Topic : Architecture iot
Scope :
IoT and Architecture
Security Architecture for IoT Network

Title	Security Architecture for IoT Network
Type	- Computer Science
Volume & Page	-
Year	2015
Author	FLAUZAC Olivier, GONZALEZ Carlos, NOLOT Florent
Reviewer	Yunus Oktaviansyah, M. Yajid Alfian, Yussi Kurniasih, Elis Malana
Date	-

Introduce

IoT is a concept where an object has the ability to communicate data through a network without requiring human-to-human or human-computer interaction. IoT has evolved from the convergence of wireless technology, micro-electromechanical systems (MEMS), and the Internet.

Software Defined Networking (SDN) emerged as a strategy to increase network functionality, reduce costs, reduce hardware complexity and enable innovative research.

In context, SDN-based architecture works within infrastructure, which we call SDN-Domain. This work describes the operation of the proposed architecture and summarizes the opportunities to achieve network security more efficiently and flexibly with SDN

Software Defined Networking Architecture

SDN Is a concept of a computer network approach where the control system of the data flow is separated from its hard role :

Here developed 3 architectural layers used inside

1. Tissue layer

2. Control layer

3. Application layer

One important feature of the SDN architecture is its ability to extend the security perimeter to the network access point of the point device (access switch, wireless access point, etc.

SDN Architecture for Ad-Hoc Network

the advantage of this new SDN-based Ad-Hoc network architecture is its compatibility with SDN legacy networks. Because each node on the Ad-Hoc network has a switch compatible with the embedded SDN and SDN controller, we can connect the Ad-Hoc network to the legacy network to build the SDN-domain

the advantage of this new SDN-based Ad-Hoc network architecture is its compatibility with SDN legacy networks. Because each node on the Ad-Hoc network has a switch compatible with the embedded SDN and SDN controller, we can connect the Ad-Hoc network to the legacy network to build the SDN-domain.

SDN Basic Architecture for IoT

Diogo et al have proposed a new architectural model for IoT, because the current situation is not designed to support high-level scalability, high amounts, traffic and data mobility. Our system proposed a secure SDN-based architecture for IoT and Ad-hoc networks.

Conclusion

This journal provides an understanding of the latest SDN-based network architecture with distributed controllers used in the context of Ad-Hoc and IoT networks. This journal considers network access control and monitoring global traffic for ad-hoc networks. Current security mechanisms such as Firewalling, Intrusion Detection and Prevention Systems are deployed on the edge of the internet. This mechanism is used to protect the network from external attacks

1. **Objective**

Resetting an SDN network architecture in applying to IoT has a very positive impact because this SDN uses ad hoc architecture so that security and use can support high level scalability, high amounts, traffic and mobility of data.

2. **Subjective**

This journal presents a new architecture with several SDN controllers in the same interaction. This reset proposes an architecture that can be scaled with many SDN domains. In each domain we can have a network with or without infrastructure and each controller is only responsible for the domain. The Ad-Hoc Network Architecture is also applied to the latest network system, 5G, so it is recommended to be used in the next IoT development.