IoT DDoS Attacks Detection based on SDN

RAMTIN ARYAN

Why DDoS Attack on IoT

- On Friday, October 21 2016, a series of Distributed Denial of Service (DDoS) attacks caused widespread disruption of legitimate internet activity in the US.

- The attacks were perpetrated by directing huge amounts of bogus traffic at targeted servers, namely those belonging to Dyn, a company that is a major provider of DNS services to other companies.

- This made it hard for some major websites to work properly, including Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, and the Playstation network.

- The attacks were made possible by the large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras.

[1].https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

Why DDoS Attack on IoT

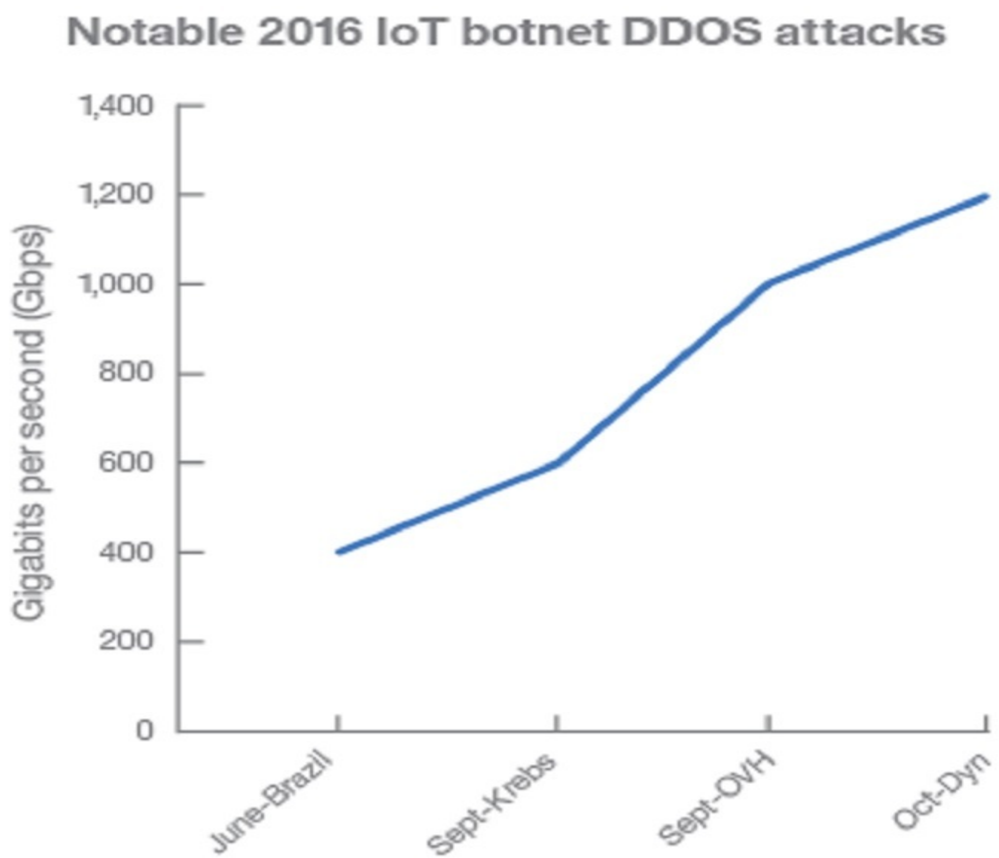
- One of the most important changes, the rising use of compromised Internet of Things (IoT) devices in botnet operations.

- The IBM X-Force team has been tracking the threat from weaponized IoT devices, also known as thingbots in 2016.

- In October 2016, reports of an IoT DDoS botnet attack against a different target revealed an approximately 200 percent size increase over the attack reported in June 2016.

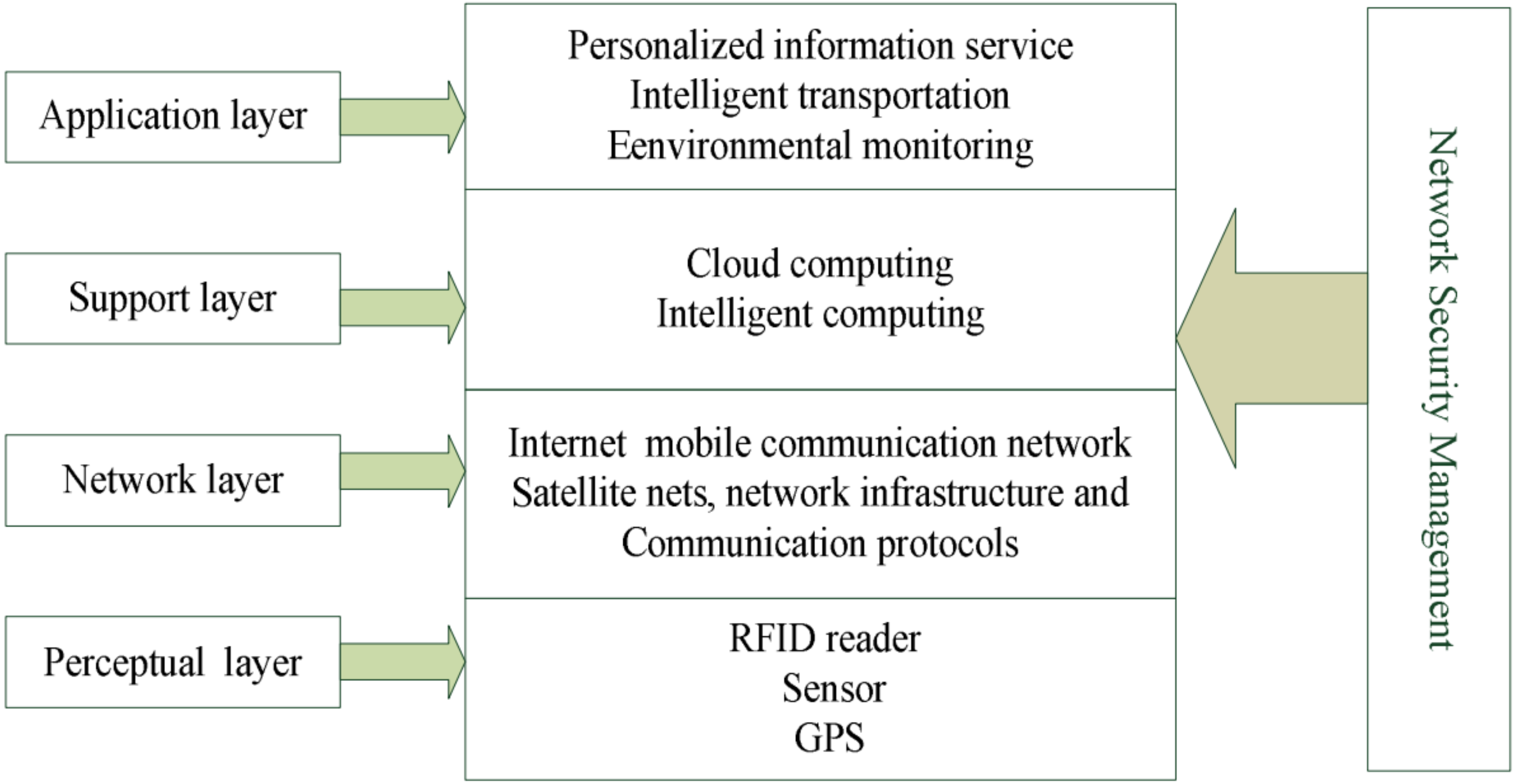
[1]. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

