A secured SDN framework for IoT

Kshira Sagar Sahoo, Bibhudatta Sahoo, Abinas Panda
Department of Computer Science and Engineering,
National Institute of Technology, Rourkela, India- 769008

***Abstract*—In the last couple of years Software Defined Network (SDN) have come into existence which empowers network operators with more flexibility to manage and program their network. This type of network solves the limitation of legacy networks. Data plane and control planes are separated from each other as a result data plane devices simple act as a packet forwarding device and leaving the decision making part to a centralized system called controller. Though it has a lot of advantages, still security of SDN is an open issue. In modern day living wireless sensor network (WSN) technologies come across all most all areas which creates another research dimension called IoT where sensors and actuators blend in one piece. Application of SDN architecture in the IoT environment is a higher challenge. In this article we will present the security challenges in SDN and a secured architecture for IoT in an SDN based network.**

***Index Terms*—SDN, IoT, Ad-hoc network**

I. Introduction

Secured communication is a major concerned while data is being transmitted from one place to another. On the other hand, with the most recent Internet technology development, billions of gadgets are interfacing with users utilizing both wired and wireless framework. As a result, it uncovered users and network devices to numerous potential threats. A special security mechanism must be worked out to the Internet of Things (IoT), since it incorporates each device with network capacities. In other words, it is an environment where each objects are having a unique identifiers and has ability to transfer data over a network without needing human-to-human or human-to-computer interaction.
In the conventional system, Intrusion Detection System (IDS) like security instrument is deployed at the edge level of the Internet. Those systems are utilized to keep safe the system from outside threat. Such systems are not sufficient to handle the security of the cutting edge Internet. IoT based on the borderless system architecture which raises extra threat to the system access control. Security is a major issue for an ad-hoc system for IoT.

The new systems administration would be, the Software Defined Networking (SDN), offers numerous chances to secure the system in a more productive and adaptable way [1]. SDN architecture solely focused on separation of the control plane from the forwarding plane in the network. In legacy network as per the built in instructions of the switches, packets are moved to the same destination along the same path. Where as in an SDN scenario, packet forwarding rules are managed by the controller. This controller is an application running on a server somewhere within the network. Controllers and network devices often communicate via an interface, usually OpenFlow interface [2]. OpenFlow was originally developed for researches to run and develop experimental protocol later it was widely used in campus networks, data centers etc.
This paper highlights the major security issues in SDN , along with the security model for the IoT in the SDN framework. Besides, we have added the proposed construction model, keeping in mind the end goal is to incorporate Ad-Hoc systems with the network devices.

II. A Bits of Software Defined Network

Software-Defined Networking (SDN) is a game changing, cutting edge technology in the network field that has attracted many people from industry and academia. In this new paradigm decoupled the control plane from data plane and enables the network control to be programmable.

Moreover a greater focus on security mechanism is required for SDN at the controller-application level. The questions have been raised authentication and authorization mechanisms, in a multi-tenant setting, that would allow protection of resources of multiple organizations accessing the network . A security model must be designed to take care of changing various requirements of the applications.

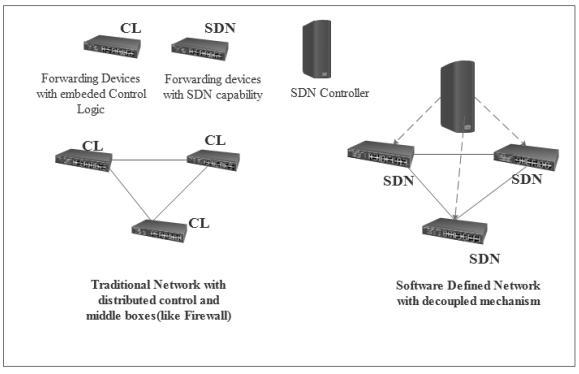

Fig. 1. SDN architecture

A. SDN Architecture

SDN has emerged as to meeting the challenges of legacy network. It allows networks to respond dynamically to fluctuations in usage patterns and availability of network resources [4] [5]. There are four additional components in SDN as compared to traditional network.

