JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Performance Improvisation for Prevention of DDoS Attacks in Smart Homes with an SDN-Based Firewall

-Kunal Thanki.
Lecturer in computer Engineering Dept.
Govt Polytechnic Porbandar

Abstract

This paper reviews the evolution of software-defined networking (SDN) as a security enabler for smart home environments, with a focus on DDoS mitigation using SDN-based firewalls. Existing approaches such as enterprise firewalls, cloud-based protection mechanisms, host-based intrusion detection systems, and SDN-specific sampling solutions including FleXam and FleXight are critically analyzed. The review highlights their limitations within heterogeneous IoT-driven smart homes. A conceptual integrated approach using sample compression and flow table reduction is discussed as a pathway for performance improvement. The review consolidates research progress and identifies open challenges for future work.

KeywordS

AI, IOT,Smart Home, SDN, OpenFlow, DDoS Attack, Flow Table, Sampling, Firewall

I. *Introduction*

With the increasing use of AI and IoT people tend to use more smart equipment in the home to make home as a smart home. This is where the requirement of smart home management arise[1]. Security and privacy risks have escalated, particularly due to the proliferation of unsecured IoT endpoints that may be exploited to conduct Distributed Denial-of-Service (DDoS) attacks Smart home product comes in a large variety and in heterogeneity. To operate with all the product under same roof , there has to be some middleware application which run with all the devices. This arise the need of managing all the network devices connected with the smarthome system. SDN can be used for such purpose. In IOT major challenge to provide security and privacy[11] to all connected devices. It is not only the privacy and security of the user owning the device that is in danger. Compromised IoT devices can be misused for different malicious activities such as Distributed Denial-of-Service (DDoS) attacks[10] targeting other hosts on the Internet. These devices are prone to DDOS attack which can be prevented by SDN approach based Firewall kind of protection. In this proposal we propose performance improvisation for SDN based firewall for intrusion detection and DDos attack prevention. This paper reviews foundational SDN concepts, smart home security challenges, and research contributions related to SDN-based firewalls.

II. *Background on SDN and OpenFlow*

With recent development in networking and AI, new concept of programmable network came into picture which is known as Software Designed Network(SDN). It basically divide control plane and data plane. In SDN architecture [1] as shown in fig 1 there are basically separation of control and data flow. Control plane of SDN implements all the flow related rules and issue directions to manages and provide traffic flow to the data plane. Data plane includes actual forwarding devices like routers and switches. Here the management is done by control plane. Control plan communicate with data plane using OpenFlow protocol.[2] . OpenFlow serves as the de facto protocol for communication between switches and controllers. Openflow architecture is shown in figure 2.[3]. With the grow in IoT use of SDN has started to connect all the devices using programmable network[5]. SDN offers programmability, global network visibility, and dynamic policy enforcement—key attributes for securing smart homes.

Fig. 1. Software-Defined Network Architecture.

