Botnets in 4G Cellular Networks

Platforms to Launch DDoS Attacks Against the Air Interface

Masood Khosroshahy, Dongyu Qiu, and Mustafa K. Mehmet Ali

ECE Dept., Concordia University, Canada

The Third International Conference on Selected Topics in Mobile and Wireless Networking (MoWNet'2013)
Montreal, Canada
Aug 20, 2013

Outline

1. Introduction
   - Threats Posed by Botnets
   - Motivation to Study Botnets in Cellular Networks
2. Botnets in 4G Cellular Networks
   - Identification and Evaluation of Botnet Threat
   - Simulation Scenario and Results
3. Summary and Our Related Work
   - Summary of Contributions and Future Work
   - Our Related Work: Analytical Lifecycle Models

Outline

What is a botnet and how is it constructed?

Botnet:

- Network of (ro)bots
- An overlay network of compromised computers

Initial Infection

- E-mail attachments
- File sharing sites
- P2P networks
- Windows vulnerabilities
- Web browser vulnerabilities

Joining the Botnet

Centralized: connect to the C&C (IRC) server

Peer-to-peer: find other peers to join the botnet

Botnet in Operation

Node receives commands of the botmaster for:

- taking part in illicit activities
- updating/managing the malware

What is a botnet and how is it constructed?

Botnet:

- Network of (ro)bots
- An overlay network of compromised computers

Initial Infection

- E-mail attachments
- File sharing sites
- P2P networks
- Windows vulnerabilities
- Web browser vulnerabilities

Joining the Botnet

Centralized: connect to the C&C (IRC) server

Peer-to-peer: find other peers to join the botnet

Botnet in Operation

Node receives commands of the botmaster for:

- taking part in illicit activities
- updating/managing the malware

What is a botnet and how is it constructed?

Botnet:

- Network of (ro)bots
- An overlay network of compromised computers

Initial Infection

- E-mail attachments
- File sharing sites
- P2P networks
- Windows vulnerabilities
- Web browser vulnerabilities

Joining the Botnet

Centralized: connect to the C&C (IRC) server

Peer-to-peer: find other peers to join the botnet

Botnet in Operation

Node receives commands of the botmaster for:

- taking part in illicit activities
- updating/managing the malware

What is a botnet and how is it constructed?

Botnet:

- Network of (ro)bots
- An overlay network of compromised computers

Initial Infection

- E-mail attachments
- File sharing sites
- P2P networks
- Windows vulnerabilities
- Web browser vulnerabilities

Joining the Botnet

Centralized: connect to the C&C (IRC) server

Peer-to-peer: find other peers to join the botnet

Botnet in Operation

Node receives commands of the botmaster for:

- taking part in illicit activities
- updating/managing the malware

Botnets are being used for a host of illicit activities

- sending e-mail spams:
  - November 2008: takedown of few botnets led to an instant drop of 80% in e-mail spam volume.
- launching Distributed Denial-of-Service (DDoS) attacks:
  - The country of Estonia came under a DDoS attack in April 2007 which knocked off critical infrastructure and the media.
- engaging in click fraud against syndicated search engines:
  - Google reports having detected a botnet of 100,000 nodes committing click fraud.

Botnets are being used for a host of illicit activities

- sending e-mail spams:
  - November 2008: takedown of few botnets led to an instant drop of 80% in e-mail spam volume.
- launching Distributed Denial-of-Service (DDoS) attacks:
  - The country of Estonia came under a DDoS attack in April 2007 which knocked off critical infrastructure and the media.
- engaging in click fraud against syndicated search engines:
  - Google reports having detected a botnet of 100,000 nodes committing click fraud.

Botnets are being used for a host of illicit activities

- sending e-mail spams:
  - November 2008: takedown of few botnets led to an instant drop of 80% in e-mail spam volume.
- launching Distributed Denial-of-Service (DDoS) attacks:
  - The country of Estonia came under a DDoS attack in April 2007 which knocked off critical infrastructure and the media.
- engaging in click fraud against syndicated search engines:
  - Google reports having detected a botnet of 100,000 nodes committing click fraud.

