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

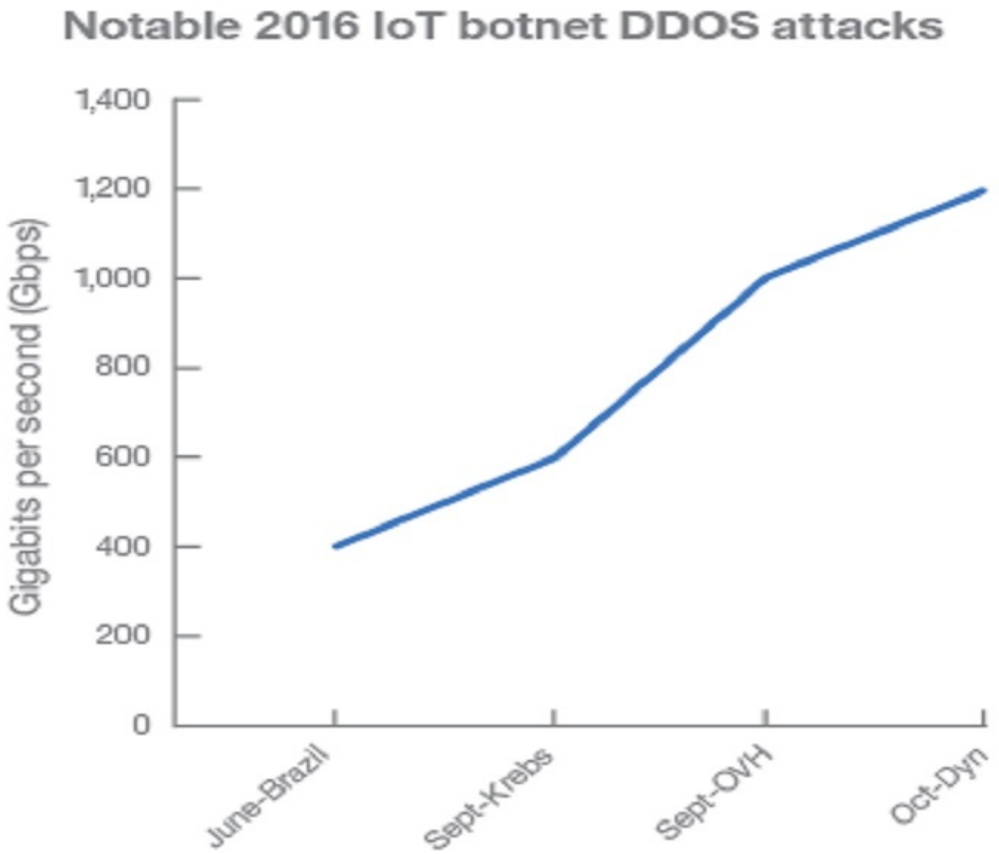
- One of the most important changes, the rising use of compromised Internet of Things (IoT) devices in botnet operations.

- 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.