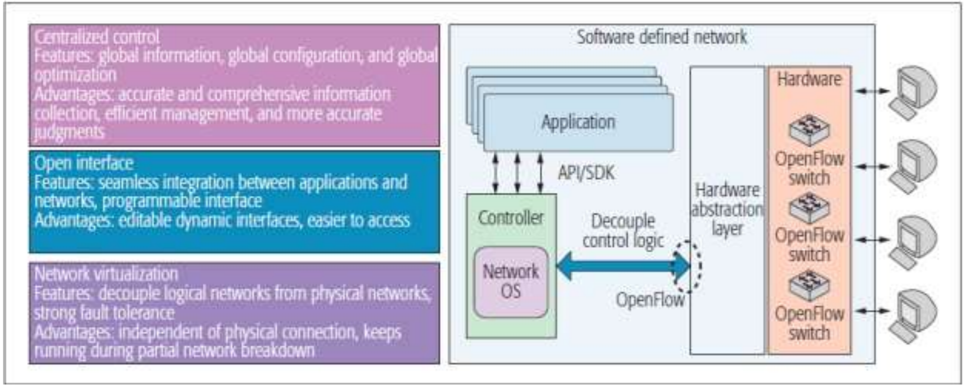
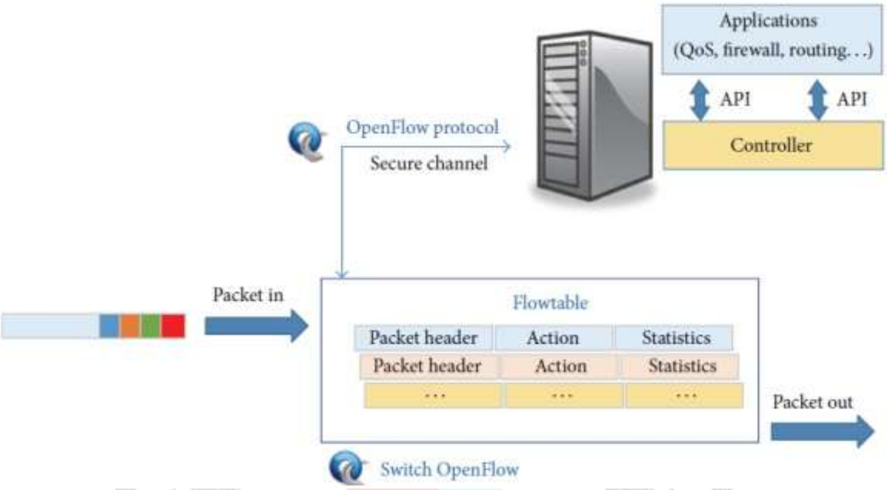

Centralized control
Features: global information, global configuration, and global optimization
Advantages: accurate and comprehensive information collection, efficient management, and more accurate judgments
Open interface
Features: seamless integration between applications and networks, programmable interface
Advantages: editable dynamic interfaces, easier to access
Network virtualization
Features: decouple logical networks from physical networks, strong fault tolerance
Advantages: independent of physical connection, keeps running during partial network breakdown
Software defined network
Application
API/SDK
Controller
Network OS
Decouple control logic
OpenFlow
Hardware abstraction layer
Hardware
OpenFlow switch
OpenFlow switch
OpenFlow switch

Fig. 2. OpenFlow Architecture



III. *Related work:*

A. Enterprise Firewalls: Many Firewalls have been developed (both software firewall and hardware firewall). But using this kind of product for smart home is not advisable for the following reason.

1. Firewall configuration are not that much easy for smart home consumer. If they install firewall at the gateway of smart home, they have to configure firewall for all the kind of device heterogeneity, which is difficult task.
2. Enterprise firewall are much costly to be used in home networking. It require regular update, which might not be possible for ordinary user.
3. Technically if smart home is accommodating SDN approach, Simple Firewall cannot be used as SDN uses controller and if all the packet that passes through data plane, passes through firewall than to take decision for filtering , it has to pass to controller which create bottleneck for controller

B. Cloud-based Firewalls: In cloud-based firewall, ideally, the service is provided by a third party and therefore the burden of configuration, maintenance, and updating is eliminated for the user. Traditional firewalls process every packet entering or leaving the network to identify potential threats and block discovered attacks. Moving the firewall to the cloud leads to a new challenge: how should the cloud-based firewall process every packet? Cloud-based firewalls that are designed for enterprise customers require all the traffic to be redirected to the cloud[4] . This is not reasonable for a home network for several reasons[4]:

1. Asymmetric upload and download rate at home ISP
2. Limit on data cap. It may create over charge for sending all data at the cloud based firewall.
3. VPN-like solutions (all traffic being routed through a third party that offers the firewall service) will face VPN problems such as added delay and possible blockage by some servers (e.g., due to geo-locationing).

