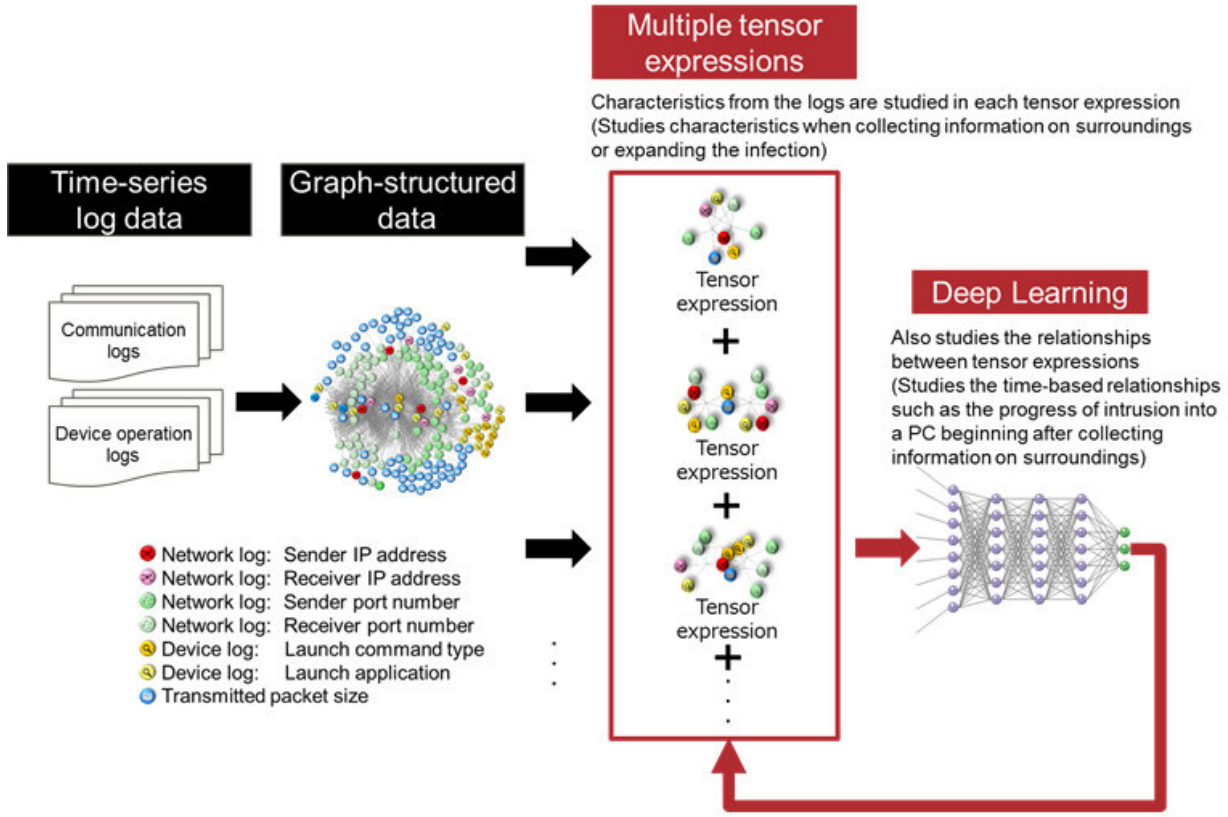
Fujitsu AI increases accuracy of malware intrusion detection

October 6 2017



Credit: Fujitsu

Fujitsu Laboratories today announced the development of AI technology to improve accuracy in detecting malware intrusions into networks within organizations, such as corporations, through an extension of its

proprietary Deep Tensor AI technology, which can learn from graph-structured data. In recent years, as cyberattack methods have grown more sophisticated, it has become ever more important to build post-intrusion countermeasures against attackers who use specialized malware to invade a system, especially in targeted cyberattacks. As methods, frequency, and scope of attacks made by malware that has invaded a system constantly evolve over time, and because they blend into the day-to-day activity on a network, it is necessary to take a more comprehensive view of the various activities of malware in order to detect them.

