Research Article Impact Factor: 4.226 ISSN: 2319-507X
Shilpa V. M., IJPRET, 2015; Volume 3 (9): 760-770 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DISTRIBUTED MOBILITY MANAGEMENT WITH SDN

SHILPA V. M[1], NILIMA DONGRE[2]

1. M.E. (Computer Science and Engineering) R.S.C.E., Buldhana.
2. Dept. of computer sci. &engg, Prof. R. S. C. E., Buldhana.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Today's cellular network is not a centralized as that of traditional. Centralized Mobility Management (CMM) introduces delays for network functions and also presents a single point of failure related to Mobility Management. With Distributed Mobility Management (DMM), the mobile network core evolving towards an un-layered and decentralized architecture, it appears to be more compatible and efficient. This paper focuses on the DMM with Software Defined Networking (SDN) technique. SDN for DMM introduces multiple controllers which harmonizes the DMM mechanism and also update the involved forwarding tables directly in case of handover. It consist the solution for the SDN's mobility and secure handover as it does not support IP mobility , with the help of Open flow and HIP which is an integration of HIPv1 layer with the existing Open Flow version to replace the SSL/TLS based mutual authentication.

Keywords: CMM, DMM, SDN, OPENFLOW Protocol

Corresponding Author: MS. SHILPA V. M.

Access Online On:

www.ijpret.com

How to Cite This Article:

Shilpa V. M., IJPRET, 2015; Volume 3 (9): 760-770

PAPER-QR CODE

INTRODUCTION

This new era of cellular network is not a centralized as that of traditional one which has conducted to deployment models are centralized. Mobility management with centralized mobility anchoring in existing mobile networks is quite prone to suboptimal routing and issues related to a single point of failure, and inevitably introduce longer delays [6]. Distributed Mobility Management (DMM) a new architectural design for evolving mobile IP networks [1] introduces the new way of handling the mobility. The detailed comparative study about the mobility management [2] describes current and traditional mobility architecture. However, when a mobile node i.e. a source node moves to another point of anchor, the previous flow is forwarded to current router by the previous router. For this reason, the optimization of router could be a consequence. [7] Proposes a routing optimization method in distributed architecture and the SDN [3] concept which is applied to DMM architecture for the routing optimization. OpenFlow architecture includes Open Flow switches which do not allow being mobile [8]. The openflow pcc rules and flow rules maintains the flow table updating [9] Openflow-HIP employs secure mobility with openflow [8]. The rest of this paper is organized as follows. Section II represents related work and literature survey. Section III compares Mobility Management techniques in detail. Section IV briefly addresses the SaDMM i e Software Defined Networking for DMM [2] with Openflow protocol and its secure mobility problem, architecture of proposed system. At the end Section V concludes the paper.

Literature Survey

Mobility Management

Future mobile networks are the combination of the Internet and telecommunication networks together. In this case Mobile Node (MN) served by the Internet Protocol (IP) to the network entities that connect the wireless networks to the Internet. Due to the merge of the two different techniques (i.e cellular mobile and data-communication) by the future mobile systems on IPv6 has become increasingly interesting. The all IP mobile network i.e the next generation network has issues of IP Mobility management [1] ; which enables the serving networks to maintain MN connection as it continues to change its point of attachment (i.e., handover management) and map the MN point of attachment for delivering data packets (i.e., location management.. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them [15]. All base stations are integrated into one area, allowing a cellular network to cover a wider area (location area).The location update procedure allows a mobile device to notify a cellular network when shifting between areas. The location update procedure call encounters that a mobile device has an area code which is differs from a previous update, then the location update service call is raised by the mobile device, by sending a location request to its network, prior location and specific Temporary Mobile Subscriber Identity (TMSI). Location area is nothing but a group of base stations assembled collectively to optimize signalling overhead. Base stations are integrated to form a base station controller (BSC), a single network area. Roaming is also the basic procedures of mobility management, enables subscribers to use mobile services when moving outside of the geographical area of a specific network.

CMM

Centralized schemes require the management of centralized entity and its relation with MNs. It requires the management of either one or no. of several hierarchical tunnels, to maintain the data path between the MN and a central entity. The fig.1 below gives the brief idea about how the mobility management is happened through centralized database. A single data path is preserved by each MN. Due to the simplicity to deploy such single tunnels, they are broadly used. However, those tunnels introduce data overhead due to the necessary encapsulations, as well as at their end-points data processing to perform encapsulations and de-capsulation functions.

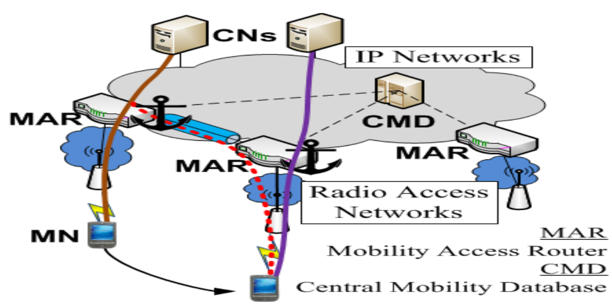

Figure 1: CMM

The effected overhead may impact, not only access networks, but also core network links, and possibly wireless links. In networks, central entities require to maintain a considerable number of per-user tunneling contexts, which may cause scalability issues. Centralization of the data path introduces bottleneck issues and single point of failure that cannot be solved without costly dimensioning and redundancy engineering.