Why DDoS Attack on IoT



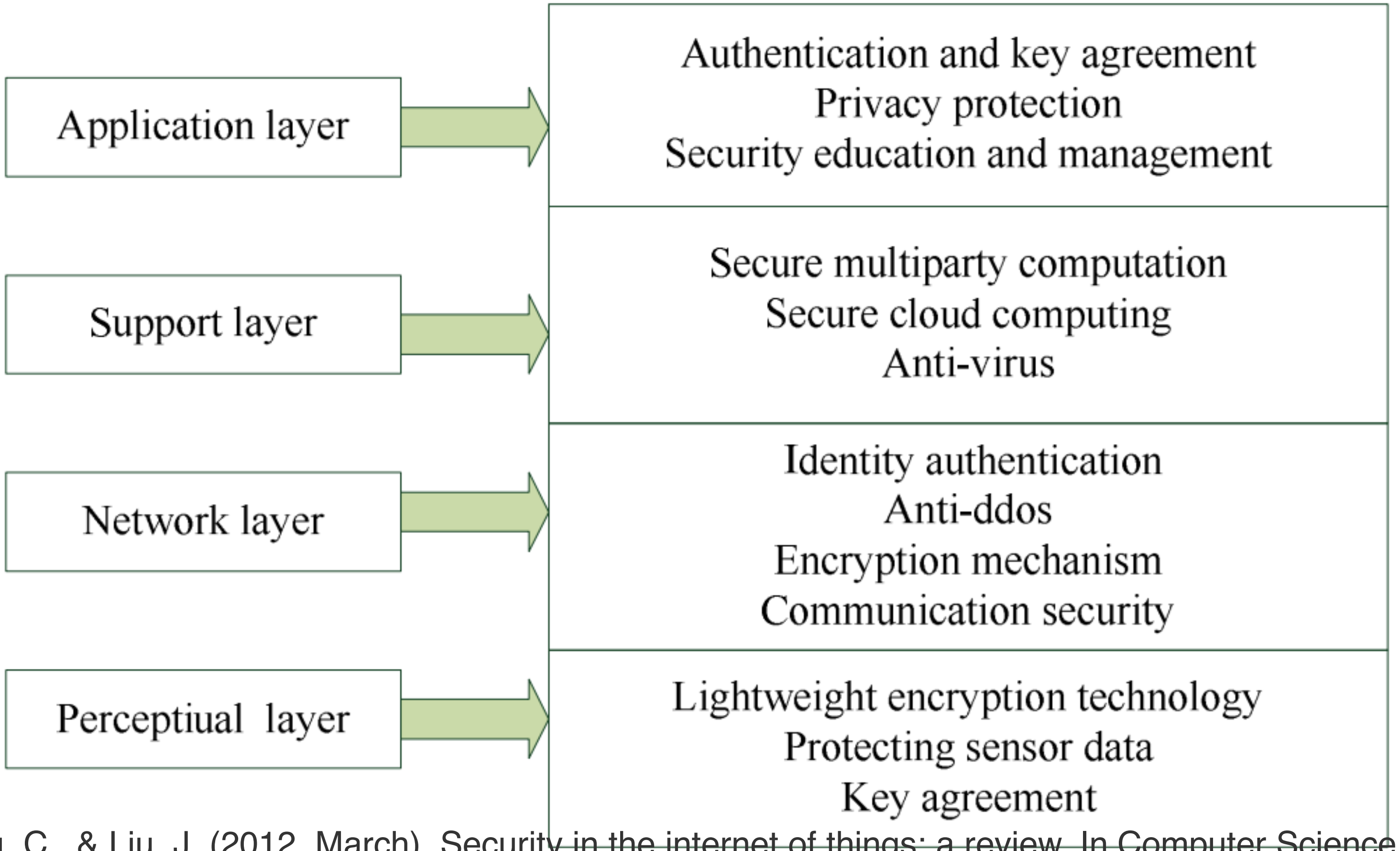
[1]. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

IoT Architecture



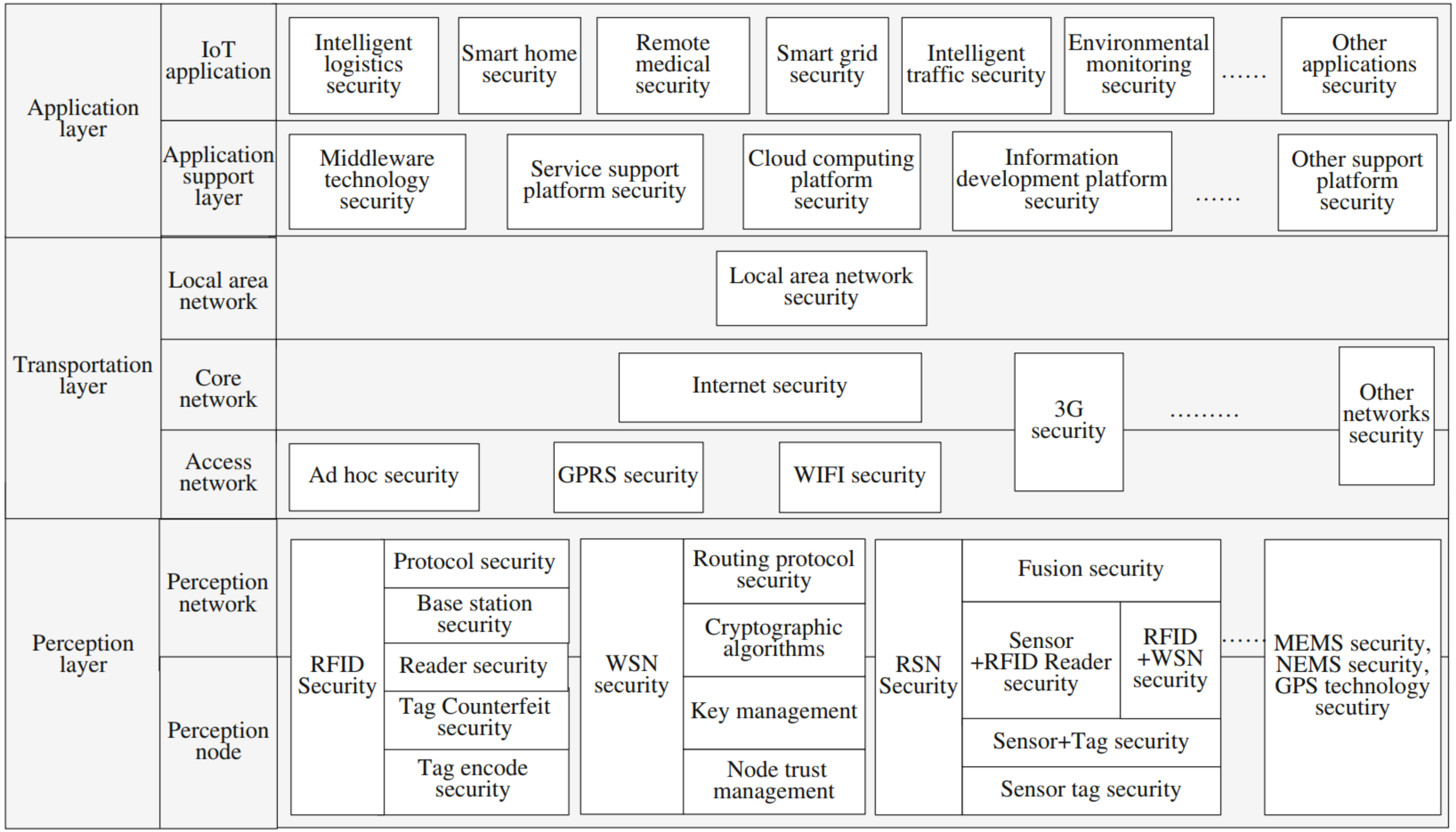
1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

