【13】

| | |
|---|---|
| 氏名 | 大下裕一（おおした ゆういち） |
| 博士の専攻分野の名称 | 博士（情報科学） |
| 学位記番号 | 第　２２５４１　号 |
| 学位授与年月日 | 平成20年９月25日 |
| 学位授与の要件 | 学位規則第４条第２項該当 |
| 学位論文名 | Measurement, Analysis and Control to Changes of Network Traffic<br>（ネットワークトラヒックの変動の観測、解析、および適応制御に関する研究） |
| 論文審査委員 | （主査）<br>教授　村田　正幸<br>（副査）<br>教授　今瀬　真　　教授　村上　孝三　　教授　東野　輝夫<br>教授　中野　博隆 |

## 論文内容の要旨

通常、ネットワークは想定したトラヒックを効率よく収容するように設計されるが、現在のトラヒックが想定されたトラヒックから大きくかけ離れた場合、効率よく収容することが出来ず、ネットワークの性能を著しく悪化させてしまう。また、サーバにおいても、想定外の大量のリクエストが到着した場合、すべてのリクエストに対応することができない。このような想定外のトラヒックが発生してしまう原因としては、悪意のあるトラヒックの混入と、通常なトラヒックの増加の２種類があり、本論文では、観測結果を元に、両方の場合に対応する手法を提案した。

悪意のあるトラヒックが混入した場合は、迅速に検出し、悪意のあるトラヒックを遮断しつつ、正常なトラヒックを保護して転送する必要がある。そこで、本論文では、(1)通常の接続要求の到着レートが正規分布に従っているということを利用し、迅速に攻撃を検出する手法、(2)各ルータで観測されているリンク使用率から、対地間のトラヒック増加量を推定することにより、攻撃元を特定する手法。(3)ISPの出口において、被害者宛の正常なトラヒックを識別し、オーバーレイネットワークを用いて転送することにより保護する手法の3種類の手法を提案した。そして、シミュレーションにより、提案手法が(1)20SYNs/sec以下の攻撃であっても既存の手法よりも早く攻撃が検出可能であること、(2)リンク使用率のみを用いた場合でも正確に攻撃元を特定できること、(3)攻撃中においても正常なパケットがロスしてしまう確率を0.1以下に抑えることが可能であるということを示した。

それに対して、正常なトラヒックが増加した場合は、トラヒックを遮断するといった対処を行うことはできない。そこで、現在のトラヒックを効率よく収容できるように、ネットワークの設定を再度組みなおすトラヒックエンジニアリング（TE）と呼ばれる手法を用いる。TEでは、トラヒックマトリクスと呼ばれる対地間のトラヒック量を入力として用いる必要があるが、トラヒックマトリクスは直接観測することは一般的に困難であり、また、リンク使用率等から推定した場合にも推定誤差がTEへ影響を与え、適切な制御が行うことができない可能性がある。この問題に対して、本論文では、ネットワークの再構成を行いつつ、リンク使用率の観測を行い、観測した結果をトラヒックマトリクス推定にフィードバックを行うことにより、トラヒックマトリクスの推定精度を向上する手法を提案した。そして、シミュレーションにより提案手法が推定されたトラヒックマトリクスに含まれる相対誤差を0.1以下まで削減することができ、それを用いて適切にTEを行う

ことができることを確認した。

**これらの検討を通じ、ネットワーク内におけるリンク使用率等の観測結果を用い、トラヒックが急変した場合も、その原因を切り分け、適切にネットワークの制御を行うことにより、ネットワークの性能劣化を防ぐことができることを明らかにした。**

## 論文審査の結果の要旨

通常、ネットワークは想定したトラヒックを効率よく収容するように設計されるため、現在のトラヒックの特性が想定から大きくかけ離れた場合、ネットワークの性能が著しく悪化してしまう。また、サーバにおいても、想定外の大量のリクエストが到着した場合、すべてのリクエストに対応することができない。このような想定外のトラヒックが発生してしまう原因としては、悪意のあるトラヒックの混入と、通常なトラヒックの増加の２種類があり、本論文では、観測結果を元に、両方の場合に対応する手法を提案している。

まず、本論文では、悪意のあるトラヒックの混入に対応する手法として、(1)通常の接続要求の到着レートが正規分布に従っているということを利用し、迅速に攻撃を検出する手法、(2)各ルータで観測されているリンク利用率から、対地間のトラヒック増加量を推定することにより、攻撃元を特定する手法、(3)ISPの出口において、被害者宛の正常なトラヒックを識別し、オーバーレイネットワークを用いて転送することにより保護する手法の3種類の手法を提案している。そして、シミュレーションにより、提案手法が(1)20SYNs/sec以下の攻撃であっても既存の手法よりも早く攻撃が検出可能であること、(2)リンク利用率のみを用いた場合でも正確に攻撃元を特定できること、(3)攻撃中においても正常なパケットがロスしてしまう確率を0.1以下に抑えることが可能であるということを示している。

次に、本論文では、正常なトラヒックが増加に対応する手法として、現在のトラヒックを効率よく収容できるように、ネットワークの設定を再度組みなおすトラヒックエンジニアリング（TE）と呼ばれる手法について検討を行っている。TEを行うためには、トラヒックマトリクスと呼ばれる対地間のトラヒック量を入力として用いる必要があるが、トラヒックマトリクスは直接観測することは一般的に困難であり、また、リンク使用率等から推定した場合にも推定誤差がTEへ影響を与え、適切な制御が行うことができないという問題がある。この問題に対して、本論文では、ネットワークの再構成を行いつつ、リンク使用率の観測を行い、観測した結果をトラヒックマトリクス推定にフィードバックを行うことにより、トラヒックマトリクスの推定精度を向上する手法を提案している。そして、シミュレーションにより提案手法が推定されたトラヒックマトリクスに含まれる相対誤差を0.1以下まで削減することができ、それを用いて適切にTEを行うことができることを示している。

以上のように、本論文では、トラヒック変動に対して適応的に動作するネットワークの実現に向けた多くの研究成果を挙げている。よって、博士(情報科学）の学位論文として価値あるものと認める。