C. Current IDS system:

Currently available IDS system like Wireshark and Snort can perform better in network intrusion detection. But with the software defined network, it will not work because of the controller –data plane architecture. In controller if we redirect the packet to fetch by IDS, it will be available with limited information because controller only get information when miss occurred in open flow switch and that too has limited information as only header will be sent to the controller. Also we have to consider heterogeneity of devices available in smart home. So this solution will not work in our current situations.

D. SDN based Ports scan detection: There are two ways for an OpenFlow controller application to access packet-level information of a given flow. The first option is to not install any flow entries for the desired flow on one of the switches on the path. Every packet of the flow will be a table miss at that switch, triggering a “packetin” message from the switch to the controller. The controller then needs to tell the switch to send out these packets on the correct port. This option was used in SDN-based portscan detection system proposed by Mehdi et al. [12]. This approach is not that much realistic due to two major limitations. First, the controller effectively sits on the packet delivery path, potentially creating a bottleneck, and leading to increased packet delivery time. Second, the switch may, and probably prefer to, buffer the packet locally and only send part of it to the controller, which will limit the amount of packet content that the controller can access.[12]

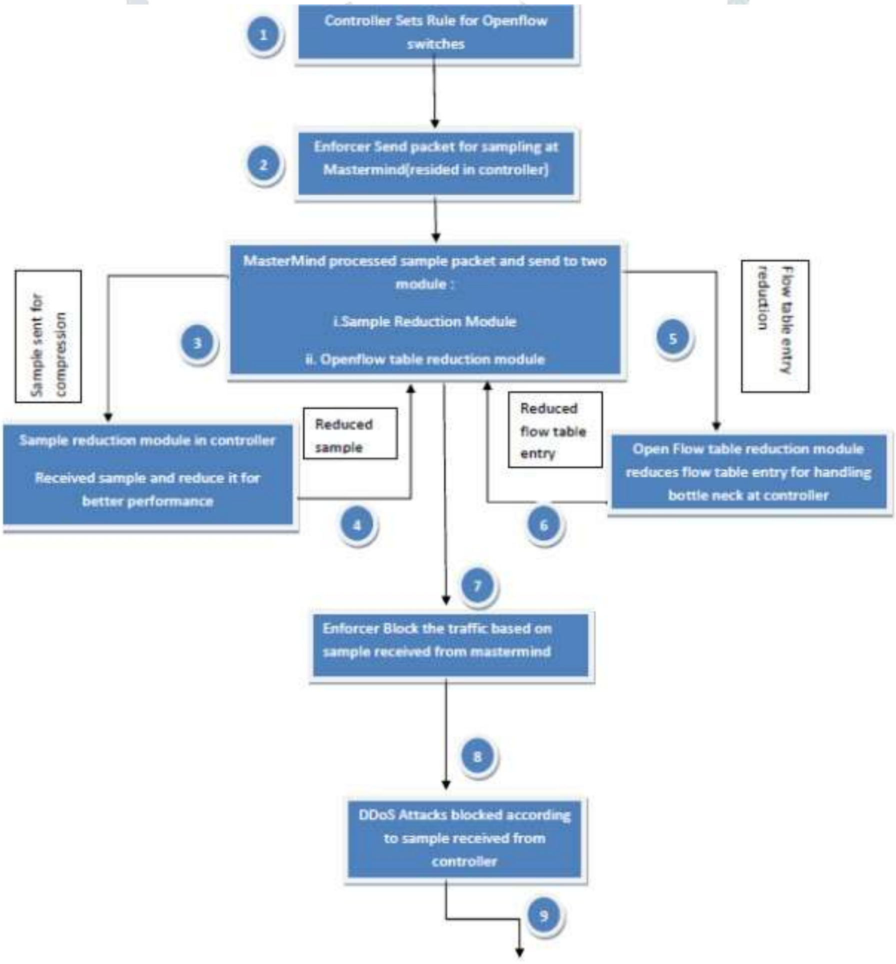
E. Host based IDS For smart homes using SDN: There are certain development in the field of host based intrusion detection using open flow.[6]. In their work authors proposed an intrusion detection and mitigation framework, called IoT-IDM, to provide a network-level protection for smart devices deployed in home environments. IoT-IDM framework, which we place it on the top of SDN controller, consists of five key modules: Device manager, Sensor Element, Feature Extractor, Detection, and Mitigation.[6]. It deals with illegitimate access to the device but does not deal with DDoS attack. And installing host based firewall at gateway level will leave management of the IDS upto the user. Some time users are not that much qualified to get in to it.