IoT Security Solution



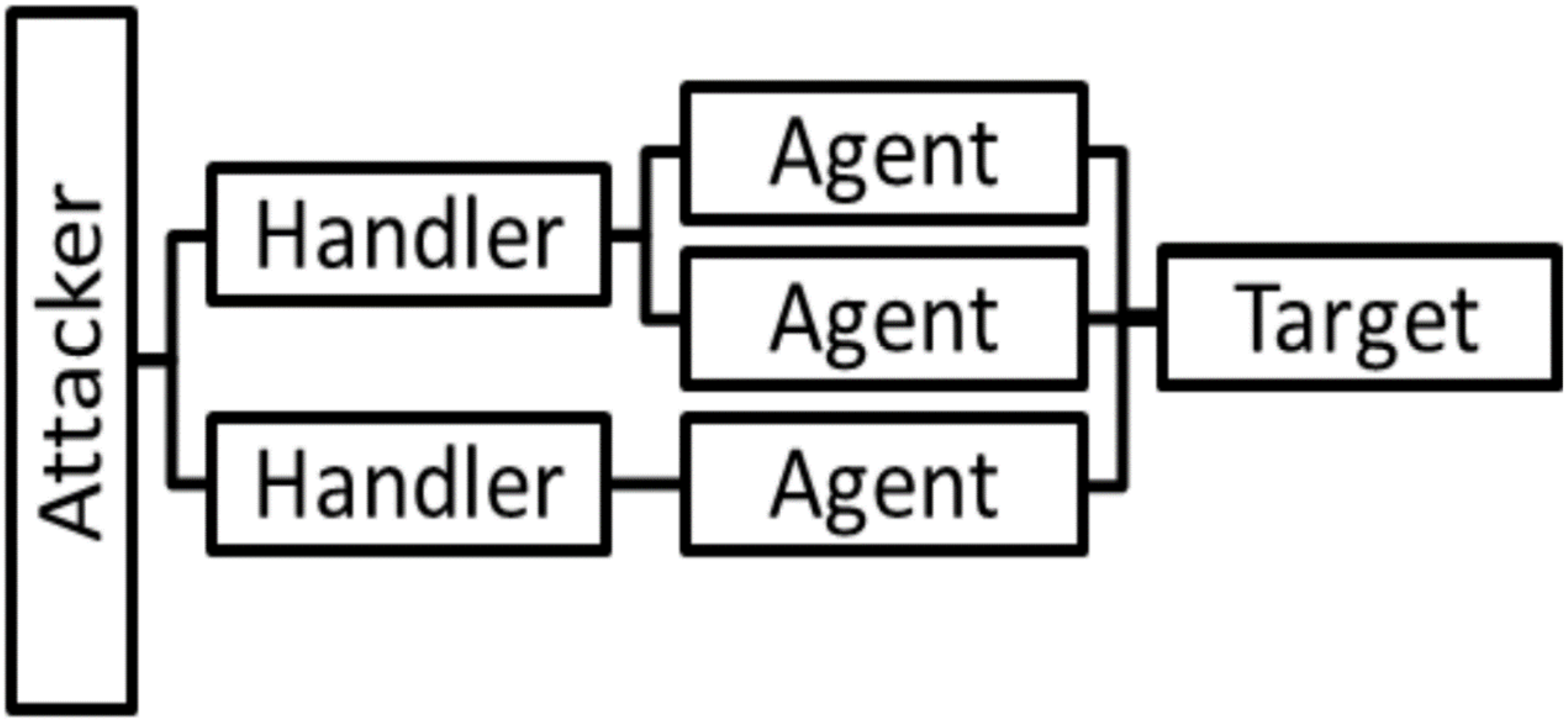
1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

IoT Security Solution



1. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

DDoS Attack



1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

DDoS Attack Types

- UDP flood
- ICMP/PING flood
- SYN flood
- Ping of Death
- Zero-day DDoS

1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

DDoS ATTACK ON IOT

DDoS on Perception Layer

- RFID Jamming
- RFID Kill Command Attack
- RFID De-synchronizing Attack

1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

DDoS ATTACK ON IOT

DDoS on Perception Layer

- 802.15.4: Wide-Band Denial and Pulse Denial
- 802.15.4: Node-Specific and Message-Specific Denial
- 802.15.4: Bootstrapping Attacks

1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

DDoS ATTACK ON IOT

DDoS on Network Layer

- Flooding Attacks

  e.g.: UDP flood, ICMP flood, DNS flood etc.

- Reflection-based flooding Attacks

  e.g.: Smurf attack

- Protocol Exploitation flooding attacks

  e.g.: SYN flood, TCP SYN-ACK flood, ACK PUSH flood etc.

- Amplification-b

  e.g.: BOTNET

1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

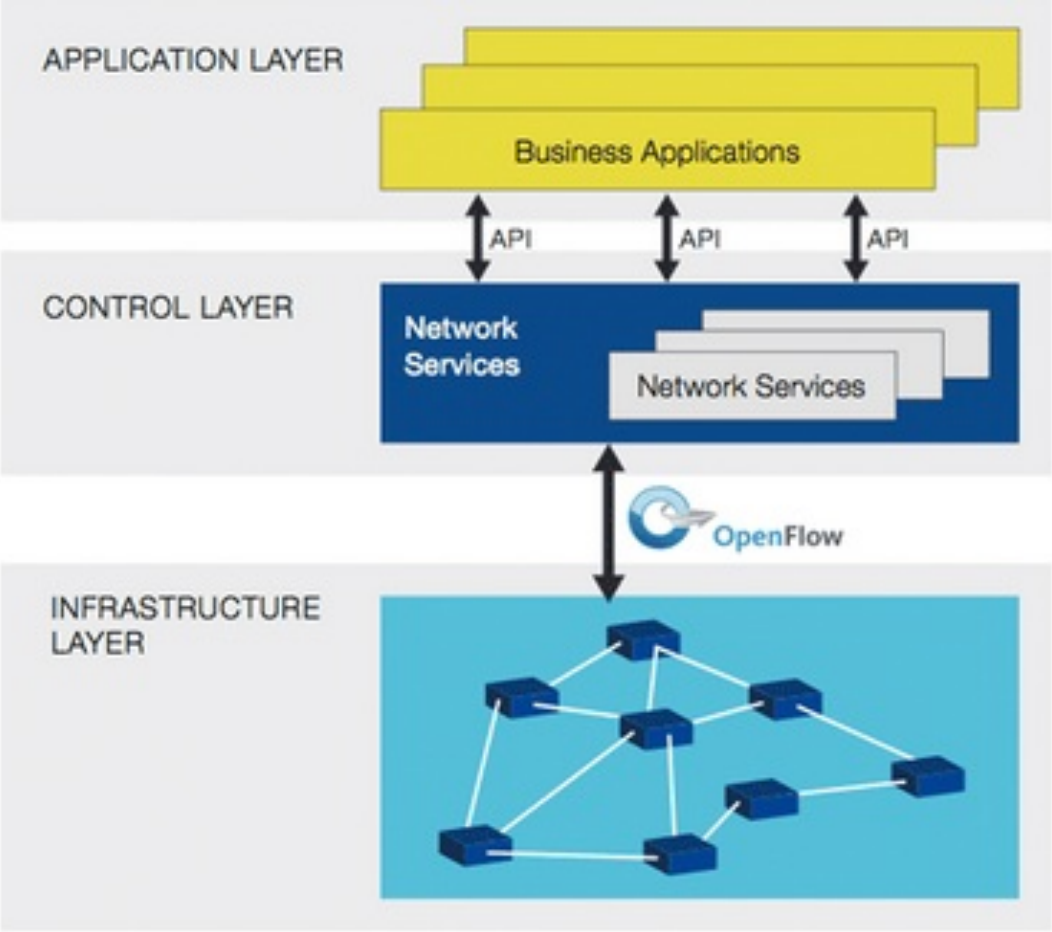
DDoS ATTACK ON IOT

DDoS on Application Layer

- Reprogramming Attack
- Path based DoS

1. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

DDoS Attack Mitigation based on SDN



Why SDN?

- SDN Is integrated and multiple layer solution.
- SDN Logically has one automated control center.
- SDN Accepts telemetry from multiple sources.
- Multivendor interoperability.
- SDN is suitable for having a timely detection solution.

