A-01

磁場監視に基づくマルウェアによるエネルギーハーベストの早期検出案

A proposal for early detection of energy harvesting by malware based on magnetic field monitoring

田中 卓† 田中恵子† 細見令香‡ 田中禎明[+3] 力石浩孝[+4]
Taku Tanaka Keiko Tanaka Reika Hosomi Tomoaki Tanaka Hirotaka Chikaraishi

1. はじめに

1.1 既存マルウェア検出手法の限界と新たな手法への展望

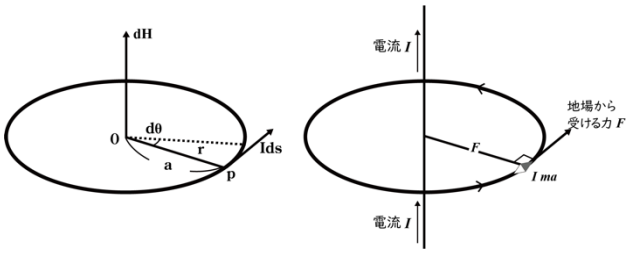
現行のマルウェア検出技術は署名ベースと行動ベースの二つが主流であるが、それぞれ新規や変異マルウェアへの対応や誤検知という課題を抱えている。署名ベースの手法は既知のマルウェアの特徴（署名）を検出するもので、新規や変異したマルウェアに対する検出力は限定的である。また、マルウェア開発者がマルウェアの特徴を頻繁に変更することで、この検出を回避することも可能である。一方、行動ベースの手法は、システム上での異常な動作を検出し、新規マルウェアに対する検出能力は高いが、誤検知率も高く、無害なプロセスをマルウェアと誤検出する問題が存在する。加えて、既存の手法はマルウェアがシステムに侵入し、何らかの活動を開始した後でしか検出できず、マルウェアによる損害を防止するための対策が遅れる可能性がある。これらの課題を解決するため、本研究では新たなマルウェア検出手法を提案する。それはシステムの電流と磁場のパターンを監視し、マルウェアによるエネルギーハーベストのパターンに基づいて異常を検出するものである。ビオ・サバールの法則とアンペールの法則に基づいており、既知だけでなく新規や変異したマルウェアの早期検出が可能となる。これにより、予防的な対策も取れるようになり、電子基板の磁場特性の監視と学習は現在のマルウェア検出手法の課題を解決する有望なアプローチとなる。

1.2 新規マルウェア検出方法の提案

本研究の新規マルウェア検出のアプローチは、システムの電流と磁場のパターンのモニタリングによるものである。この手法は、電子デバイスの電流と磁場の変動を監視し、その変動が正常な範囲を超えた場合にマルウェアの存在を示す。中核には、マルウェアがシステムに影響を及ぼし、エネルギーハーベスト（エネルギーの不正利用）を行うという考え方がある。正常な電流と磁場のパターンから逸脱した場合、それが既知、未知、変異したマルウェアの存在を示す可能性のあるエネルギーハーベストを検出する。このアプローチは、特に大量の計算能力を必要とし、したがって大量の電力を消費するマルウェアに対して有効であると予想される。一方で、低電力で動作するマルウェアや電力消費パターンを巧妙に偽装するマルウェアに対しては、この手法の有効性が低下する可能性がある。これらのマルウェアは、電流や磁場の変化を最小限に抑えることで、検出を避けることが可能である。しかし、本研究の提案する手法は、他のマルウェア検出技術と組み合わせて用いることで、その有効性を最大化することが可能となり、様々なタイプのマルウェアに対して広範で効果的な対策を提供し、システムのセキュリティを向上させる可能性がある。