- Control Plane
  This plane is a part of SDN that carries signaling traffic, monitoring the network and responsible for routing. The controller of the control plane brings an abstract view of the complete network infrastructure by connecting to the switches via OpenFlow protocol [3]. NOX, POX, Floodlight, Beacon controllers are the most commonly used controller.
- Northbound Interfaces
  The northbound APIs are the most critical API in SDN architecture. Interfaces among the software modules of the controller and the applications of SDN running on the top of the network platform are characterized by these API. Northbound Application Program Interfaces support wide variety of applications, includes dynamic provisioning of quality of service to the end user, performing intrusion protection system and enabling firewall on the deployed device.
- East-West Protocols
  This protocol used where multi-controller-based architecture, come into the picture. This protocol handles interactions among various controllers.
- Southbound Protocols
  The forwarding (deployed) devices in the SDN network architecture are coming under data plane. The communication between the controller and the deployed device is commonly referred to as south bound API. The OpenFlow protocol most used south bound protocol. It is used to send commands from controller to deployed device.

III. SECURITY INVESTIGATION ON SDN

Confidentiality, integrity, availability, authentication and non-repudiation are the basic five properties of a secure communications network. Security professionals always try to protect the network from malicious attack and accidental damage. In the similar way the newly born SDN network architecture must be secured and satisfying the above properties. SANE, Ethane like architectures [6] consider the security aspects of an isolated control and forwarding infrastructure. Ethane is a simplified version of SANE which allowed more programmable to both data and control plane. Ethane is having certain similarity with SDN and OpenFlow, but it has certain problems related to network policy. But today's SDN network architecture provide various services. Security is the main perspective of the application layer in the SDN framework which has shown in the Fig.1. We have collected some challenges associates with different layer and interfaces of SDN.

A number of investigations on security issues of SDN have recently been performed. At first, paper [7] highlighted the DoS attack on OpenFlow protocol. In [8] authors have presented a deep analysis of the overall security of SDN with OpenFlow switch specification describing the usage of transport layer security. New threats are introducing on SDN because of many reasons, among them centralized controller and the programmability of the network. Researchers have been proposed many techniques in order to address the various threat issues. Lastly, ProtoGENI [9] a network testbed , have discovered numerous attacks. We have taken the various classification of

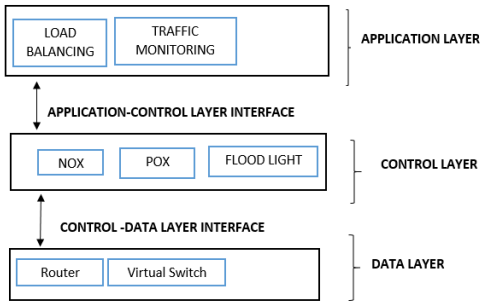

Fig. 2. Architecture of SDN illustrating the different layers and interfaces

the SDN security issues from [10] which is in Table I. From the table it is observed that the control and data layers are major point of attack.

A. Single Point of Failure

Related works on single point of failure has discussed in [12], [14] . A security frame work has been developed by the authors for failure of a single controller. In a SDN environment where a single controller used , a Denial of Service (DoS) attack is a major threat. Furthermore, compromising the SDN controller an attacker can have full control over the network. A major risk is associated with a single controller in the entire network. Multiple controller is the solution for reduce the risk and enhance trustworthiness to the system [11]. Upon failure of one controller, another SDN controller can take over the control to prevent system failures.

B. Coordination among Multiple Controllers

A standard TCP connection is required to communicate among switches and the controller. One of the main advantages of the controller is obtaining the global view of the network. Introduction of multiple controllers increase the network performance, since each controller has a partial view of the network, adding to this the controllers cooperatively exchanging information with each other.

IV. SDN BASED AD-HOC ARCHITECTURE

In [13] one SDN model has been proposed, here we expand these thoughts into IoT. This paper present that a node can be seen as a combination of legacy interfaces, programmable layer and an SDN controller. More over a controller has full access to the data-link layer switches and controllers present in the network follow the same standards. Ad-Hoc clients will associate with different nodes through their embedded SDN-compatible switch. At the same time, the SDN controller, in equivalent communication, can improve the security and availability among the nodes.One of the benefits of this new SDN based Ad-Hoc system model is its compatibility with SDN legacy system.Since every node in the Ad-Hoc system