SDN-based Mitigation

Radware

Protected Networks Stats

	Name	Network	R.Total P/sec	N.Total P/sec	R.Total B/sec	N.Total B/sec	TPS	R.TCP P/sec	N.TCP P/sec	R.TCP B/sec	N.TCP B/sec	R.ICMP P/se
☑	Cust4	100.0.0.14	1,037	889	105,539	90,760	167	1,036	888	105,441	90,613	1
☑	Cust1	100.0.0.11	896	793	91,301	81,650	149	893	792	91,007	81,432	3
☑	Cust2	100.0.0.12	892	875	90,869	90,217	164	891	874	90,771	90,119	1
☑	Cust3	100.0.0.13	921	810	93,546	83,632	153	920	809	93,448	83,534	1

Apply

Attacks, Handled by Scrubbing Center

Attack Category	Name	Network	Detector	Rate	N. Rate	Attack Name	Detected Proto	Src Address	Dest Address	Dest Port

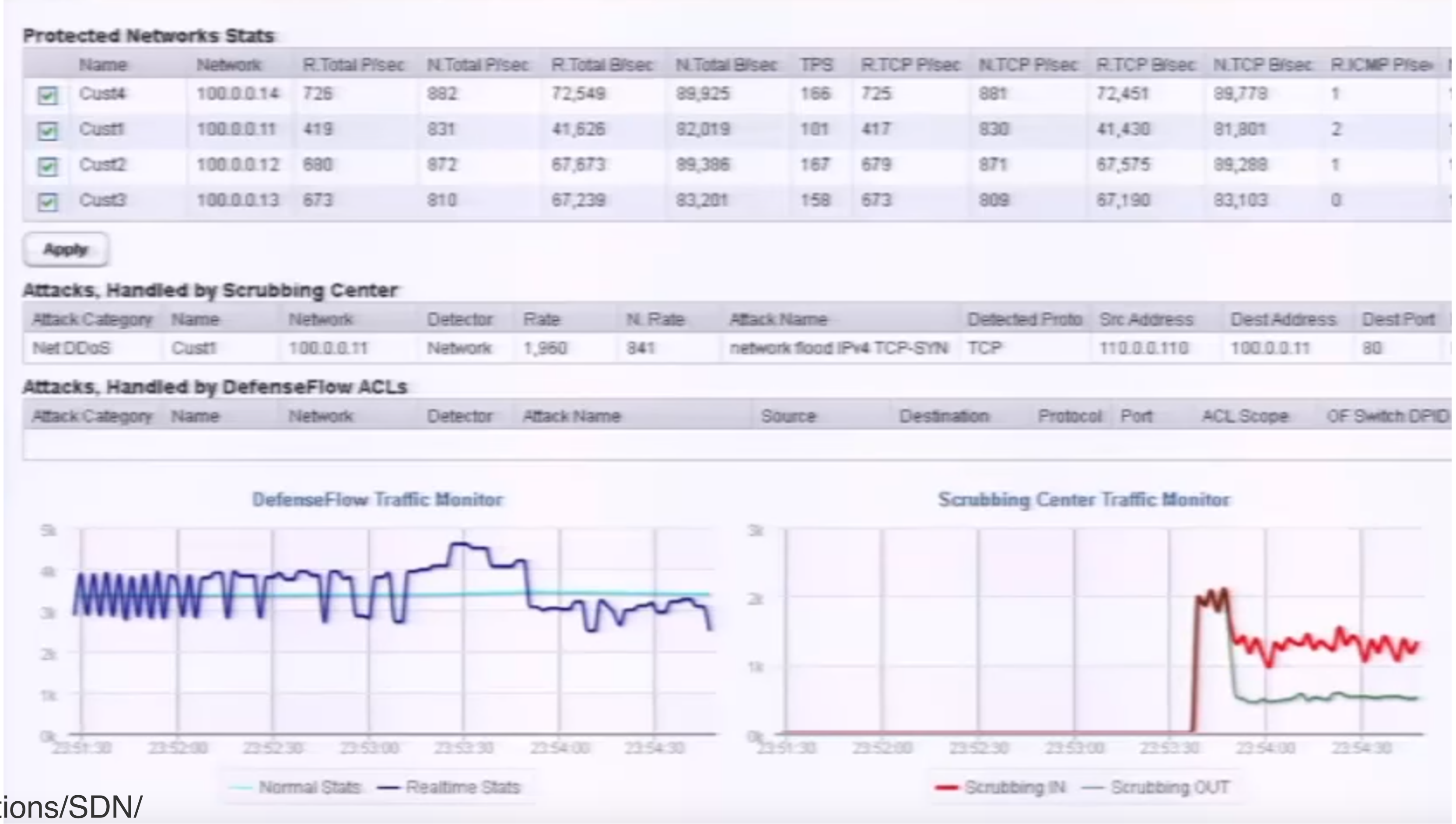
Attacks, Handled by DefenseFlow ACLs

Attack Category	Name	Network	Detector	Attack Name	Source	Destination	Protocol	Port	ACL Scope	OF Switch DPID

https://www.radware.com/Solutions/SDN/

SDN-based Mitigation

Radware



https://www.radware.com/Solutions/SDN/

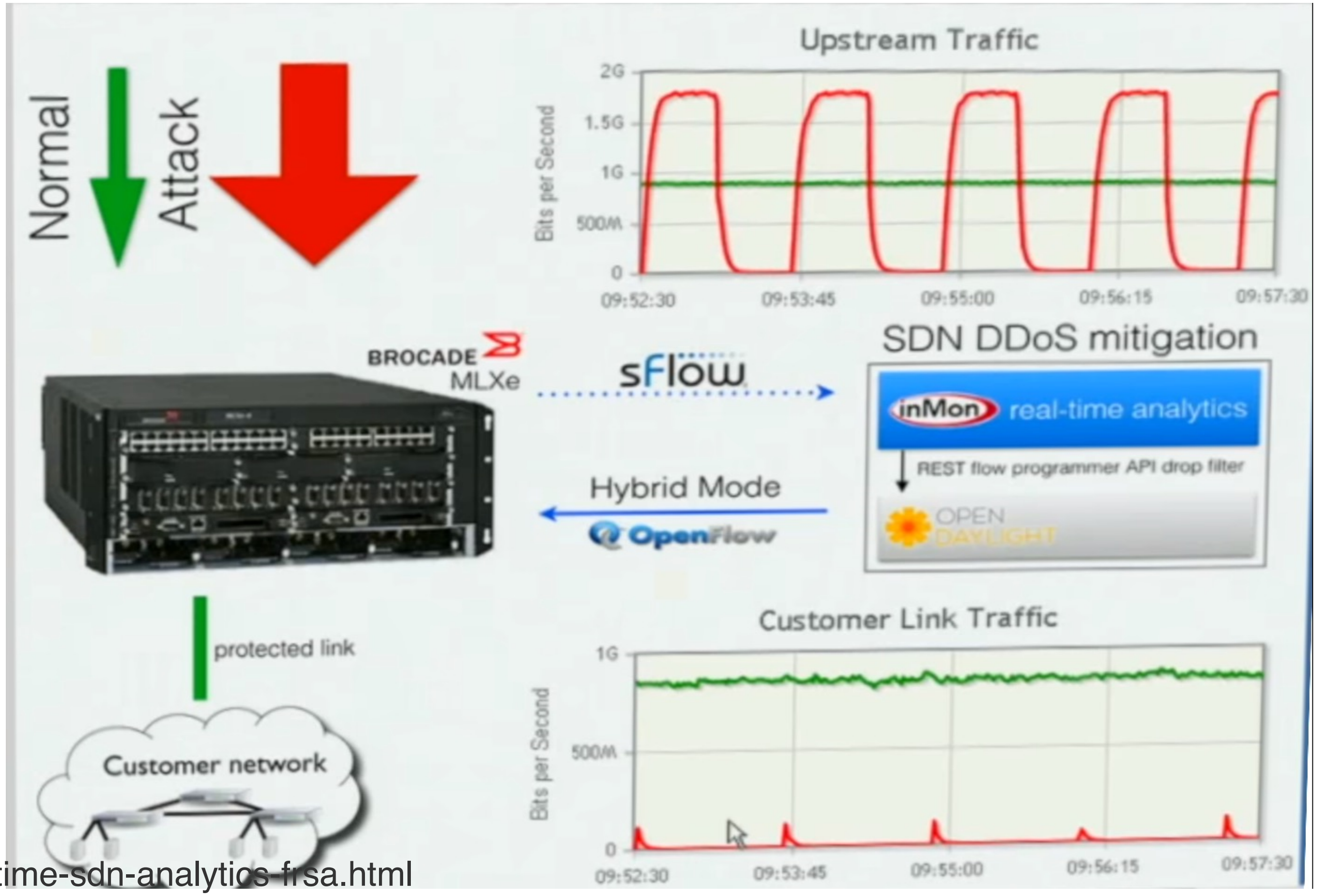
SDN-based Mitigation

Radware

https://www.radware.com/Solutions/SDN/

SDN-based Mitigation

Flow-aware Real-time SDN Analytics (FRSA)



http://blog.sflow.com/2014/02/flow-aware-real-time-sdn-analytics-frsa.html

SDN-based Mitigation Challenges

- DDoS usually do not come from a single identified source.
  - makes remediation very difficult without also affecting legitimate traffic.
- DDoS appears either very suddenly.
  - thus requiring fast reaction to counter their effects.
  - very slow reaction makes the detection even more complicated.