1.3. 磁場特性の監視の重要性

新しいマルウェア検出手法として、電子基板上の磁場特性の監視と学習に注目する。磁場は、システムの電流パターンと密接に関連しており、これらのパターンがマルウェアの活動を反映する可能性がある。特定のシステムにおける正常な磁場特性を理解することは、異常な状況を検出するための基礎を提供する。例えば、通常の電力消費とは異なるパターンが検出された場合、これは電子基板上の磁場が異常な変動を示している可能性があり、エネルギーハーベストによる電流の急激な変化を反映していると考えられる。さらに、これらの磁場特性のパターンを機械学習モデルに学習させることで、モデルはシステムの状況変化に対応し、異常検出に重点を置くことが可能になる。つまり、正常なパターンからの逸脱を識別し、マルウェアの侵入を早期に検出し、適切に対応することが可能となる。このように、電子基板上の磁場特性の監視と学習は、マルウェア検出の新たなアプローチとして有望である。



2. エネルギーハーベストの影響評価

ビオ・サバールの法則とアンペールの法則は、磁場の挙動を理解するための重要な法則である。仮にシステムが通常状態で 1A の電流を流しており、マルウェアによるエネルギーハーベストが発生し電流が 2A に増加した場合を考えると、ビオ・サバールの法則によれば、特定の dl と r で計算される微小な磁場 dB は電流 I に比例するため、電流が 2 倍になると微小な磁場も 2 倍になる。また、アンペールの法則によれば、閉回路内の電流 I_enc が 2 倍になると、∮B・dl の値も 2 倍になる。これらの理論的な解釈は、電流の異常な増加が電子システムに及ぼす影響を理解するための重要なフレームワークを提供する。ビオ・サバールの法則とアンペールの法則を用いて、マルウェアによるエネルギーハーベストがシステムの電流パターンに与える影響を計算し、予測することが可能である。これらの法則を組み合わせて使用することで、システムに流れる電流の異常な増加とそれに伴う磁場の変化を定量的に評価し、異常な磁場パターンの早期検出が可能となる。これらの物理法則は、マルウェアによるエネルギーハーベストを早期に検知し、システムの安全性を維持する上で非常に重要である。マル

†京都大学, Kyoto University
‡元京都工業繊維大学, (Former) Kyoto Institute of Technology
3 元九州産業大学大学院, (Former) Kyushu Sangyo University
4 核融合科学研究所,National Institute for Fusion Science

ウェア侵入検出の評価指標としては次の 3 つを定義する。
1. 磁場の変化率 ΔB
2. ΔB の時間的な変化速度 v
3. システムパラメータの異常度 a
磁場の変化率ΔB は先ほど導入したものであり、具体的な計算式は以下の通りである。
ΔB = (B_measured - B_baseline) / B_baseline
次に、磁場の変化率の時間的な変化速度 v は、磁場がどれほど速く変化しているかを示す。これは磁場の変化率 ΔB の時間微分として定義できる。
v = d(ΔB)/dt
さらに、システムパラメータの異常度 a は、マルウェアの活動により変動する可能性のある他のシステムパラメータ（例えばCPU使用率、メモリ使用量など）の異常度を表す。これは各パラメータのベースラインからの偏差を正規化したものとして定義できる。
a = (P_measured - P_baseline) / P_baseline
ここで、P_measured は測定されたシステムパラメータの値、P_baselineはそのベースライン値である。これら 3 つの評価指標を用いて、マルウェア侵入の多次元評価関数 F を次のように定義する。
F = w_1 * ΔB + w_2 * v + w_3 * a
ここで、w_1、w_2、w_3 はそれぞれの評価指標の重みであり、これらは機械学習や統計的手法を用いて最適化される。重みは問題の性質や、各評価指標が全体の評価にどれだけ影響を与えるかにより決定される。したがって、上記の多次元評価関数 F を用いることで、複数の要素が複雑に絡み合うシステムの挙動を定量的に評価し、マルウェアの侵入を検出することが可能である。具体的なマルウェア侵入から検出までのプロセスは、先ほど述べた通りである。なお、重みの最適化には、例えば機械学習の手法である勾配降下法や確率的勾配降下法を用いることが考えられる。これらの手法は、評価関数の値を最小化（または最大化）するような重みを反復的に更新することで、最適な重みを求める。