F. SDN-based Firewall: In their research work , Sajad Shirali-Shahreza, and Yashar Ganjali have proposed good solution for DDos attack mitigation using SDN based firewall approach[7]. They proposed cloud-based firewall controller and a local enforcer. In which they shifted firewall controller to the cloud so that user does not need to install firewall and manage it. They used FleXam [8] for selecting samples for comparison for analyzing packets, identifying anomalies, and deciding how to handle them. The the first component of their firewall called enforcer is a packet processor that simply examines a packet and either drops it or forwards it based on a short action list that is set by the mastermind the second component called of the designed. This platform decouples the enforcement component of the firewall from the decision-making part and moves the decision-making component to the cloud. This will make it easier and more affordable for home users to have aneffective firewall and increase their network security. This platform intelligently selects parts of the traffic needed for decision-making (using FleXight). This makes this approach best for DDoS attack mitigation .But in that also no work of data compression and flowtable reduction has done.

IV. Proposed work:

In my research, I extend the work done by Sajad Shirali-Shahreza and Yashar Ganjali. This approach seems to have improvisation criteria if we consider the selection of sample for comparison. In proposed approach the research work of Sajad Shirali-Shahreza and Yashar Ganj will be used and will be extended to reduce sample overhead using sample technique. Because Different packets that are sampled from a flow can be very similar to each other. For example, the header of such packets contains many identical fields, because they are from the same sender and to the same destination. This makes them ideal candidates for compression. To perform compression of this kind of data we can use either **Run- Length Encoding or PackBits** that is used for MacOsTherefore, compressing sampled packets can significantly reduce the channel overhead. We will also use techniques to reduce flow table entry for improving performance of the SDN.

Fig. 3. Conceptual Workflow for Sample Compression and Flow Table Reduction.


1
Controller Sets Rule for Openflow switches
2
Enforcer Send packet for sampling at Mastermind(resided in controller)
MasterMind processed sample packet and send to two module :
i.Sample Reduction Module
ii. Openflow table reduction module
Sample sent for compression
3
Flow table entry reduction
5
Sample reduction module in controller
Received sample and reduce it for better performance
Reduced sample
4
Reduced flow table entry
6
Open Flow table reduction module reduces flow table entry for handling bottle neck at controller
7
Enforcer Block the traffic based on sample received from mastermind
8
DDoS Attacks blocked according to sample received from controller
9

How it works:

Step1.Controller in SmartHome sets rules for Openflow switch For forwarding and or dropping the packets.

Step 2. Enforcer module at Home will collect sample packet and send to Mastermind module in the cloud based firewall.

Step 3. Mastermind process the sample and send it to Sample reduction module for reduce redundant samples using compression method. Compression takes place by reducing Flow table entry for multiple same entry. Like PackBits used in Macintosh user. Study shows that it has not been used for SDN approach. In PackBits 1,2,3,3,3,4 is replaced by 1,2,3,-2,4. **–digit** shows that previous number is used (number +1) times in the string. So in flow table suppose we have entry like:

Source	Destination	Action
123.112.11.1	134.123.112.2	forward
123.112.11.2	134.123.112.2	Forward
123.112.11.3	134.123.112.2	Forward

We can reduce entry like

Source	Destination	Action
123.112.111,-2.1,2,3	134.123.112.2	Forward

And upon extraction, we have to develop an algorithm that get IP address from above pattern.
Step 4. Compressed reduced sample will be sent back to SDN based Firewall. Mastermind module
Step 5. Mastermind will send it to flow table reduction module for reducing bottleneck at controller.
Step 6. Reduced flow table entry will be sent to Mastermind.
Step7 and 8. According to this sample, enforcer will decide which packet will be blocked for avoiding DDoS attack at smart home .
Step 9. DDoS attack will be blocked based on reduced sample to improve performance of smart home based firewall.