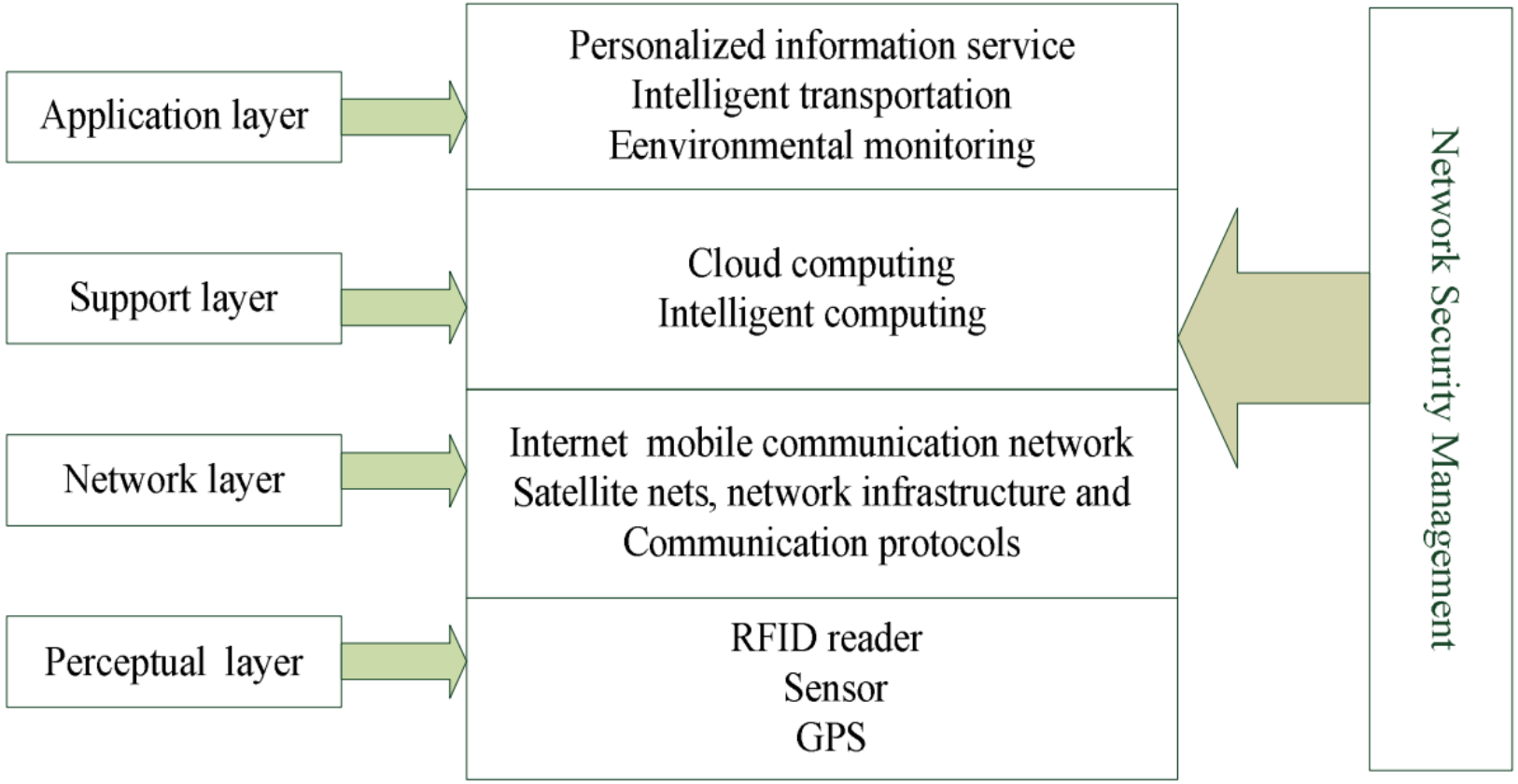
[1]. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