3. 実験計画案

3.1 計測のモデリング

本章では、マルウェアによるエネルギーハーベストを早期に検出するための具体的な実験計画を提案する。基本的な目標は、ビオ・サバールの法則とアンペールの法則を利用して電流と磁場の間の関係を定量的に理解し、それによりエネルギーハーベストの検出を試みることである。具体的な手順としては、ハードウェアの設定、センサーの位置設定、Python スクリプトの設定、データ収集、異常状態のデータ収集、そしてデータ解析を挙げる。ラズベリーパイとディジタルコンパスモジュールを用いてシステムを構築し、電流の異常な増加が磁場に及ぼす影響を定量的に評価することで、異常な磁場パターンの早期検出が可能となることが期待される。磁場の異常な変化を検出することで、マルウェアによるエネルギーハーベストを早期に検出する方法を評価する。このプロセスは、ビオ・サバールの法則とアンペールの法則を使用して、電流と磁場の間の関係を定量的に理解することにより、エネルギーハーベストの検出に役立つ可能性がある。
1. ハードウェアの設定: ラズベリーパイを専用の電源に接続し、オペレーティングシステムを起動する。次に、MMC5603 3 軸ディジタルコンパスモジュールをラズベリーパイの GPIO ピンに接続する。このモジュールは I2C 通信プロトコルを使用し、ラズベリーパイの SDA と SCL ピンに接続する。
2. センサーの位置設定：センサーはシステム全体の電流分布を正確に計測するために、電流源の近くに配置する。具体的には、ラズベリーパイと同じ平面上、ラズベリーパイの中心から 5cm の距離に設置する。また、センサーは電流の方向に対して垂直に設置する。これにより、磁場の影響を最大限に捉えることができる。
3. Python スクリプトの設定: Python スクリプトは、MMC5603 から磁場データを収集し、タイムスタンプ付きのファイルに記録する。また、電流の変化を制御し、それに対応する磁場の変化をモニタリングする。このスクリプトは、初期状態（電流 1A）で 1000 回のデータ収集を行い、その後電流を 2A に増加させてから再度 1000 回のデータ収集を行う。各データ収集は 0.1 秒間隔で実施され、CSV ファイルにはタイムスタンプと磁場データ（X、Y、Z）、ならびに現在の電流値が記録される。
4. データ収集: Python スクリプトを実行し、初期状態（電流 1A）のデータを収集する。収集するデータは、時間、3 軸の磁場強度、電流値を含む。
5. 異常状態のデータ収集: 次に、システムの電流を 2A に増加させ、磁場データを再び収集する。このステップでは、異常な電流パターンが磁場にどのような影響を与えるかを観察する。
6. データ解析: Python スクリプトを使用してデータを解析し、1A の時と 2A の時の磁場の変化を計算する。電流が倍になった場合、磁場も理論的には倍になると推察できる。

3.2 計測箇所の考察

パソコンの電子基板上で磁場を計測する際の理想的な位置について考えると、最も電流の変化が顕著に現れると考えられる場所が適切であろう。具体的には、電力供給部（電源ユニット）やマザーボード上の VRM（電圧レギュレータモジュール）など、大量の電流が流れる部分が考えられる。なぜなら、これらの部分で電流の変化が生じると、それに伴って磁場の変化も大きくなり、その結果検出が容易になるからである。
1. 電源ユニット：電源ユニットは PC の全体的な電流供給を担当しており、全体的な電流の流れを捉えるのに適している。しかし、電源ユニットの内部は一般に密閉されているため、磁場センサーを適切に配置するのが難しい可能性がある。
2. VRM（電圧レギュレータモジュール）：マザーボード上の VRM は、CPU や GPU などの主要なコンポーネントに対して電力を供給する役割を担っている。これらのコンポーネントは大量の電力を消費するため、電流の変化が大きい。したがって、VRM 周辺は磁場変化の検出に適していると考えられる。
3. CPU や GPU：これらの主要なコンポーネントは高い電力を消費するため、それぞれが発生する電流の変化も大きい。しかし、これらの部品は高温になりやすく、また、物理的なスペースが限られているため、センサーを直接配置するのは困難である。以上の考察から、理想的な磁場の計測位置はマザーボード上の VRM 近辺であると言える。ここでは、電流の変化が大きく、センサーを配置するのに適したスペースが確保できる可能性がある。具体的には、センサーは VRM の近く、かつ電流の流れる方向に対して垂直に配置することで、磁場の変化を最大限に捉えることが可能となる。また、センサーは基板から適切な距離を保つことで、センサーが基板の熱によって影響を受けるのを防ぐことも重要である。