TABLE I
SECURITY ISSUES RELATED TO DIFFERENT SDN LAYERS

Security Issues	Application Layer	Application-Control Interface	Control Layer	Control-Data Interface	Data Interface
Unauthorized Access					
Unauthorized Control Access			T	T	T
Unauthorized Application	T	T	T		
Data Leakage					
Flow Rule Discovery					T
Forward Policy Discovery					T
Data Modification					
Flow rule modification to modify packets			T	T	T
Malicious Application					
Fraudulent Rule Insertion	T	T	T		
Control Hijacking			T	T	T
Denial of Services					
Control Switch Communication Flood			T	T	T
Switch Flow Table Flooding					T
Configuration Issue					
Lack of TLS Adoption			T	T	T
Policy Enforcement	T	T			

has a pre-installed SDN-compatible switch and a controller, we can interconnect the Ad-Hoc system to the legacy system to develop an Extended SDN area depicted in Fig.3, in addition all rules can be synchronized among controllers in the extended domain because of cooperative nature of the controllers.

Existing routing protocols are mostly used by SDN, but proposed middleware relies on ad hoc networking services written in the application layer present on each node. Neighbor nodes are identified by using periodic Hello packet.
Control messages like route request (RREQ),route reply (RREP) and route error (RERR) are required to built a secure connection among nodes in the Ad-Hoc scenario. Compatibility with SDN system and SDN based Ad-Hoc model is the main advantage which help to develop an Extended SDN domain (Fig 3) . Ad-Hoc users will associate with different nodes through their inserted SDN-compatible switch. At the same time, security policies must be adopted that are designed to ensure an appropriate level of security by SDN controller.In addition all rules can be synchronized among controllers in the extended domain because of the cooperative nature of the controllers.

Since each IoT device has its own particular SDN controller, the controller needs to deal with the SDN virtual switch on every update. At the same time when another device add to or leaves from the system, numerous messages like RREQ and RREP need to exchange to get synchronize in the system. Keeping in mind to ensuring a fault tolerant system, usage of multiple controller in SDN environment is a better alternative.

Initially distributed SDN model working on small Ad-Hoc zone, moreover these controllers will be in charge of observing the conduct of the virtual switches. A new proposed architecture can handle the faster response to the unpredictable network change. While sharing the load with the main controller it is desired to have a secured communication in transit. In [13] the authors describes a proposed SDN architecture for IoT environment but they have not given any security mechanism to it. But various security issues related to IP based IoT has illustrated in [16].

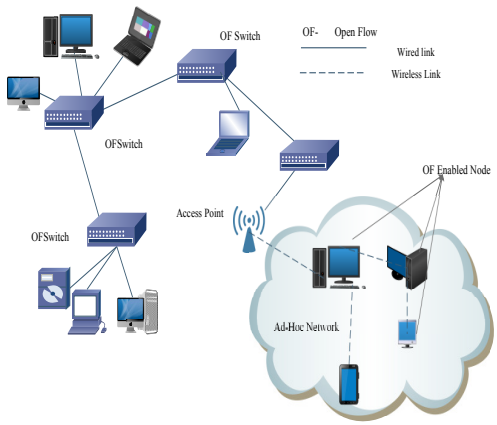

Fig. 3. The extended SDN Domain

The IoT embeds some intelligence in Internet-connected devices to communicate, exchange information, take decisions, invoke actions and provide wonderful services to the human being. Since it is difficult to have an in-built SDN compatible switch on each device in IoT environment, we have assumed that in the network domain few node having SDN capabilities. The node having sufficient resources would be considered as OF (OpenFlow) node otherwise treated as it is a smart device. A SDN controller domain denotes an enterprise network or a datacentre. In the proposed model a single or multiple SDN controllers is used in the each SDN domain which manages devices pertaining to that domain. A new type of controller is used to achieve a large scale interconnection i.e. Border controller. All security rules and routing functions can be distribute to both controllers as well as to the border controller. If due to some reason the border controller are fails to manage, other controllers come into picture. To take care of potential

issues raised by the heterogeneity of the security strategies particular to the interconnected SDN areas, we are proposing to use a middle-ware proposed in [15].