Why DDoS Attack on IoT



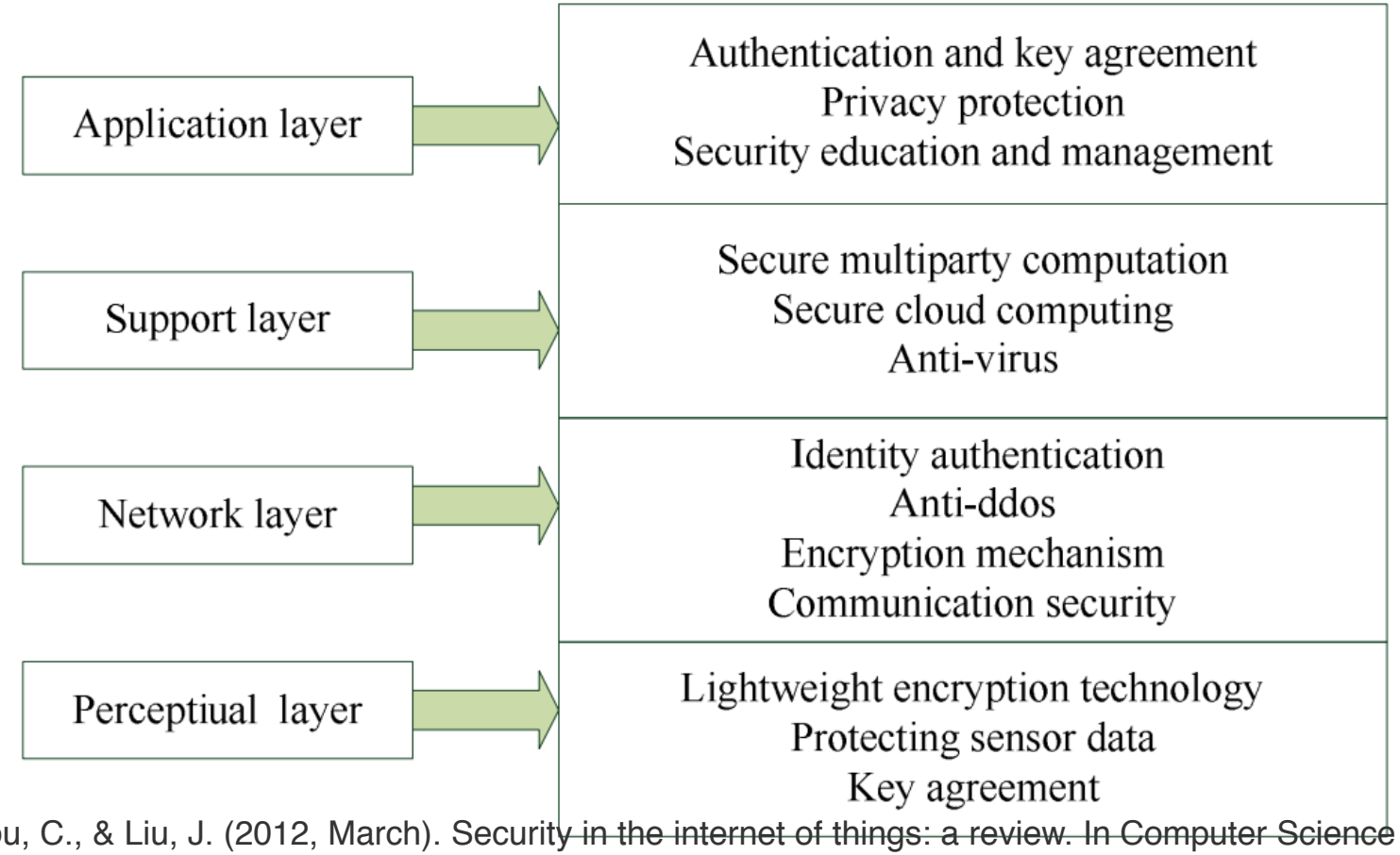
[1]. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

IoT Architecture



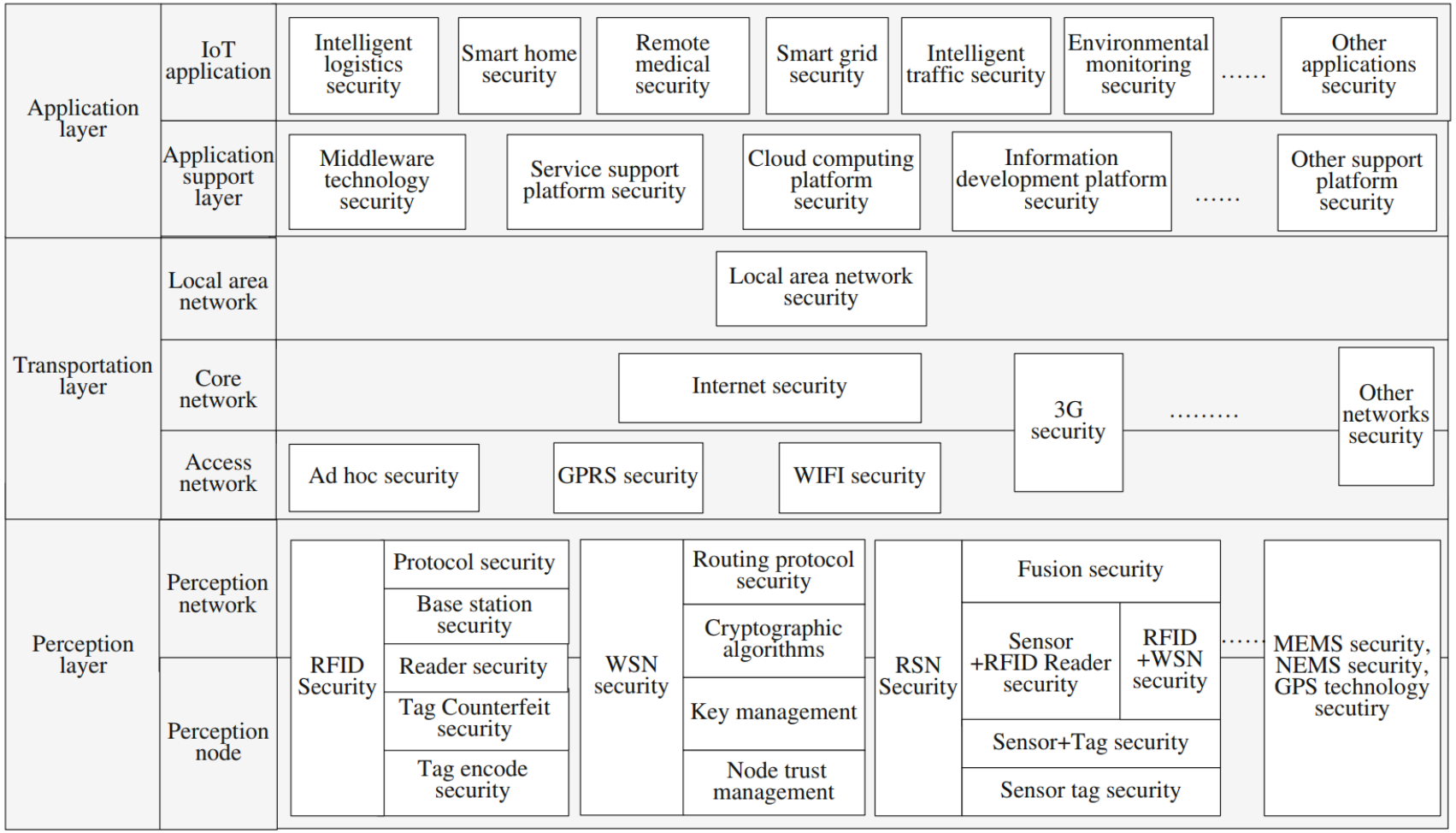
1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