Outline

Motivation to Study Botnets in Cellular Networks

- As the convergence of Internet and traditional telecommunication services is underway, the threat of botnets is looming over essential basic communication services.
- Examples of cellular botnets are iKee.A/B which were released in 2009 and targeted iPhone users in several countries
  - 21,000 infected iPhone users in Australia alone

Motivation to Study Botnets in Cellular Networks

- As the convergence of Internet and traditional telecommunication services is underway, the threat of botnets is looming over essential basic communication services.
- Examples of cellular botnets are iKee.A/B which were released in 2009 and targeted iPhone users in several countries
  - 21,000 infected iPhone users in Australia alone

Earlier Research on 2G/3G Cellular Networks

- A DDoS attack on the Home Location Register (HLR) has been tested:
  - A DDoS attack that can successfully overload the HLR would make the network unusable for the clients.
  - "Insert/Delete Call Forwarding" is the most demanding request that can be sent by the handsets that needs to be processed by the HLR.
  - Up to 141,000 botnet nodes needed (infection rate of 14.1%.)

Outline

Identification/Evaluation of Botnet Threat in 4G Networks

- Contribution of this paper:
  - Identification and evaluation of botnet threat against the LTE air interface in 4G networks
  - We consider the air interface as the main target of the DDoS attack
- Through simulation using an LTE simulator, we determine the number of botnet nodes per cell that can significantly degrade the service availability of such cellular networks.

Identification/Evaluation of Botnet Threat in 4G Networks

- Contribution of this paper:
  - Identification and evaluation of botnet threat against the LTE air interface in 4G networks
  - We consider the air interface as the main target of the DDoS attack
- Through simulation using an LTE simulator, we determine the number of botnet nodes per cell that can significantly degrade the service availability of such cellular networks.

Evaluation of Botnet Threat in 4G Networks

- In order to do performance evaluations of the LTE air interface, one of the best options is to use the LTE-Sim simulator; it has an implementation of:
  - physical layer
  - radio resource schedulers
  - applications (Voice over IP [VoIP], video, etc.)
  - i.e., a full protocol stack
- The total botnet size is equal to the number of botnet nodes per cell times the number of cells.

Evaluation of Botnet Threat in 4G Networks

- In order to do performance evaluations of the LTE air interface, one of the best options is to use the LTE-Sim simulator; it has an implementation of:
  - physical layer
  - radio resource schedulers
  - applications (Voice over IP [VoIP], video, etc.)
  - i.e., a full protocol stack
- The total botnet size is equal to the number of botnet nodes per cell times the number of cells.

Evaluation of Botnet Threat in 4G Networks (cont.)

- In each simulation run, there are:
  - a number of botnet nodes that are configured to download video simultaneously
  - and other normal nodes (users) in the simulation that would be using VoIP in the meantime
- We examine the relationship between the number of botnet nodes and the level of degradation of service quality for the VoIP users.

Evaluation of Botnet Threat in 4G Networks (cont.)

- In each simulation run, there are:
    - a number of botnet nodes that are configured to download video simultaneously
    - and other normal nodes (users) in the simulation that would be using VoIP in the meantime
- We examine the relationship between the number of botnet nodes and the level of degradation of service quality for the VoIP users.

Outline

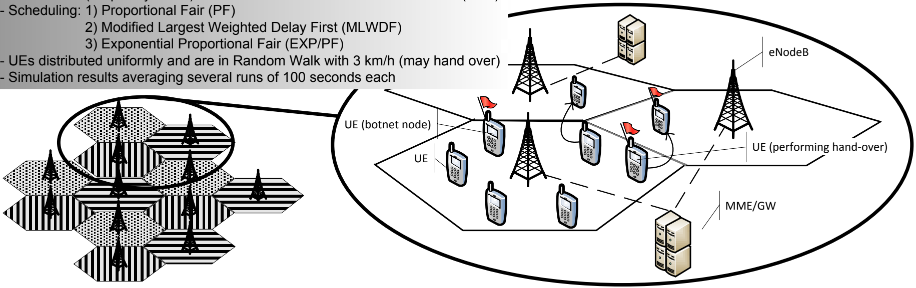
1. Introduction
   - Threats Posed by Botnets
   - Motivation to Study Botnets in Cellular Networks
2. Botnets in 4G Cellular Networks
   - Identification and Evaluation of Botnet Threat
   - Simulation Scenario and Results
3. Summary and Our Related Work
   - Summary of Contributions and Future Work
   - Our Related Work: Analytical Lifecycle Models