J. Park, K. Iwai, H. Tanaka, and T. Kurokawa, “Analysis of slow read dos attack,” in ISITA, 2014, pp. 60–64.

SDN-based Mitigation

- Stateless
  - Switches just send data to the controller.
  - Controller handles analyzing, detection and mitigation.
- Stateful
  - delegate as much computation as possible to the switches without compromising their performance.
  - letting the controller being only in charge of mitigation .

SDN-based Mitigation

- Stateless
  - Does not have fast and timely reaction.
  - Not efficient.
  - Not scalable.
- Stateful
  - Fast and timely reaction.
  - Less traffic load on the controller.

Stateful Method

Stateful method has three main steps:

- Monitoring
- Detection
- Mitigation

Stateful Method

Monitoring Methods:

- Native
  - overhead on the flow tables.
  - need to add more monitoring rules (max length is 3000 rules).
- Sflow
  - periodically take a sample and send the predefine info to the controller.
  - The sample time and the data is important and has a direct effect on the control band overhead.

Stateful Method

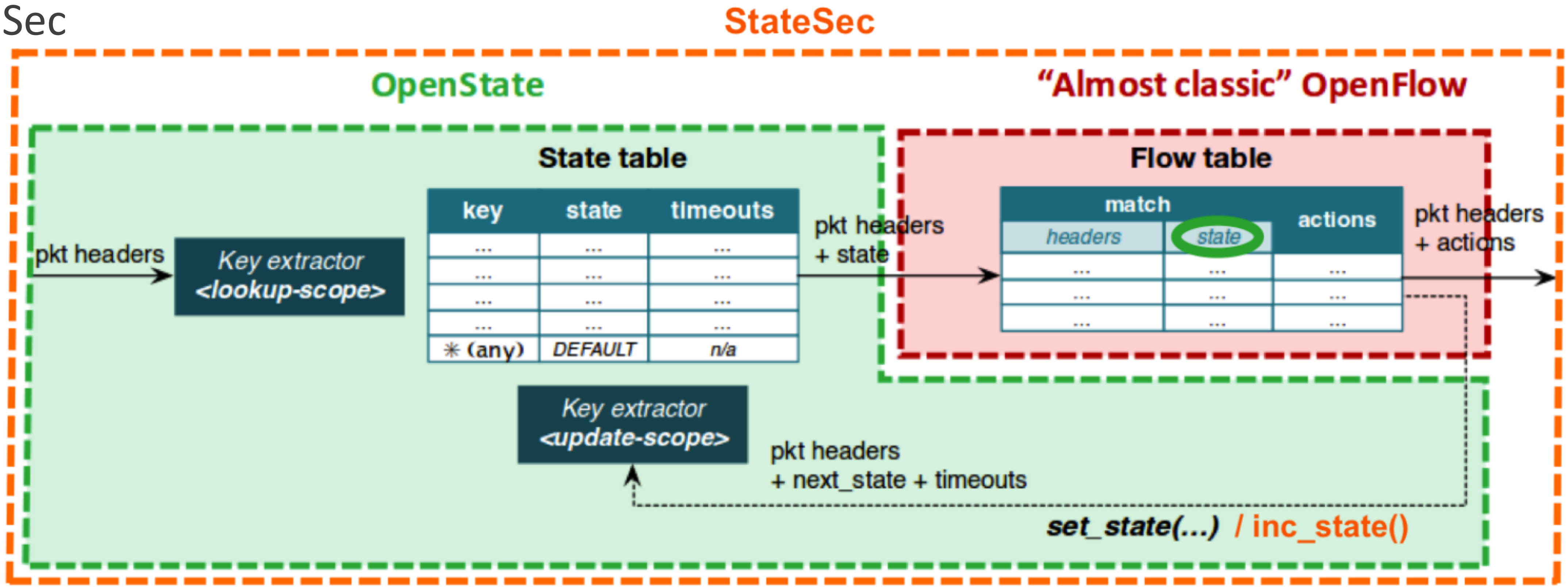
Monitoring Methods:

- StateSec
  - use the state and flow tables in an OpenState-compliant switch to independently from the forwarding rules:
    - list features
    - count the exact number of times they appear

Boite, J., Nardin, P. A., Rebecchi, F., Bouet, M., & Conan, V. (2017). StateSec: Stateful Monitoring for DDoS Protection in Software Defined Networks.

Stateful Method

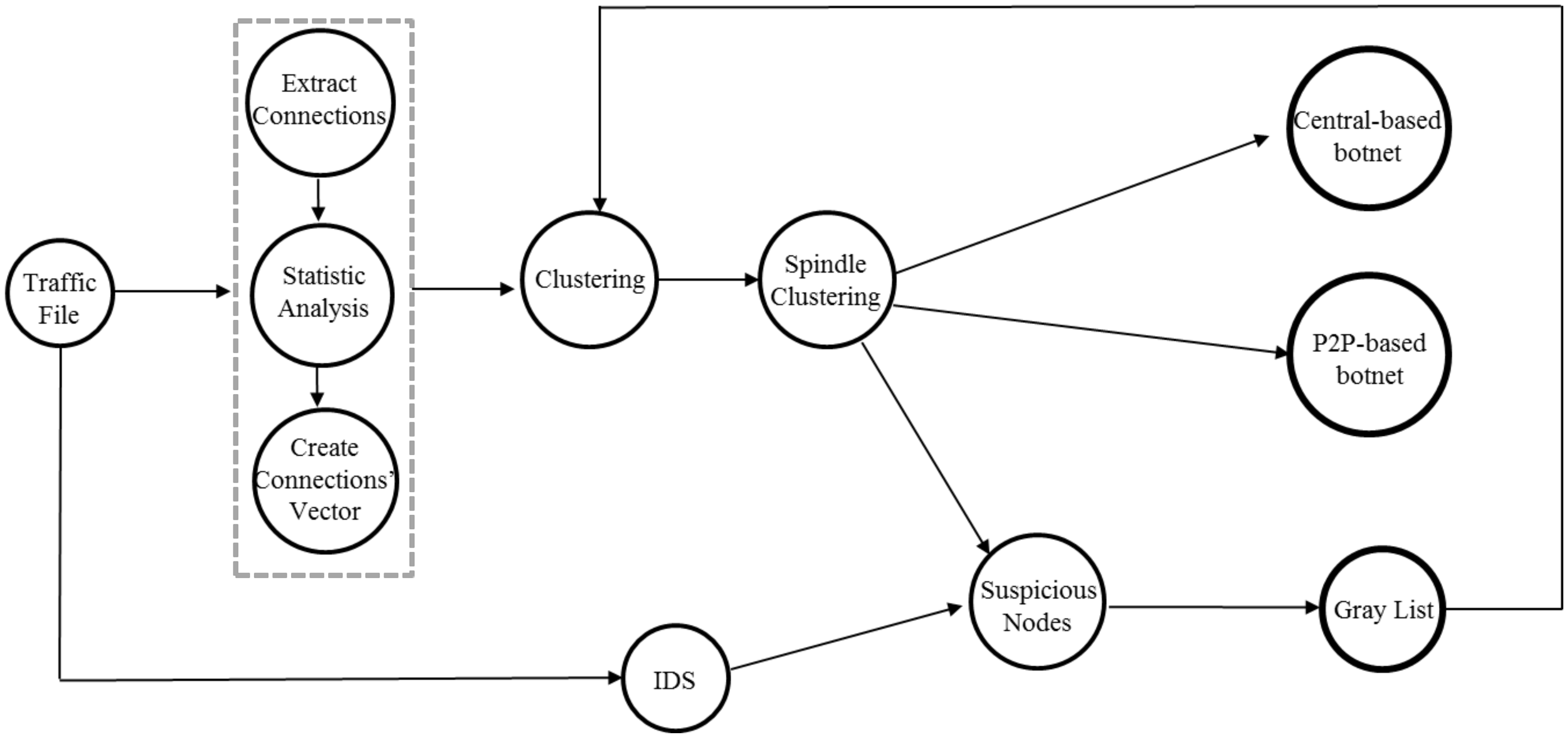
StateSec



Boite, J., Nardin, P. A., Rebecchi, F., Bouet, M., & Conan, V. (2017). StateSec: Stateful Monitoring for DDoS Protection in Software Defined Networks.

