様式3

論 文 内 容 の 要 旨

氏 名 （ 山内 雅明 ）	
論文題名	Anomalous Operation Detection for Smart Home based on In-home Behaviors of Users (宅内のユーザ行動に基づくスマートホーム不正操作検出手法)

論文内容の要旨

Anomalous operation attack that an attacker operates home Internet of Things (IoT) devices by sending packets via an intruded IoT device or a smartphone is an important problem. Because the home IoT devices are physically close to users, this attack may make users unsafe and could even harm users physically. For example, an attacker operates to turn on and off the room light, change the temperature of an air conditioner, or unlock a smart home lock. Furthermore, simultaneous attacks on high-power IoT devices can suddenly increase energy demands, which could lead to major power outages. Therefore, the detection and prevention of packets of the attack are paramount importance.
Unfortunately, existing intrusion detection systems are difficult to detect packets of the anomalous operation attack. The existing intrusion detection systems assume that legitimate and anomalous traffic patterns are notably different. However, both attackers and legitimate users send the same types of packets to operate IoT devices. For instance, if an attacker sends packets via the malware-infected smartphone of a legitimate user, even the source IP address is identical to that of the legitimate user. Consequently, existing intrusion detection systems cannot distinguish between packets sent by legitimate users and attackers based on the available information. It is necessary to grasp whether the users intended to perform the operation of the home IoT devices or not.
Therefore, we first propose a method to detect such attacks based on user behavior. This method models user behavior as sequences of user events including operation of home IoT devices and other monitored activities. Considering users behave depending on the condition of the home such as time and temperature, our method learns event sequences for each condition. To mitigate the impact of events of other users in the home included in the monitored sequence, our method generates multiple event sequences by removing some events and learning the frequently observed sequences. For evaluation, we constructed an experimental network of home IoT devices and recorded time data for four users entering/leaving a room and operating devices. We obtained detection ratios exceeding 90% for anomalous operations with less than 10% of misdetections when our method observed event sequences related to the operation. However, this method modeled users' home states based on the time of day; hence, attackers can exploit the system to maximize attack opportunities.
Thus, we second propose a behavior-modeling method that combines home state estimation and event sequences of IoT devices within the home to enable a detailed understanding of long- and short-term user behavior. The state estimation is that estimating the home state using not only the time of day but also the observable values of home IoT sensors and devices. We compared the proposed model to the first method using data collected from real homes. Compared with the estimation-based method, the proposed method achieved a 15.4% higher detection ratio with fewer than 10% misdetections. Compared with the sequence-based method, the proposed method achieved a 46.0% higher detection ratio with fewer than 10% misdetections.
Learning the behavior of users sufficiently may require a large amount of data, but the amount of data collected in each home is limited. When the data is not enough, the detection of the anomalous operation would be difficult. The data shortage will also occur in the case that a user introduces a new home IoT device.
However, anomalous operations still need to be detected regardless of whether the data amount is sufficient or not. Thus, we consider the cooperation between trained models that learned behaviors of users in the homes. However, an attacker who tries anomalous operations may participate in the cooperation; and gets hints about the timing that the anomalous operations tend to be achieved by watching the cooperation traffic that includes information of behaviors in the past. Therefore, the cooperation should be taken with hiding personal identification. Furthermore, to achieve accurate detection, the trained models that learned the same behaviors of users have to cooperate. Therefore, we need a method that the users having similar lifestyles cooperate without identification of users. We also propose a framework to utilize data of similar users without sharing private information. We introduce an agent that learns behaviors of users to detect anomalous operations in each home and

cooperates with other agents. In this framework, an agent requiring cooperation with other agents sends a question to the other agents, attaching identifiers of past questions that are similar to the behaviors learned. The receivers decide whether the question is from a similar agent by using the attached information. If the question is from a similar agent, the agent answers the question. We evaluate our framework by using behavior datasets collected from real homes. We simulate two cases: (1) sequences of operations are monitored, and (2) home IoT devices are used alone but sequences cannot be used for detection. The results show that our framework has a 50.5% higher detection ratio for case (1) when using the behavioral data of each user. For case (2), our framework has a 13.4% higher detection ratio when using all the behavioral data of users. However, if an attacker participates in this framework and send fake questions and answers, there are risks that users receive false data via the framework.
Therefore, we propose a countermeasure to suppress the impact of such negative impact while maintaining the advantage of the framework. In this countermeasure, we check the message is sent from the similar agent by checking the attached IDs to the message. If the agent who received the message answered ``Yes'' to the same questions of the attached IDs, the agent accepts the message. By doing so, the agent avoids accepting the messages that sent from attackers because it is difficult for attackers to attach the IDs that the agent answered ``Yes'' in the past. We discuss the effects of this countermeasure with numerical examples.

