Десятая независимая научно-практическая конференция «Разработка ПО 2014»

23 - 25 октября, Москва

IP Fast Hopping Protocol Design

Vladimir Krylov and Kirill Kravtsov

Nizhny Novgorod State Technical University

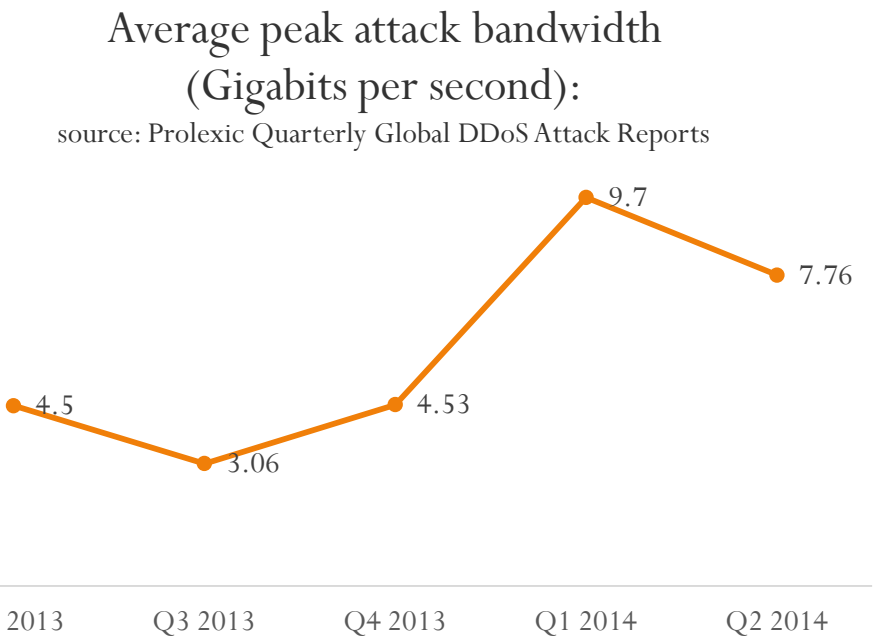
n.a. R.E. Alekseev

Outline:

- Why we need a new DDoS protection mechanism?
- What principles we should follow?
- Main idea
- Frequency hopping
- Simplest scenario of brute-force DDoS attack
- IP Fast Hopping architecture
- IP Fast Hopping algorithm
- Basic implementation
- IP Fast Hopping advantages
- IP Fast Hopping limitations
- Conclusion

Why we need a new DDoS protection mechanism?

- A Denial-of-Service (DoS) attack is characterized by an explicit attempt to prevent the legitimate use of a service
- A Distributed Denial-of-Service (DDoS) attack deploys multiple attacking entities to attain this goal



What principles we should follow?

1. Real world applicability
   - software-based solution
   - re-use of already widely used technologies
2. The solution must be designed to prevent misuse
   - robustness of already established connections