Stateful Method

Anomaly Detection Methods:



R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Methods:

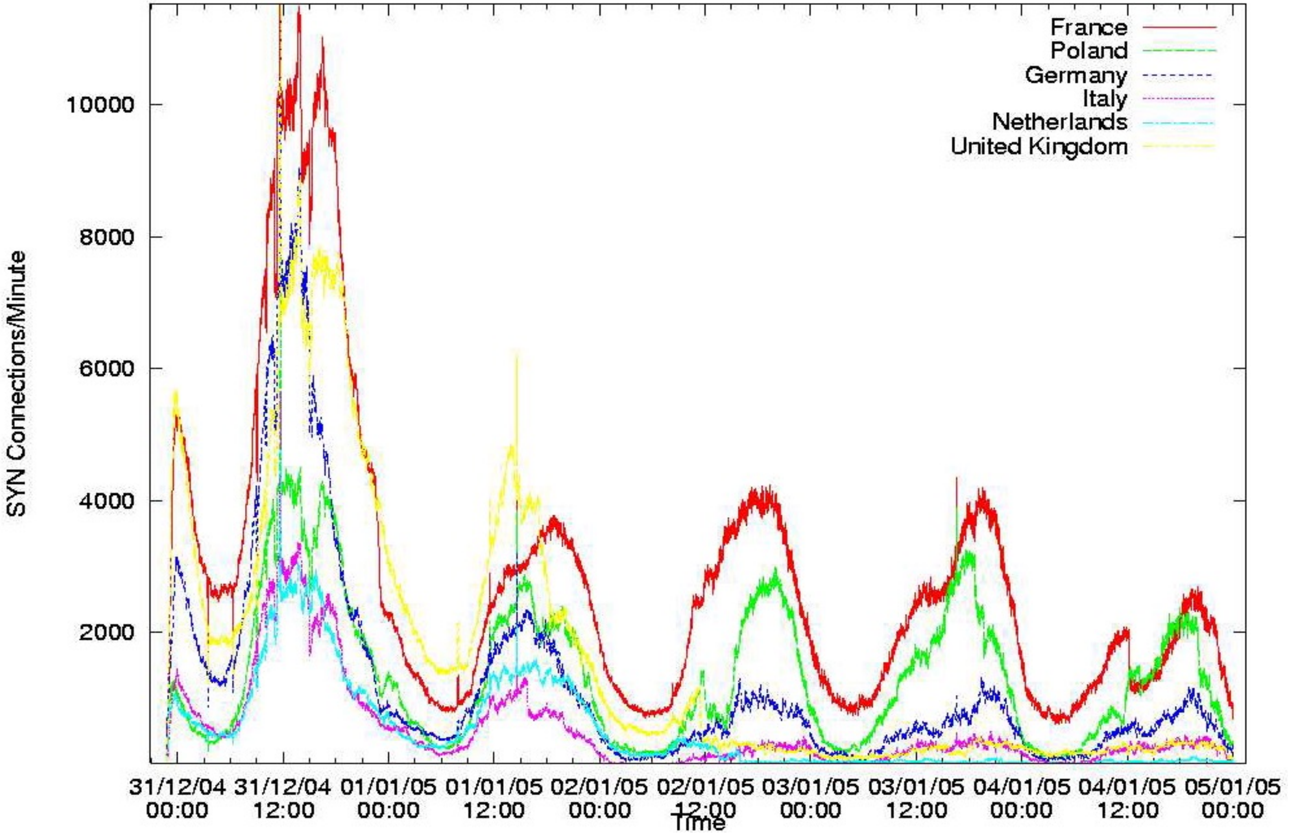
- Clustering
  - ✓ Number of sent packets for each connection
  - ✓ Size of data which has been transferred
  - ✓ Connection start time
  - ✓ Connection duration
  - ✓ Destination port number

R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Met

- Clustering



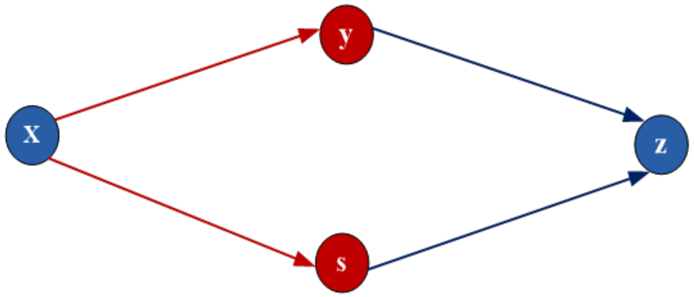
From Zou and Lee

R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Methods:

- Spindle Method



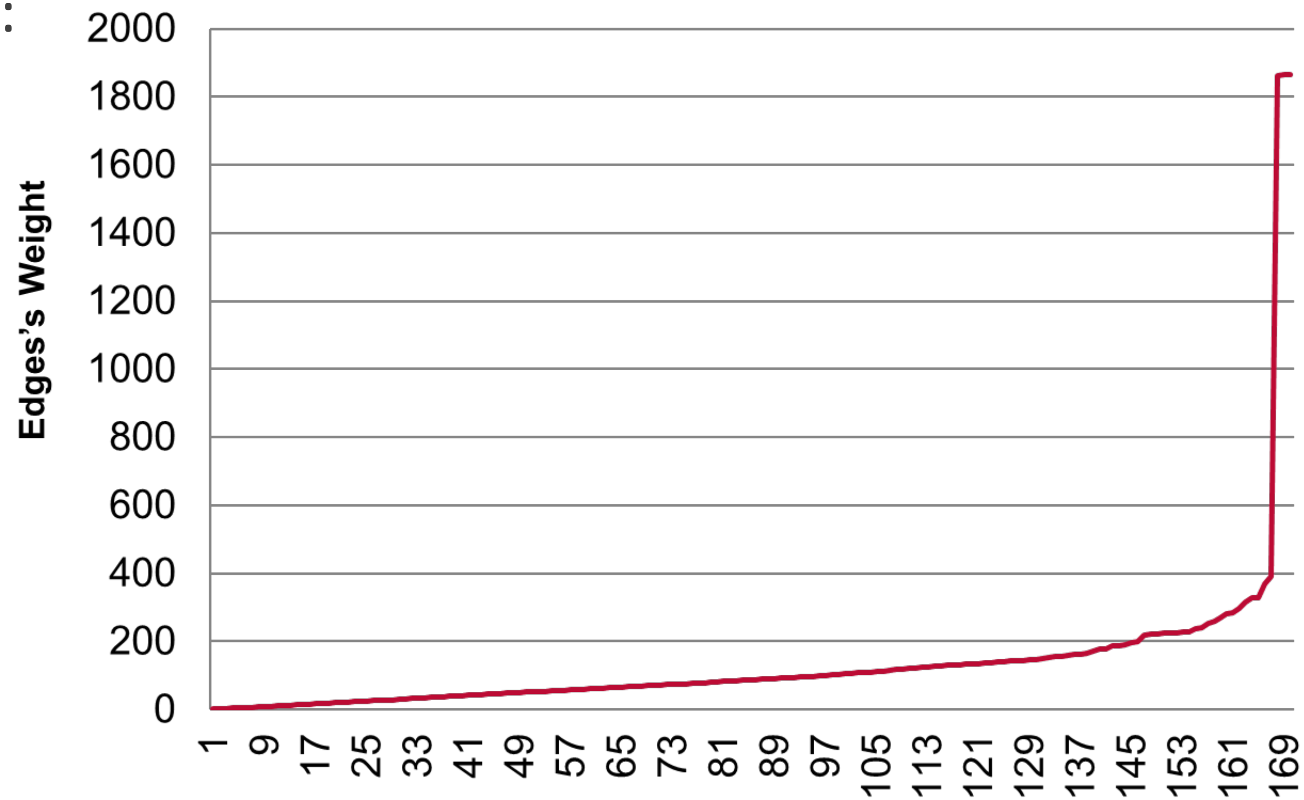
$$\forall\, x, y, s, z \in network\ model \mid$$
$$[link(x,y) \land link(x,s)] \land [link(y,z) \land link(s,z)] \Leftrightarrow infected(y,s)$$