Simulation Scenario

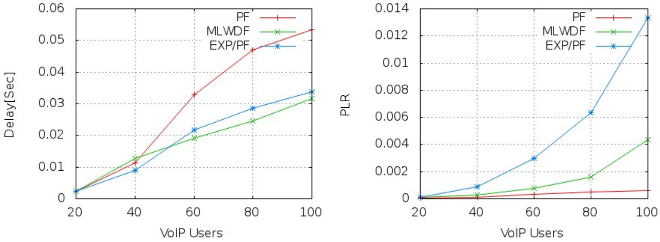
Attack scenario: botmaster instructing the botnet nodes to start downloading dummy data to overwhelm the air interface

Simulation Scenario:

- User Equipment (UE) connected to eNodeB of each cell with radius of 1 km
- eNodeBs connected to Mobility Management Entity/Gateway (MME/GW)
- Cluster size (frequency reuse) of 3 cells with 5 MHz downlink in each cell (FDD)
- Scheduling: 1) Proportional Fair (PF)
  2) Modified Largest Weighted Delay First (MLWDF)
  3) Exponential Proportional Fair (EXP/PF)
- UEs distributed uniformly and are in Random Walk with 3 km/h (may hand over)
- Simulation results averaging several runs of 100 seconds each



Simulation Results: Cell Capacity



- Downlink Schedulers:
  - Treating every flow the same: Proportional Fair (PF)
  - Optimized for real-time flows:
    - Modified Largest Weighted Delay First (MLWDF)
    - Exponential Proportional Fair (EXP/PF)
- Cell capacity is around 100 VoIP users.

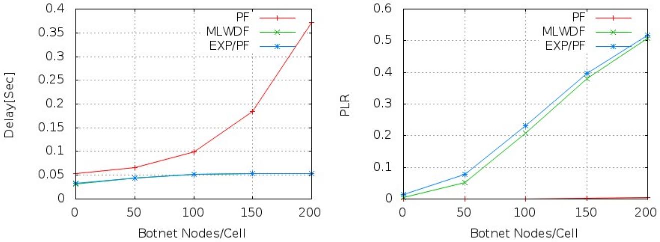
Simulation Results: Cell Capacity (cont.)

- Cell capacity is around 100 VoIP users ($\approx$ 3,300 subscribers).
- Subscribers number: based on reports on user behavior regarding average monthly phone conversations
  - Each subscriber is actively using the system resources (i.e., it becomes one of the 100 simultaneous VoIP users) about 3% of the time each day.
  - We can now consider that the maximum number of simultaneous VoIP users is about 3% of the average number of subscribers that are present in each cell.
- Mean Opinion Score (MOS) value for a voice communication ranges from 1 (impossible to communicate) to 5 (very satisfied).
  - At 50% packet loss, we will have a MOS value of 1.

Simulation Results: Cell Capacity (cont.)

- Cell capacity is around 100 VoIP users ($\approx$ 3,300 subscribers).
- Subscribers number: based on reports on user behavior regarding average monthly phone conversations
  - Each subscriber is actively using the system resources (i.e., it becomes one of the 100 simultaneous VoIP users) about 3% of the time each day.
  - We can now consider that the maximum number of simultaneous VoIP users is about 3% of the average number of subscribers that are present in each cell.
- Mean Opinion Score (MOS) value for a voice communication ranges from 1 (impossible to communicate) to 5 (very satisfied).
  - At 50% packet loss, we will have a MOS value of 1.