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　山内　雅明　）			
論文審査担当者		（職）	氏　名
	主 査	教授	村田 正幸
	副 査	教授	渡辺 尚
	副 査	教授	長谷川 亨
	副 査	教授	山口 弘純
	副 査	教授	松岡 茂登

論文審査の結果の要旨

IoT技術が発展し、様々な機器がインターネットに接続している。特に、複数の家電がホームネットワークに接続することで、ネットワークを介して管理可能なスマートホームが構築されている。ユーザはスマートフォンやAIスピーカーを介して、ホームIoT機器の操作やセンサ情報の利用が可能となっている。このようなIoT機器の普及に伴い、IoT機器を標的としたサイバー攻撃のリスクが高まっている。現在、観測されている攻撃としては、IoT機器の脆弱性を利用した乗っ取りのように、パソコンやスマートフォンと同様の攻撃が挙げられる。このような攻撃は、正常時のIoT機器の挙動や攻撃者の挙動を分析して現在の状態と比較することで検知可能である。

ネットワークに接続したIoT機器に対する特有の攻撃として、乗っ取ったスマートフォンなどを経由して操作パケットをIoT機器に送信して勝手に動作させるという不正操作攻撃が考えられる。具体的には、部屋の照明の操作や、エアコンの温度変更、スマートロックの解錠といったことが考えられる。このような不正操作攻撃は、ホームIoT機器がユーザと物理的に近い位置にあることからユーザに対して物理的被害を与える可能性や、電力を多く消費する家電を一斉に操作することで大規模な停電を発生させる可能性が指摘されている。そのため、不正操作攻撃の検出は重要課題となっている。しかし、不正操作時の通信パケットは、正常時の操作パケットと同じプロトコルに従って送信されることから、既存の侵入検知システムで検知することは困難である。例えば、ユーザのスマートフォンを経由して不正操作パケットを送信することで、送信元IPアドレスの情報まで正常時の通信と同じとなる。そのため、各操作パケットが、ユーザが意図して送信したものかどうかを把握する必要がある。

本論文の研究成果は、ユーザの行動に着目することで、ホームIoT機器に対する不正操作パケットの検出を可能としたことである。まず、ユーザが機器を操作する順番に着目して、IoT機器の通信を中継するホームゲートウェイにおいてユーザの時間帯ごとの機器操作順序を学習し、学習モデルから外れた機器操作を不正操作として検出する手法を提案した。また、ホームIoTセンサから得られる室温や騒音などの観測値に基づいてユーザの状態を推定し、各状態における行動順序を学習することで、さらに高い精度で不正操作を検知する手法についても提案した。監視カメラの映像等を利用せず、複数のユーザが存在するスマートホームに適用可能なことから、より実現可能性の高い不正操作検知が可能となった。また、ユーザの行動を学習する際に各家庭から得られるデータ数に限りがあることに着目し、似た行動様式の家庭の学習モデル間で連携して異常検知を行う方法を提案した。その際、攻撃者が過去の操作履歴を含む連携トラヒックを観測してしまうと、不正操作攻撃のヒントとなりうるため、自分が誰かという情報を隠しながら連携する方法を提案した。また、攻撃者が偽の情報を大量送信し、連携を妨害して不正操作攻撃を成功させようとすることも考えられるため、このような偽情報による悪影響を防止する方法についても提案している。これらの連携手法によって、各家庭の異常検知精度の向上も達成されている。

以上のように本論文は、ユーザの行動情報を用いた異常検知と、他家庭との連携による異常検知精度の向上を達成することで、スマートホームに対する不正操作攻撃検知を実現するために有用な研究成果を上げている。よって、博士（情報科学）の学位論文として価値のあるものと認める。