R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Methods:

- Spindle Method

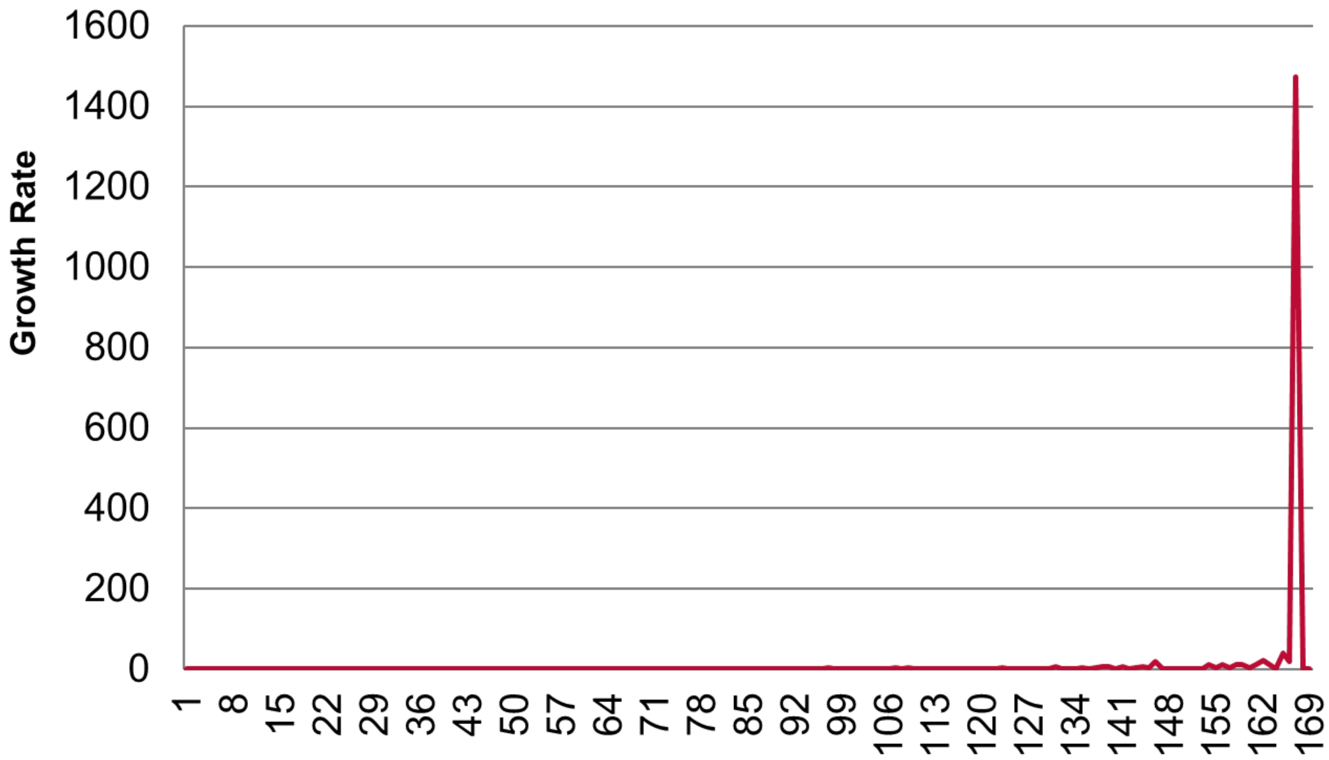


R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Methods:

- Spindle Method

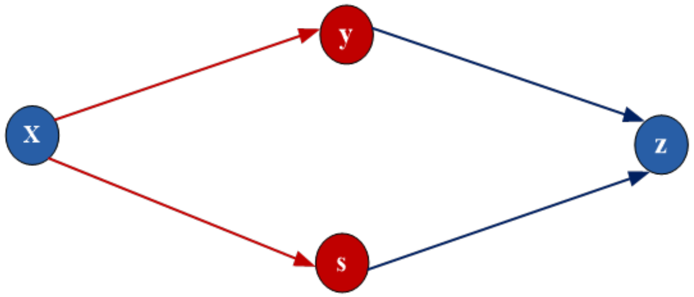


R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Anomaly Detection Methods:

- Spindle Method



$$\forall\, x, y, s, z \in network\ model \mid [link(x,y) \wedge link(x,s)] \wedge [link(y,z) \wedge w(y,z)] \wedge [link(s,z) \wedge w(s,z)] \Leftrightarrow infected(y,s)$$

R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

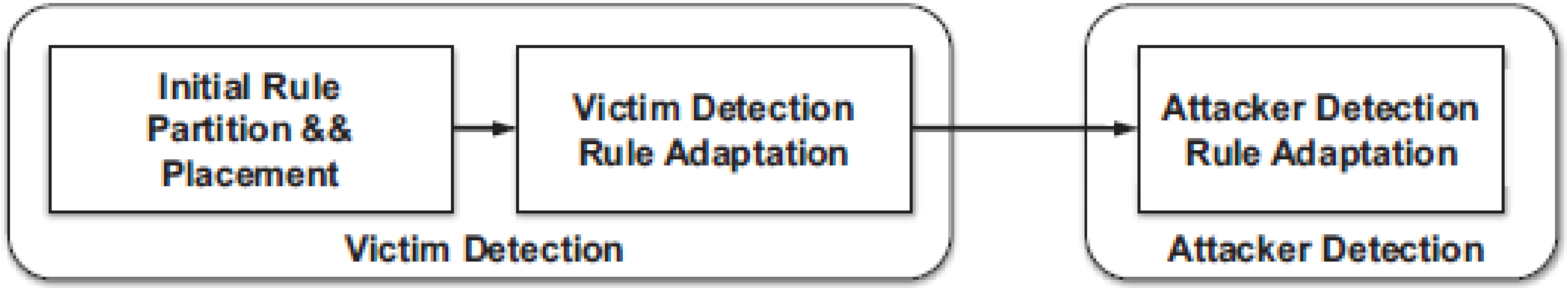
Anomaly Detection Methods:

	Infected	Detected	False negative	False Positive
IRC bot	10	10	0	0
Http bot	10	10	0	0
Zeus	10	9	1	0
Spy bot	10	8	2	0

R. Aryan, H.R Shahryari. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

Stateful Method

Mitigation Methods:



Xu, Yang, and Yong Liu. "DDoS attack detection under SDN context." Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. IEEE, 2016.