Simulation Results: Botnet Size



- At capacity, we add an increasing number of botnet nodes:
  - PF scheduler: PLR acceptable, delay large.
  - MLWDF and EXP/PF schedulers: PLR large, delay acceptable.

Simulation Results: Botnet Size (cont.)

- 100 botnet nodes and 200 botnet nodes represent a 3% infection rate and a 6% infection rate, respectively, among the subscribers in each cell.
- A botnet that has spread to only 3% of subscribers is capable of lowering the voice quality from 4.3 to 2.8 (MOS).
- On the other hand, a botnet that has managed to spread to 6% of subscribers can cause a MOS value of 1, i.e., a complete outage.

Simulation Results: Botnet Size (cont.)

- 100 botnet nodes and 200 botnet nodes represent a 3% infection rate and a 6% infection rate, respectively, among the subscribers in each cell.
- A botnet that has spread to only 3% of subscribers is capable of lowering the voice quality from 4.3 to 2.8 (MOS).
- On the other hand, a botnet that has managed to spread to 6% of subscribers can cause a MOS value of 1, i.e., a complete outage.

Simulation Results: Botnet Size (cont.)

- 100 botnet nodes and 200 botnet nodes represent a 3% infection rate and a 6% infection rate, respectively, among the subscribers in each cell.
- A botnet that has spread to only 3% of subscribers is capable of lowering the voice quality from 4.3 to 2.8 (MOS).
- On the other hand, a botnet that has managed to spread to 6% of subscribers can cause a MOS value of 1, i.e., a complete outage.

Outline

Summary of Contributions

- We identified a potentially devastating threat against the LTE/4G cellular networks: launch of a DDoS attack against the **air interface**:
  - simple to implement
  - does not require inside knowledge about core network elements
- Through the simulations, we determined that a botnet that has spread to only 6% of subscribers can effectively cause an outage in cellular services.
  - Earlier research has shown a needed infection rate of 14.1% in 2G/3G networks

Summary of Contributions

- We identified a potentially devastating threat against the LTE/4G cellular networks: launch of a DDoS attack against the **air interface**:
  - simple to implement
  - does not require inside knowledge about core network elements
- Through the simulations, we determined that a botnet that has spread to only 6% of subscribers can effectively cause an outage in cellular services.
  - Earlier research has shown a needed infection rate of 14.1% in 2G/3G networks

Future Work

- Investigation of the potential mitigation techniques in order to reduce and possibly eliminate the threat of air interface falling victim to a DDoS attack
  - e.g. enhancement of the CAC
- Determining how a botnet could attack a core network element in 4G systems
  - e.g. Home Subscriber Server of IMS

Outline

Modeling Techniques and Assumptions

- Nodes go through different stages in the lifetime of the botnet: *Susceptible*, *Infected* and *Connected*.
- State of the system: number of nodes in each stage.
- System modeled by Continuous-Time Markov Chain (CTMC).
- From the CTMC models, we derive:
  - either the probability distribution of number of nodes in each stage – *more difficult*.
  - or at least the mean/variance of number of nodes in each stage directly and without the probability distribution derivation – *easier*.

Modeling Techniques and Assumptions

- Nodes go through different stages in the lifetime of the botnet: *Susceptible*, *Infected* and *Connected*.
- State of the system: number of nodes in each stage.
- System modeled by Continuous-Time Markov Chain (CTMC).
- From the CTMC models, we derive:
  - either the probability distribution of number of nodes in each stage – *more difficult*.
  - or at least the mean/variance of number of nodes in each stage directly and without the probability distribution derivation – *easier*.

Modeling Techniques and Assumptions

- Nodes go through different stages in the lifetime of the botnet: *Susceptible*, *Infected* and *Connected*.
- State of the system: number of nodes in each stage.
- System modeled by Continuous-Time Markov Chain (CTMC).
- From the CTMC models, we derive:
  - either the probability distribution of number of nodes in each stage – *more difficult*.
  - or at least the mean/variance of number of nodes in each stage directly and without the probability distribution derivation – *easier*.