IoT Security Solution



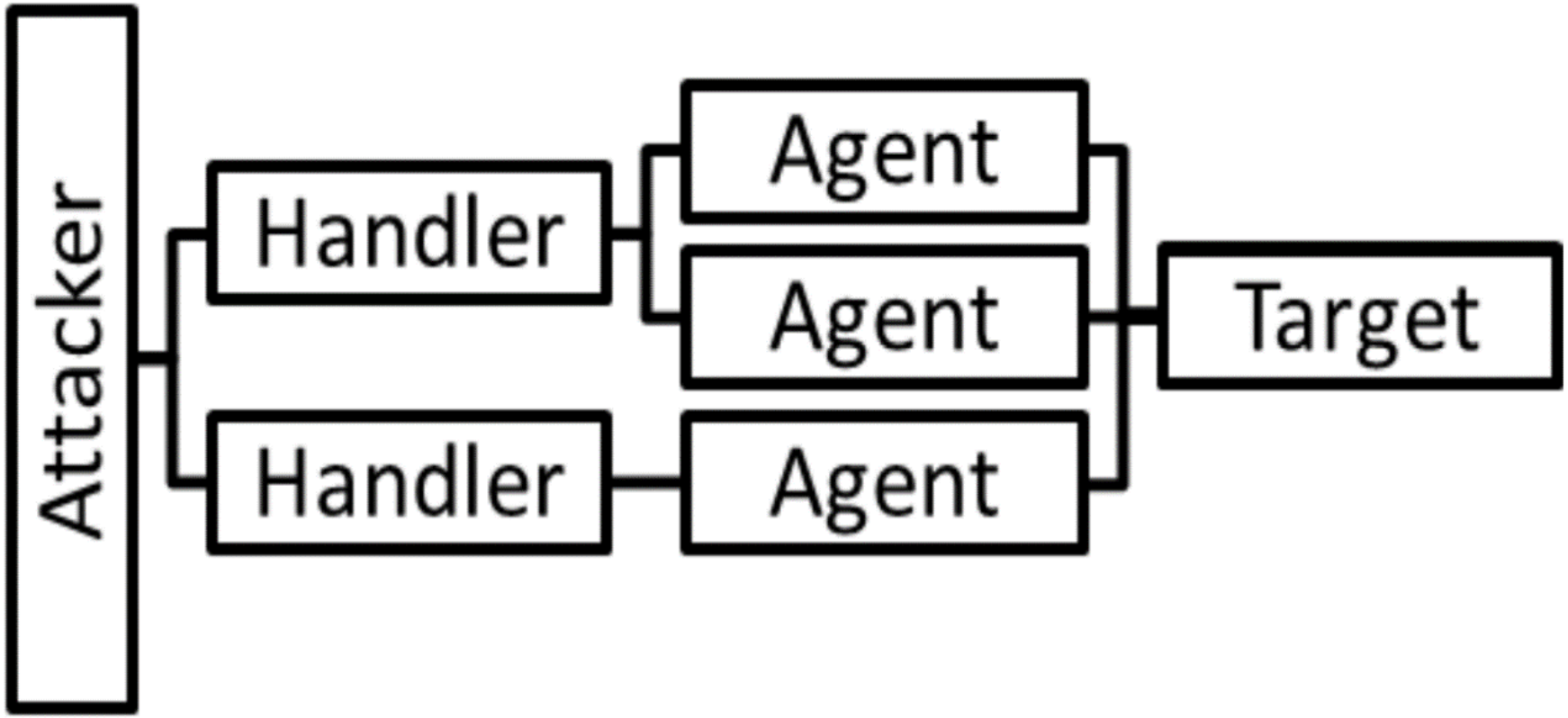
1. Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