The main idea

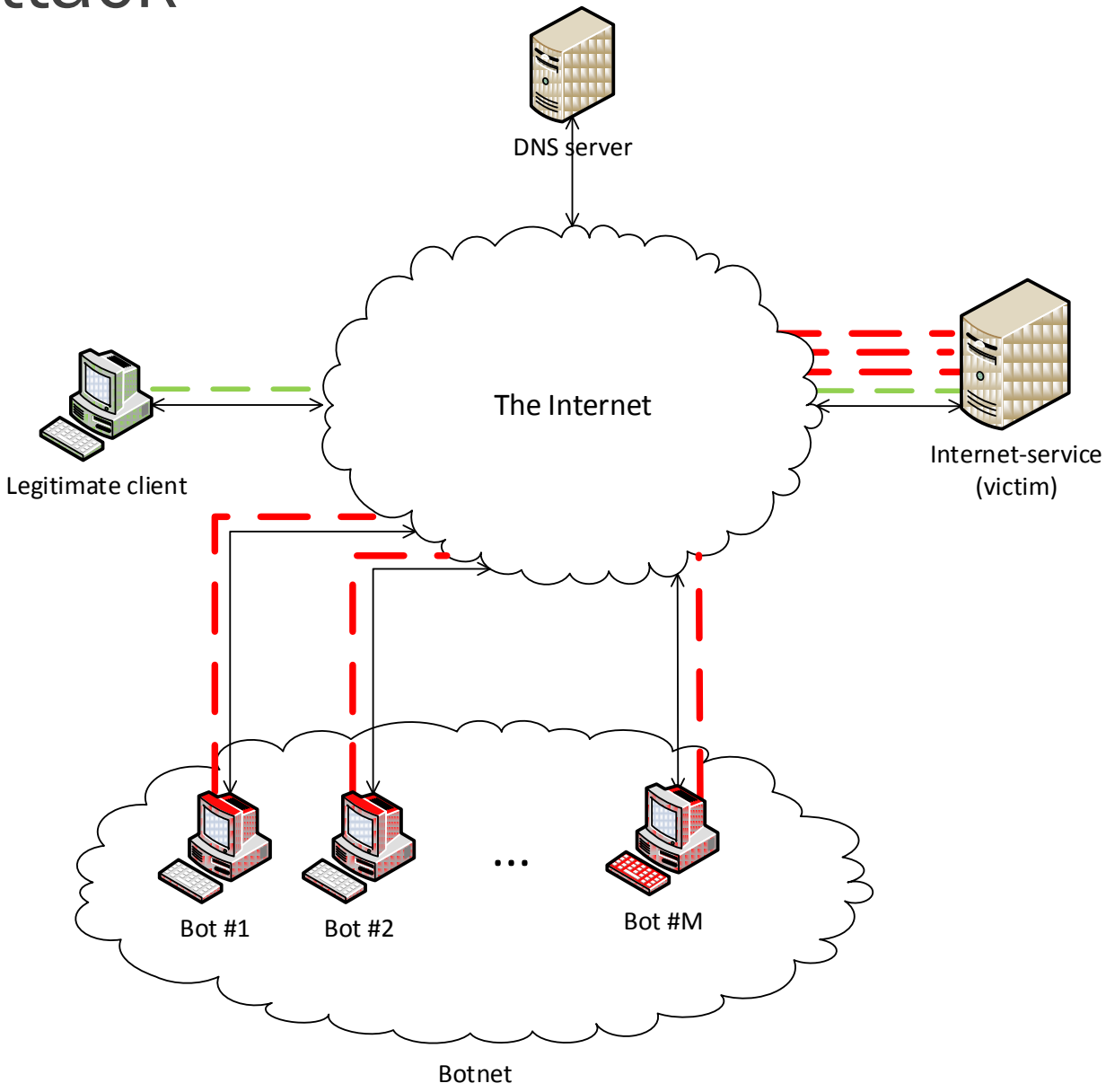
IP Fast Hopping is based on dynamic pseudorandom calculation of valid server’s IP address for each packet of each client session