V. *Tools and technical skills required:*

- Basic knowledge of security, a programming language like c++, java, python will require.
- To implement SDN we need to study OPENFLOW protocol.
- To provide simulation we need to use MiniNet and Flood light.
- Need to Study FleXight for SDN Based Firewall understanding.
- Need to Stuy FleXam for sampling protocol for SDN based Firewall.

VI. Research Gaps Identified

A review of existing literature identifies several gaps:

1) Lack of integrated frameworks combining sample compression with SDN-based firewall mechanisms.
2) Limited techniques for compressing redundant sampled packets before transmission.
3) Absence of practical flow table reduction strategies tuned for smart home environments.
4) Inadequate evaluation of sampling algorithms under heterogeneous smart home traffic conditions.
5) Need for coordinated controller–enforcer architectures capable of real-time DDoS mitigation.

VII. Conclusion

This paper reviewed SDN-based smart home security research, focusing on DDoS defense mechanisms. SDN provides a flexible foundation for enforcing fine-grained security policies, yet challenges persist in sampling overhead, flow table congestion, and scalable firewall deployment. A conceptual direction combining sample compression and flow table reduction presents an opportunity for improving SDN firewall performance in future studies.

REFERENCES

[1] Toward Software Defined Smart Home, Ke Xu, Xiaoliang Wang, Wei Wei, Houbing Song, and Bo Mao,IEEE Communications Magazine • May 2016

[2] N. McKeown et al., “Openfl ow: Enabling Innovation in Campus NetworksACM SIGCOMM Comp. Commun. Rev., vol. 38, no. 2, 2008, pp. 69–74

[3] SDN: Evolution and Opportunities in the Development IoT Applications, International Journal of Distributed Sensor Networks Volume 2014, Article ID 735142,

[4] J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy, S. Ratnasamy, and V. Sekar, “Making middleboxes someone else's problem: network processing as a cloud service,” SIGCOMM Comput. Commun. Rev., vol. 42, no. 4, pp. 13-24, Aug. 2012

[5] SDN in the home: A survey of home network solutions using Software Defined Networking Abdalkrim M. Alshnta1, Mohd Faizal Abdollah1 and Ahmed Al-Haiqi2* Alshnta et al., Cogent Engineering (2018), 5: 1469949

[6] A Host-based Intrusion Detection and Mitigation Framework for Smart Home IoT using OpenFlow

[7] Protecting Home User Devices with a SDN-based Firewall Sajad Shirali-Shahreza, Member, IEEE, Yashar Ganjali, Senior Member, IEEE

[8] FleXam: Flexible Sampling Extension for Monitoring and Security Applications in OpenFlow

[9] FleXight: Flexible Information Channel for Software-Defined Networking. Shirali-Shahreza_Sajad_201803 PhD_thesis

[10] S. Mansfield-Devine, “DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare,” Network Security, vol. 2016, no. 11, pp. 7-13, Nov. 2016.

[11] J. H. Lee and H. Kim, “Security and Privacy Challenges in the Internet of Things [R0Security and Privacy Matters],” IEEE Consum. Electron. Mag., vol. 6, no. 3, pp. 134-136, Jul. 2017.

[12] Mehdi, S.A., Khalid, J., and Khayam, S.A. 2011. Revisiting traffic anomaly detection using software defined networking. In RAID'11. 161-180.

[13] S. Shirali-Shahreza and Y. Ganjali, “Delayed Installation and Expedited Eviction: An Alternative Approach to Reduce Flow Table Occupancy in SDN Switches,” *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1547–1561, Aug. 2018.