Fujitsu Laboratories has now developed technology that learns from various characteristics, including time series log data, and from the relationships between those characteristics. With this technology, Fujitsu Laboratories succeeded in training its AI to recognize the relationships between the types and numbers of the various activities of malware that has invaded an organization, as well as factors such as the spacing between these activities and their sequence, grasping the characteristics of malware. Using data provided by MWS2017, Fujitsu Laboratories tested this technology's ability to differentiate between day-to-day network communications and malware attacks, and confirmed that by learning the numerous traces left by malware which change over time, it could detect malware with 93% accuracy.

Fujitsu Laboratories aims to commercialize this technology during fiscal 2017 as part of Fujitsu's AI technology, Fujitsu Human Centric AI Zinrai, aiming for fields outside cybersecurity, such as marketing using records of the activities of people over time. In addition, malware intrusion detection technology that utilizes this newly developed technology will be combined with previously developed cyberattack analysis technology to form a countermeasure support technology, which will be trialed internally during fiscal 2018. Details of this technology will be announced at the Anti Malware Engineering Workshop 2017

(MWS2017), to be held in Yamagata, Japan on October 23-25.

As huge numbers of new types and subtypes of malware are emerging day by day, and the harm these cyberattacks cause is only increasing, improving cyberattack countermeasures has become an urgent issue. Cyberattack methods have become increasingly sophisticated in recent years, making it more difficult to prevent attacks with just countermeasures at the entrances to an organization's internal network and antivirus software on individual devices, as could be done previously. With targeted cyberattacks in particular, because attackers use dedicated malware focused on a specific company as a target, it is extremely difficult to completely prevent intrusion within the organization, making it important to build countermeasures for after the malware has infiltrated the network. Post-intrusion countermeasures require personnel who have high cybersecurity skills, but because there are not enough security personnel to meet the rising number of increasing cyberattacks, automation and AI are much anticipated to provide support.

Malware that has infiltrated inside an organization's network can make malicious use of the network communications and command operations used in day-to-day tasks, continuing its attack while changing its activities, including gathering information on its surroundings, testing possible infiltration of other PCs, and spreading its infection. For this reason, the differences in characteristics between network communications due to day-to-day tasks and those due to malware activities are minor, making highly accurate detection difficult.

Fujitsu Laboratories has now developed AI technology that can accurately detect intrusions, expanding the Deep Tensor technology it developed, which can learn from and categorize graph-structured data, in order to enable it to learn from time-series characteristics. By developing technology that, for the various characteristics included in time-series

log data, could learn the relationships between characteristics that occur sequentially, versus those that occur simultaneously, Fujitsu Laboratories was able to successfully train this system on the types and numbers of activities taken by malware that had infiltrated an organization, as well as on the relationships between the sequences and intervals between these activities, getting a grasp on the distinctive characteristics of malware. Details of this technology are as follows.

Deep Tensor technology enables a system to learn from graph-structured data with high accuracy by using learning methods that convert graph-structured data to mathematical expressions called tensors, while simultaneously applying deep learning methods. This technology extracts sets of characteristics that are highly interrelated from time-series log data by first preparing in advance multiple tensor expressions, then learning characteristics recorded in the log at different times, and then also applying deep learning to the relationships between characteristics (tensor expressions), enabling the system to differentiate them.

In addition, in response to increasing numbers of tensor expressions, Fujitsu Laboratories has also concurrently developed technology to speed up the processing of tensor calculations, as well as technology enabling distributed, parallelized processing of these computations. With these technologies, it is possible to use dozens of tensor expressions for learning in the time previously required to process a single tensor expression.

Using this newly developed technology, it is possible to detect malware intrusions that change factors such as attack method, frequency and scope over time, and that mix their activities in with day-to-day network traffic. Using a research dataset provided by MWS2017, Fujitsu Laboratories carried out a trial to differentiate between day-to-day network communications and malware attacks, which confirmed that this technology was able to detect malware attacks with an accuracy of

93% by learning from multiple traces that change over time, as compared with an accuracy of 76% for existing machine learning methods.

With this technology, Fujitsu Laboratories has created a detection method that can continually grow and respond rapidly to cyberattacks, which continue to change and grow more sophisticated.

Fujitsu Laboratories aims to commercialize this technology during fiscal 2017 as part of Zinrai, aiming at fields outside cybersecurity, such as marketing that utilizes peoples' activity history.

In addition, it will conduct an internal trial in fiscal 2018 of malware intrusion detection technology incorporating this technology, which combines this technology with a previously developed cyberattack analysis technology to form a countermeasure support technology.

Provided by Fujitsu