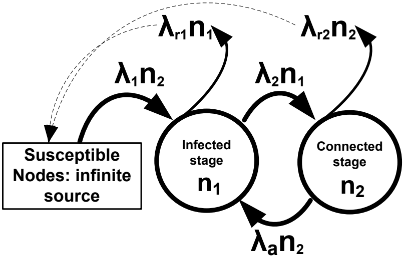
Modeling Techniques and Assumptions

- Nodes go through different stages in the lifetime of the botnet: *Susceptible*, *Infected* and *Connected*.
- State of the system: number of nodes in each stage.
- System modeled by Continuous-Time Markov Chain (CTMC).
- From the CTMC models, we derive:
  - either the probability distribution of number of nodes in each stage – *more difficult*.
  - or at least the mean/variance of number of nodes in each stage directly and without the probability distribution derivation – *easier*.

SIC: Susceptible-Infected-Connected

2-dimensional birth-death process: inter-stage-rate diagram

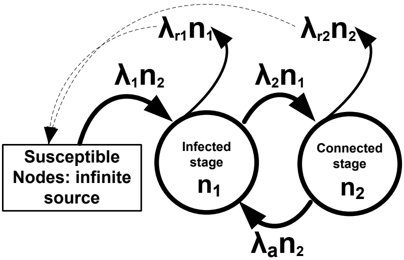
- Node stages considered:
  - **S**usceptible: a node is susceptible to be infected.
  - **I**nfected: the node has been infected, but it is not infectious.
  - **C**onnected:
    - The infected node has joined the botnet and is infectious now.
    - Botnet size = number of nodes that are in Connected stage.



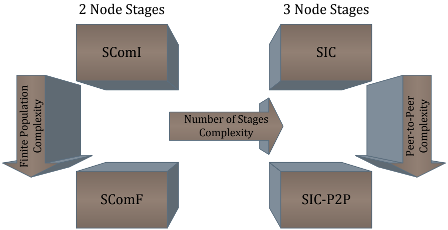
SIC: Susceptible-Infected-Connected

2-dimensional birth-death process: inter-stage-rate diagram

- SIC model incorporates both botnet mitigation strategies:
  - Removal rates from two stages due to disinfection of nodes.
    - Attacks on botnets: nodes lose the ability to communicate (they might be able to reconnect again).

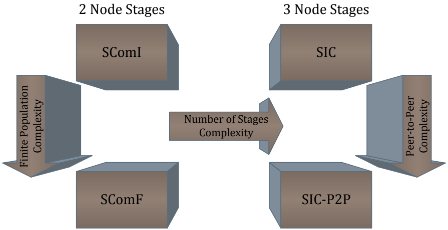


Botnet Models: The Big Picture



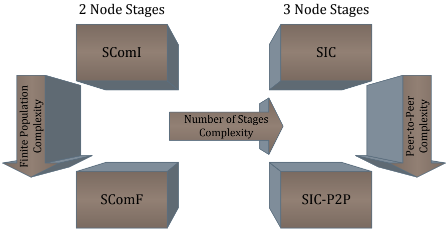
- Main aspects of the developed botnet models:
  - SComI/SComF: 1) Initial expansion; 2) Probability distribution
  - SIC/SIC-P2P: 1) Full lifecycle analysis; 2) Mean/variance
- Time-dependent (transient) closed-form expressions for derived probability distributions and means/variances.
- Values for model parameters can come from measurements.

Botnet Models: The Big Picture



- Main aspects of the developed botnet models:
  - SComI/SComF: 1) Initial expansion; 2) Probability distribution
  - SIC/SIC-P2P: 1) Full lifecycle analysis; 2) Mean/variance
- Time-dependent (transient) closed-form expressions for derived probability distributions and means/variances.
- Values for model parameters can come from measurements.

Botnet Models: The Big Picture



- Main aspects of the developed botnet models:
    - SComI/SComF: 1) Initial expansion; 2) Probability distribution
    - SIC/SIC-P2P: 1) Full lifecycle analysis; 2) Mean/variance
- Time-dependent (transient) closed-form expressions for derived probability distributions and means/variances.
- Values for model parameters can come from measurements.

Thank you for your attention!

Q&A