3.3 センサー装着

本研究では、マザーボード上の電圧レギュレータモジュール（VRM）近傍の磁場を、MMC5603 3 軸ディジタルコンパスモジュールを用いて観測する。以下に具体的な装着方法、設定方法、および検証方法を述べる。

1. MMC5603 3 軸ディジタルコンパスモジュールの装着:
このモジュールはマザーボード上の VRM 近傍に配置される。具体的には、センサーは VRM の直近で、電流の流れる方向に対して垂直に配置することで、電流に伴う磁場の変化を最大限に捉えることが可能となる。センサーは基板から適切な距離を保つことで、センサーが基板の熱によって影響を受けるのを防ぐ。この位置決めは 3D プリント技術を用いた専用のブラケットを製作することで実現される。ブラケットは、センサーと基板との間に適切な絶縁と距離を確保し、さらにセンサーを安定的に固定する役割を果たす。

2. MMC5603 3 軸ディジタルコンパスモジュールの設定:
センサーは、I2C 通信プロトコルを使用してラズベリーパイに接続される。Python スクリプトを用いて、センサーから磁場データを取得し、そのデータを CSV ファイルに記録する。このスクリプトは、各データ収集が 0.1 秒間隔で行われるように設定され、これによりリアルタイムの磁場変化を捉えることが可能となる。

3. 仮想的なマルウェアによる電力変化の検証:
初めに、マザーボードの電源を投入し、システムが通常動作している間にデータ収集を開始する。この初期状態でのデータ収集を通じて、システムの正常な状態下での磁場のパターンを理解する。次に、マルウェアが電力を奪取すると仮定した場合の電力増加を模擬し、その電力変化が磁場にどのように影響を与えるかを観察する。この電力増加は、電源の電流を制御することにより達成される。以上の方法を通じて、電流と磁場の間の関係を定量的に理解し、それにより仮想的なマルウェアによる電力変化の影響を評価することが可能となる。この研究が成功すれば、マルウェアの電力奪取行為を磁場の変化を通じて間接的に検知する新たな手法が開発されることになり、それによりシステムの異常な動作、特にマルウェアの侵入を早期に検出し、適切に対応することが期待される。

4. まとめと今後の研究計画

この研究計画では、コンピュータの電子基板上で電流の変化を通じてマルウェアの活動を検出する新たな手法を提案した。特に、電流の変化が最も大きいと予想される場所であるマザーボード上の電圧レギュレータモジュール（VRM）近傍で磁場を計測する方法を詳細に説明した。また、計測には MMC5603 3 軸ディジタルコンパスモジュールを用い、その装着方法、設定方法、検証方法について説明した。今後の研究では、まずこの実験計画を実行し、実際にマザーボード上の磁場変化を観測する。その結果を通じて、本研究の理論が実際の環境で機能するかどうかを検証する。さらに、観測された磁場のパターンを元に、マルウェアの活動を予測するためのモデルを開発する。これにより、マルウェアの活動がもたらす磁場のパターンを理解し、それに基づく異常検知アルゴリズムの設計を試みる。さらに、現実の環境でのマルウェアの活動とその電流消費のパターンについて詳細に調査し、本研究の理論を実際のマルウェア検出に応用するための基礎を作る。これにより、新たなタイプのマルウェアを早期に検出し、対策を講じることが可能となることを期待している。また、MMC5603 3 軸ディジタルコンパスモジュール以外のセンサーを使用した場合の効果についても調査する。これは、異なる種類のセンサーがもたらす潜在的な利点や欠点を理解し、最適なセンサー選択を促進するためである。最終的には、本研究が新たなマルウェア検出手法を提供し、セキュリティシステムの強化に寄与することを期待している。