops user authentication schemes corresponding to the three layers of IIoT to ensure the secure operation of IIoT systems. First, for user authentication of the Manufacturing Execution (ME) layer, this dissertation explores the behavioral biometrics from user sequential operation actions to propose a passive authentication framework, which poses good anti-electromagnetic interference capability in the interference-intensive environment of ME layer. Second, for user authentication of the Monitoring and Control (MC) layer, we explore the user consecutive screen-touch actions and propose a passive authentication method, which can meet the real-time authentication requirement of the MC layer. Finally, for user authentication of the Decision and Optimization (DO) layer, we develop a novel two-dimensional passive authentication framework based on both the temporal feature of user sequential operation actions and spatial feature of Channel State Information (CSI) caused by these actions, which applies to the authentication of the DO layer with high security performance requirement. It is expected that the new authentication methods proposed in this dissertation can significantly facilitate the applications of IIoT systems.

・学位論文の構成

Chapter 5 Authentication Utilizing Two-Dimensional Features for the Decision and Optimization (DO) Layer

Chapter 6 Conclusion

・研究目的の妥当性，従来の手法との比較においての有意性，および理論・実験手法の新規性

Industrial Internet of Things (IIoT) serves as an important network architecture for information collection, exchange and analysis in the industrial platform. An IIoT system usually consists of a vast number of users with highly diverse authority rights and constantly generates / stores huge amounts of confidential information, so how to design flexible and cost-effective authentication approaches to ensure the secure operations of IIoT systems becomes an increasingly urgent demand. Specially, the passive user authentication is of great importance for IIoT systems to implement continuous and non-intrusive user identity verification.

The IIoT can be roughly divided into three layers according to functions of IIoT, i.e., the manufacturing execution (ME) layer, monitoring and control (MC) layer, and decision and optimization (DO) layer. This dissertation develops user authentication schemes corresponding to these three layers to ensure the secure operation of IIoT systems. First, for user authentication of the ME layer, this dissertation explores the common behavioral biometrics from user sequential operation actions in IIoT systems to propose a passive authentication framework, which provides continuous / non-intrusive user authentication and poses good anti-electromagnetic interference capability in the interference-intensive environment of ME layer. Second, for user authentication of the MC layer, we explore the user consecutive screen-touch actions during routine work processes and propose a passive authentication method based on both the time-varying characteristics and spatial image characteristics of the user touch trajectory sequences, which provides implicit / non-intrusive user identity verification and can meet the real-time authentication requirements of the MC layer. Finally, for user authentication of the DO layer, we develop a novel two-dimensional passive authentication framework by jointly utilizing both the time-varying characteristics of the user sequential operation actions and spatial variation characteristics of Channel State Information (CSI) caused by these actions, which applies to the authentication of the DO layer with high security requirement. It is expected that the new authentication methods proposed in this dissertation can significantly facilitate the applications of IIoT systems.

・得られた知見のシステム情報科学の分野における意義

The results of this thesis provide the following valuable insights.

1. This dissertation develops three passive authentication protocols corresponding to ME, MC, and DO layer respectively, to ensure the secure operation of IIoT systems.
2. It is expected that the new authentication methods proposed in this dissertation can significantly facilitate the applications of IIoT systems .
3. The passive authentication solution developed in this thesis can be used as a promising supplement or alternative to the traditional pin-based and pattern-based active authentication methods to achieve security enhancement in the IIoT systems.