Stateful Method

Mitigation Methods:

$$A - Victim\ IP = A'$$

$$B - Victim\ IP = B'$$

$$A \rightarrow B$$

$$A' \rightarrow B$$

$$A \rightarrow B'$$

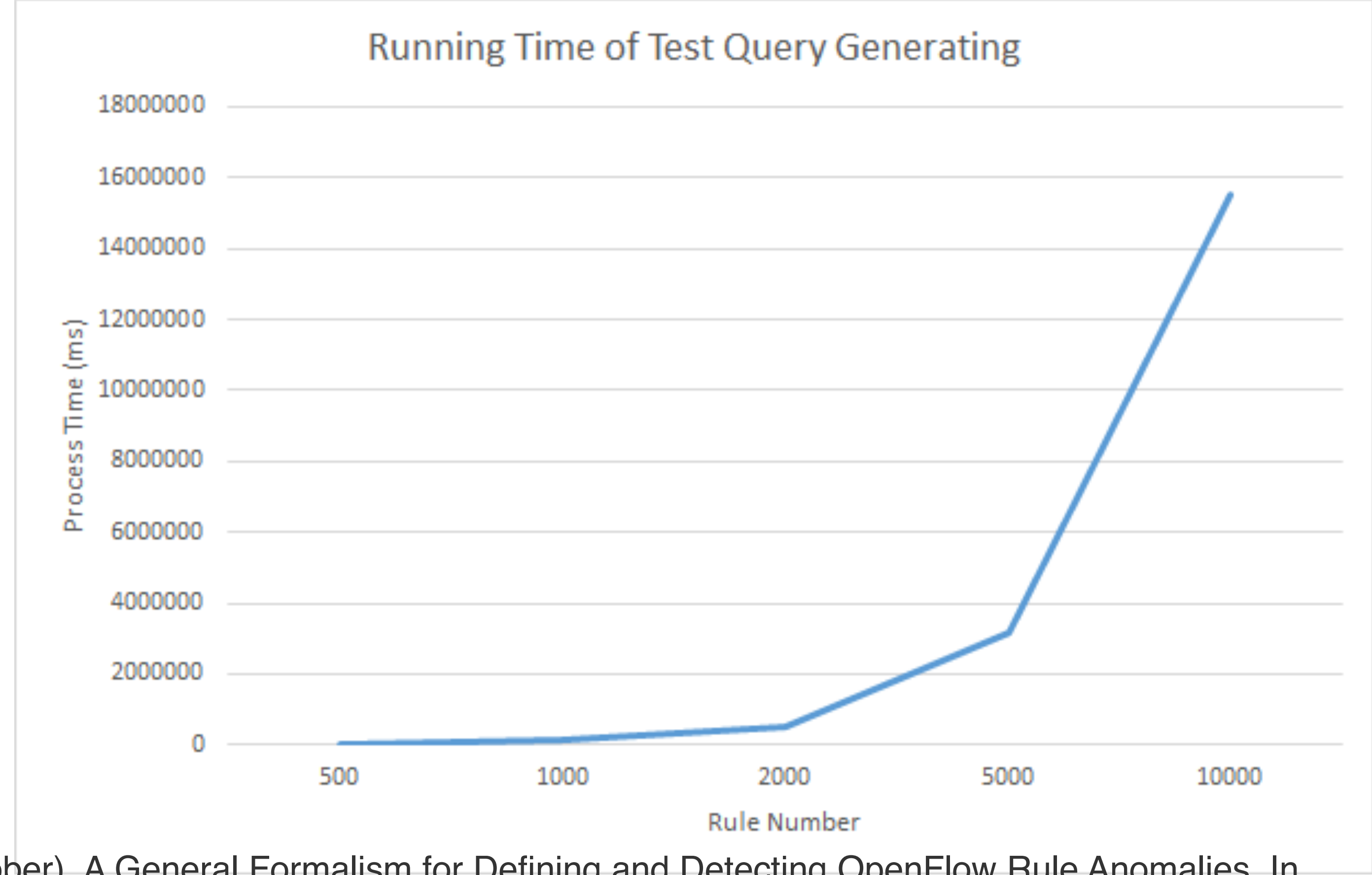
Xu, Yang, and Yong Liu. "DDoS attack detection under SDN context." Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. IEEE, 2016.

Stateful Method

Mitigation Methods:

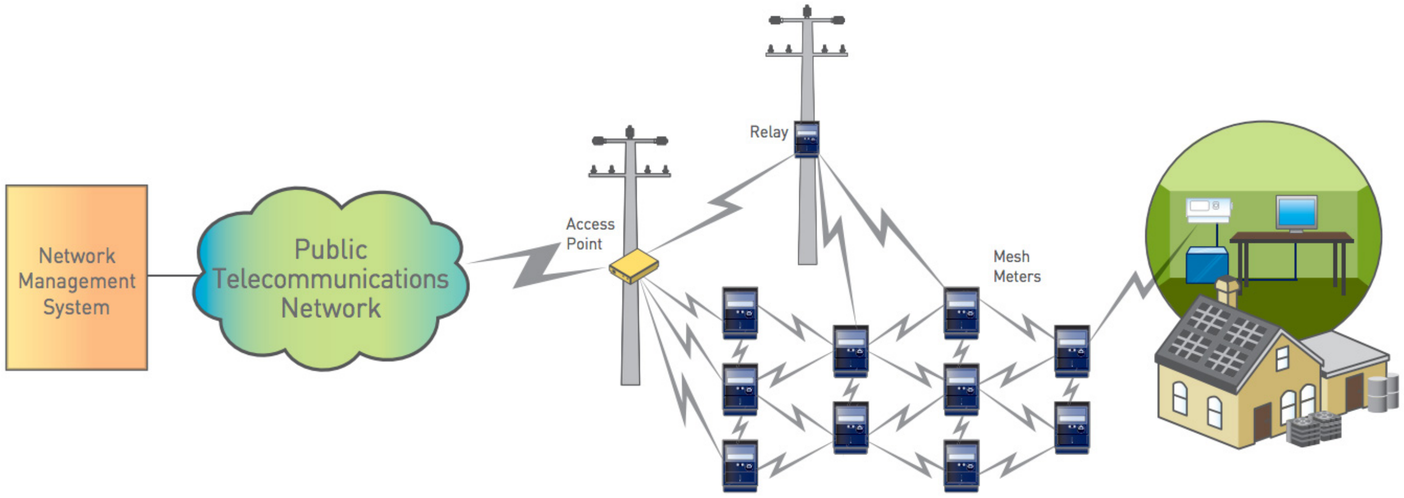
- Subtraction Rules

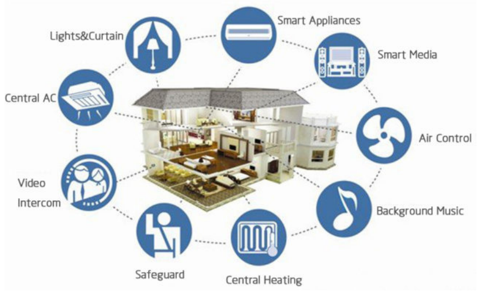
Rule Number	500	1,000	2,000	5,000	10,000
Process Time (ms)	31,543	126,104	508,206	3.17×10^8	1.55×10^8



Aryan, R., Yazidi, A., Engelstad, P. E., & Kure, O. (2017, October). A General Formalism for Defining and Detecting OpenFlow Rule Anomalies. In 2017 IEEE 42nd Conference on Local Computer Networks (LCN) (pp. 426-434). IEEE.

Conlusion


Network
Management
System
Public
Telecommunications
Network
Access
Point
Relay
Mesh
Meters


Lights&Curtain
Smart Appliances
Smart Media
Central AC
Air Control
Video
Intercom
Background Music
Safeguard
Central Heating

REFERENCES

1.https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

2. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

3. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

4. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

5. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on Internet of Things. International Journal of Engineering Research and Development, 10(11), 58-63.

6. https://www.radware.com/Solutions/SDN/

7. http://blog.sflow.com/2014/02/flow-aware-real-time-sdn-analytics-frsa.html

8. Boite, Julien, et al. "StateSec: Stateful Monitoring for DDoS Protection in Software Defined Networks." (2017).

9. Aryan, R, Shahryari, Hamid. R. StateSec: Botnet Detection Based on Behavioral Pattern and Misuse Detection.18thComputer Society Of Iran Annual Conference, Sharif University of Technology, 2013.

THANK YOU...