V. SECURITY MECHANISM FOR SDN BASED IOT

Here we have proposed an architecture that provides a security mechanism and dynamic network configuration to the network. Due to the absence of the network-less infrastructure, global traffic monitoring is not possible in Ad-Hoc. For achieving better security service, the controllers start authenticating to the network devices. All switch ports are immediately blocked by the controller whenever a secure connection establish between the switch and the controller. After user authentication, the correct flow entries will push to the switches. It is same for the IoT environment, where authentication process includes Internet enabled devices. There is an association among the network devices with OF enabled node, where each node is connected to the controller. Controller of each domain exchanges their security rules with another. In order to ensure network safety in the SDN domain there are some SDN controllers which behave as security guards on the edge of the network. Whenever there is a need of communication between two nodes present in different domain, initial transmission flow is moved towards security controller.Then the security controller asks to each neighbor controller whether they know the destination of the requested flow. At any point of time failure of a border controller of any domain, a pre-selected controller will act as border controller and monitor the traffic.

VI. CONCLUSION

This paper must be considered as the first step towards the construction of a general secured architecture for SDN based IoT environment. In the initial part of this paper we have made an attempt to highlight the various security issues related to the layers of SDN framework. Also we have discussed a SDN based network architectures with distributed controllers in the context of Ad-Hoc network and IoT. Border Controllers are the special controllers deployed for inter domain and secure communications within the extended SDN domain . In case of failure of a Border controller one of the pre-selected controller within the domain act as a border controller. Finally grid of security introduced in each controller to prevent attacks. In fact, several issues remain open. In future work we work to build this architecture and test it in a real test-bed.

REFERENCES

[1] Sood, Manu. "Software defined networkArchitectures." Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on. IEEE, 2014.

[2] Sezer, Sakir, et al. "Are we ready for SDN? Implementation challenges for software-defined networks." Commun6ications Magazine, IEEE 51.7 (2013): 36-43.

[3] Jammal, Manar, et al. "Software defined networking: State of the art and research challenges." Computer Networks 72 (2014): 74-98.

[4] Shin, M.K., Ki-Hyuk Nam, K.H., Kim, H.J., "Software-Defined Networking (SDN): A Reference Architecture and Open APIs," Proceedings, 2012 International Conference on ICT Convergence (ICTC), pp.360361, 1517 October 2012.

[5] IBM, Software-Defined Networking: A New Paradigm for Virtual, Dynamic, Flexible Networking, October 2012.

[6] M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker, Ethane: Taking control of the enterprise, in ACM SIGCOMM Computer Communication Review, vol. 37, no. 4. ACM, 2007, pp. 112

[7] R. Kloeti, OpenFlow: A Security Analysis, April 2013. [Online]. Available: ftp://yosemite.ee.ethz.ch/pub/students/2012-HS/MA-2012-20 signed.pdf

[8] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, Threat modeling-uncover security design flaws using the stride approach,

[9] D. Li, X. Hong, and J. Bowman, Evaluation of Security Vulnerabilities by Using ProtoGENI as a Launchpad, in Global Telecommunications Conference (GLOBECOM 2011). IEEE,2011, pp. 16.

[10] S. Scott-Hayward, G. OCallaghan, and S. Sezer, SSDN security: A survey, in Proceedings of the IEEE SDN for Future Networks and Services. pp. 1-7, 2013.

[11] Network Functions Virtualization (NFV), OpenDaylight,http://www.opendaylight.org/, [Online; accessed 12-July-2015].

[12] R. Braga, E. Mota, and A. Passito, Lightweight DDoS flooding attack detection using NOXIOpenFlow, in Local Computer Networks (LCN), 2010 IEEE 35th Conference on. IEEE, 2010, pp. 408415.

[13] FLAUZAC, Olivier, et al. "SDN based architecture for IoT and improvement of the security."

[14] H. Jafarian, E. Al-Shaer, and Q. Duan, Open flow random host mutation: transparent moving target defense using software defined networking, in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 127132.

[15] O. Flauzac, F. Nolot and C. Rabat; and L. Steffenel, Grid of security: A new approach of the network security, in Proceedings Third International Conference on Network and System Security.

[16] Heer, Tobias, et al. "Security Challenges in the IP-based Internet of Things." Wireless Personal Communications 61.3 (2011): 527-542. 6772, 2009.