Frequency hopping

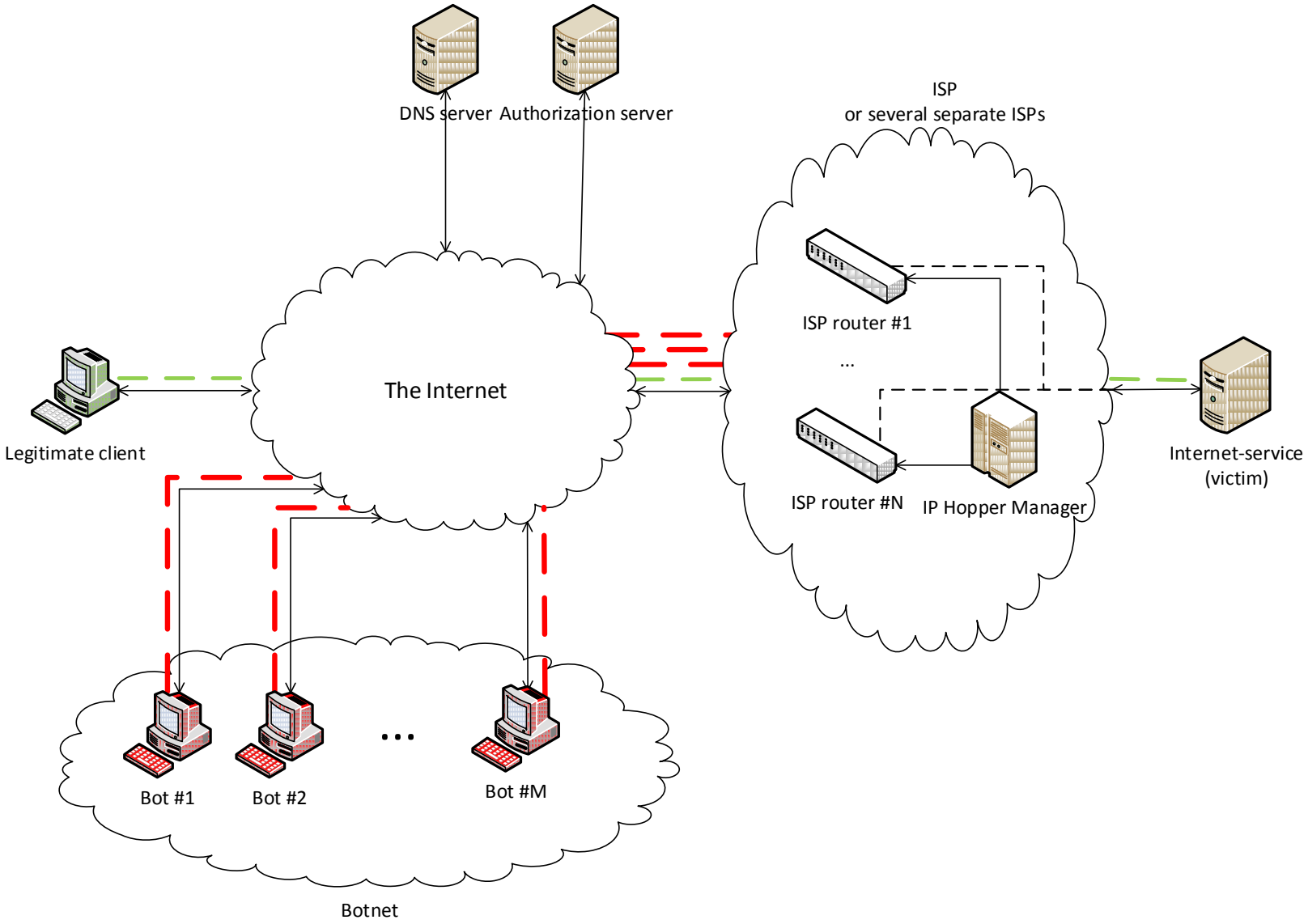
The method is similar to frequency hopping:

Receiver and transmitter are switching from one frequency to other frequency synchronously during an ongoing data transmission session

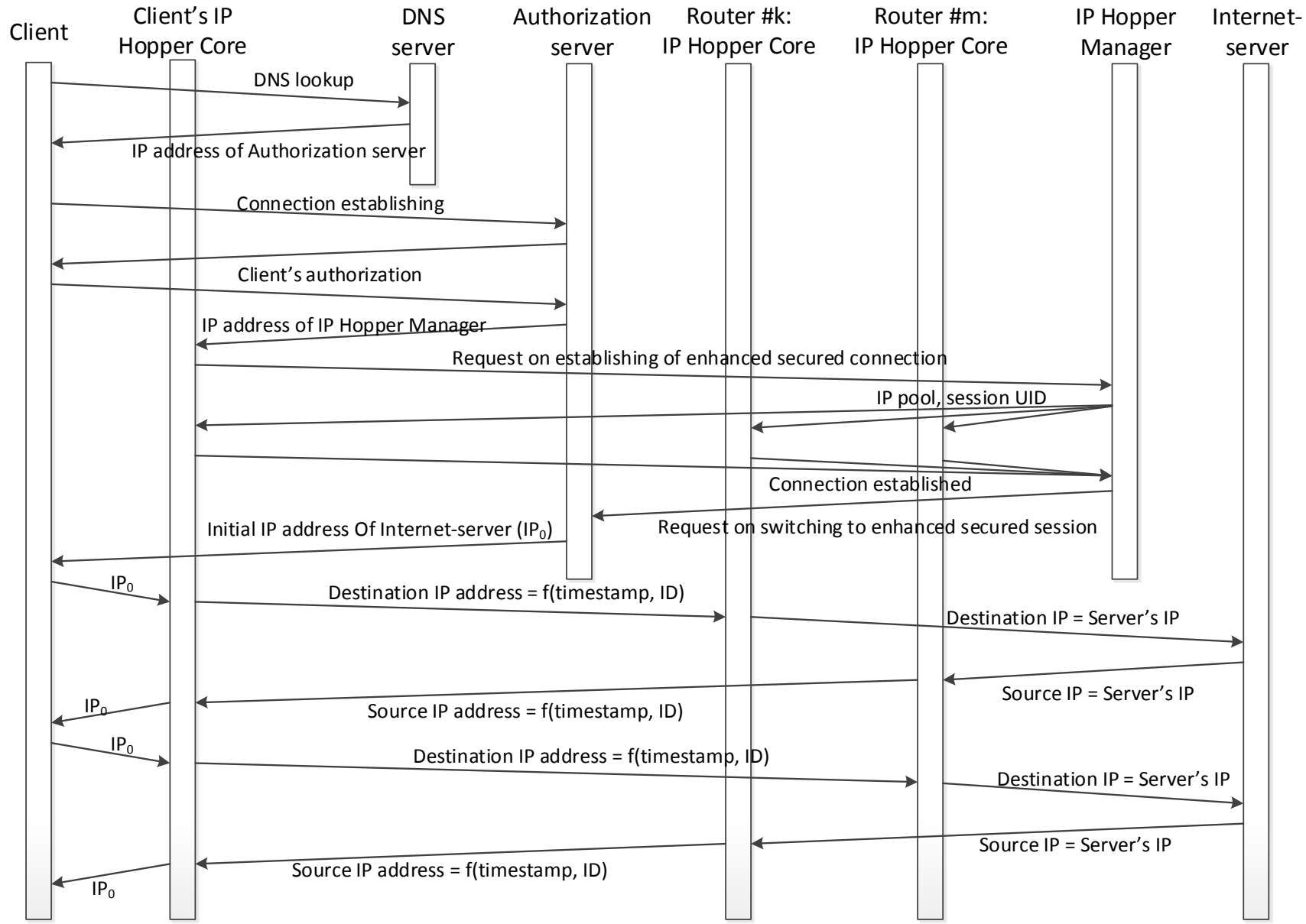
Simplest scenario of brute-force DDoS attack