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.

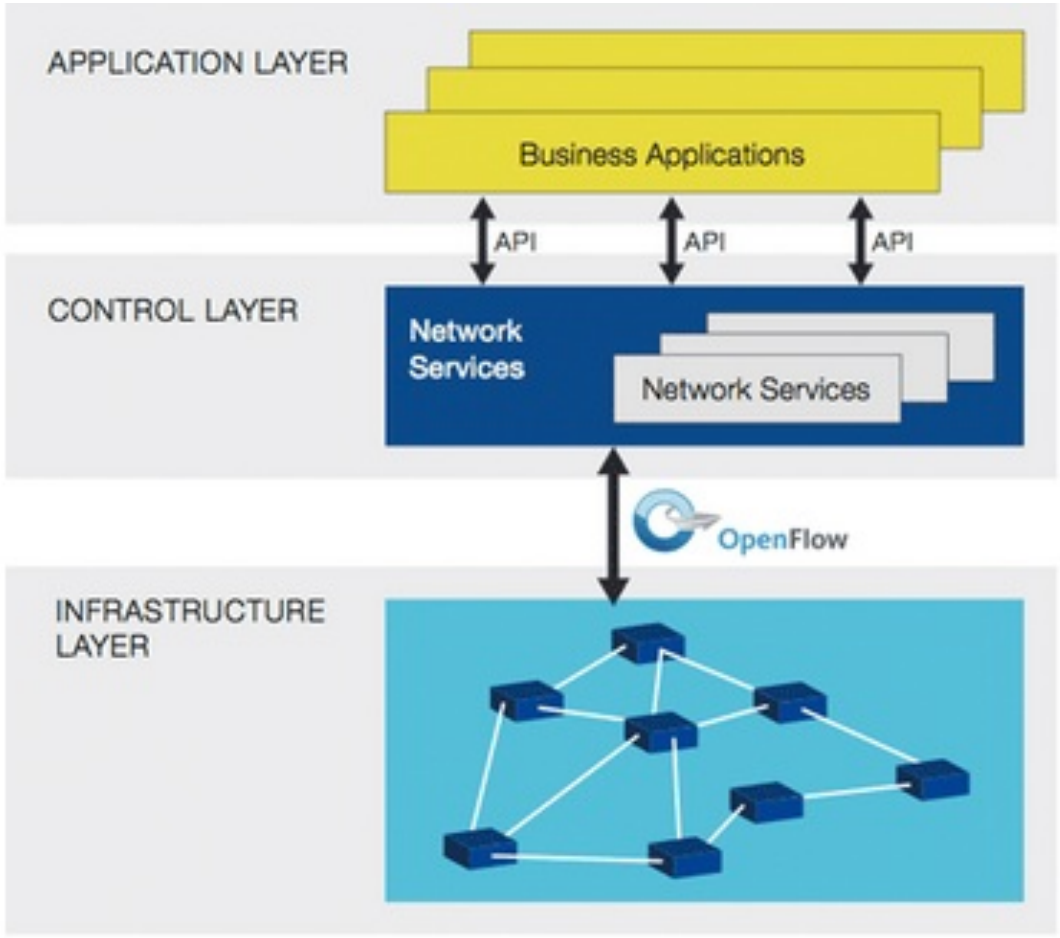
DDoS ATTACK ON IOT

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



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.


THANK
YOU...