IP Fast Hopping architecture

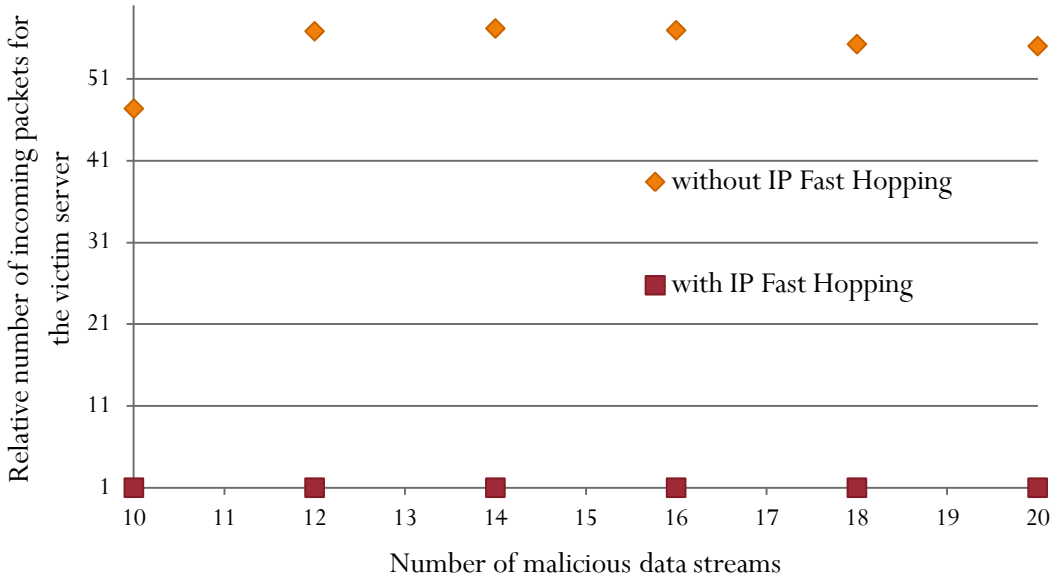


IP Fast Hopping algorithm



Basic implementation

IP Hopper Core is new module of Linux build-in firewall Netfilter.



IP Fast Hopping advantages

- Software solution utilizes existing network protocols
- Resistance to traffic interception
- Server’s protection against unauthorized access
- Hidden data destination

IP Fast Hopping limitations

- This particular implementation is limited to protect against TCP-based attacks
- Unprotected Authorization server
- Requires clients authorization

Conclusion

- We presented the new approach to prevent brute-force DDoS attacks
- The same method can be used to hide content and destination of communication session

Десятая независимая научно-практическая конференция «Разработка ПО 2014»

23 - 25 октября, Москва

Thank you

vkrylov@heterarchica.com

kirill@kravtsov.biz