DMM

CMM faces several problems and limitations such as low scalability, suboptimal routing, signaling overhead, more complex network deployment, also single point of failure [2]. For this reason several mobile operators are finding for alternative solutions which are more distributed in nature, which allows efficient and cheaper network deployments [1]. This new prototype is defined as Distributed Mobility Management (DMM).

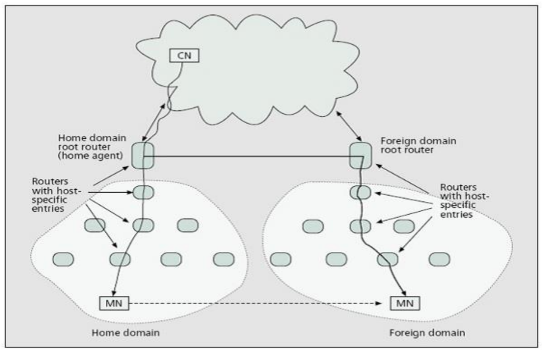

Figure 2: DMM

Fig 2.2 generalizes the idea about the DMM Architecture. DMM is a flatter system. The mobility anchors are placed closer to the user which distributes the data and control infrastructures among the entities located at the edge point (access point) of the network. DMM may be partially or fully distributed. Which distribution scheme should apply, it depends on which technique is going to follow by network. The partially distributed scheme where the distribution scheme is applied to data plane only and the distributed anchor keeps the location information provided by a centralized entity. In a fully distributed approach the distribution scheme is applied to both the Data plane and Control plane and this information is stored at every distributed anchor point which used to share with its peers. The distribution of the mobility anchors is improved scalability and robustness of the mobility infrastructure. In DMM the placed mobility management functions always attain routing optimality and lower delays.

SDN

SDN i.e. Software-defined networking [8] is a new way to networking that allows network managers or administrators to manage network services through lower level abstraction of functionality. This is done by uncoupling the system that makes decisions about where traffic is sent from the underlying systems that forward traffic to the selected destination i.e. from control plane to the data plane. SDN requires some method for the control plane to

communicate with the data plane. One such mechanism is Open Flow. SDN is architecture that cost-effective, is dynamic, manageable and adaptable, making it ideal for dynamic and the high-bandwidth nature current applications The Open Flow protocol is a foundational element for building SDN solutions. Fig 3 describes the overview about the architecture of the SDN and its components. The following list defines and explains the architectural components:
• *SDN Application (SDN App):* SDN Apps are programs that directly, and programmatically communicate to the SDN Controller via a northbound interface (NBI).

• *SDN Controller*: The SDN Controller is centralized entity used for understanding the requirements from the SDN Application layer to the SDN Data paths and also provides the SDN Applications with an abstract view of the network. An SDN Controller consists of more no. of the SDN Control Logic NBI Agents, and the Control to Data-Plane Interface (CDPI) driver.

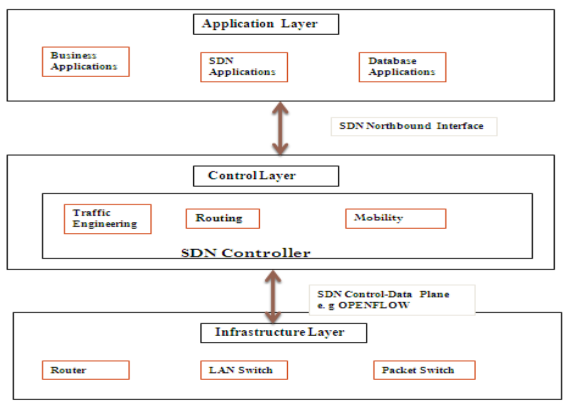

Figure 3. SDN Architectural Diagram

• *SDN Data path:* The SDN Data path is a logical network device. It revels and uncontained control and visibility over its advertised forwarding and data processing capabilities.
• *SDN Control to Data-Plane Interface (CDPI):* The SDN CDPI is the interface between an SDN Controller and an SDN Data path, which provides (i) capabilities advertisement, (iii) programmatic control of all forwarding operations, statistics reporting, and event notification.

OPENFLOW

OpenFlow [8] is the first standard communications interface defined between the control and data layers of SDN architecture. OpenFlow allows direct access to forwarding plane and manipulation of the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based).OpenFlow is needed to move network control out of the networking switches to logically centralized control software. The OpenFlow protocol is implemented on both sides of the interface between network infrastructure devices and the SDN control software. OpenFlow supports and uses the concept of flows that used to identify network traffic based on pre-defined match rules that can be statically or dynamically programmed by the SDN control software. OpenFlow-based SDNs can be deployed on existing networks, both virtual and physical. Network devices can support OpenFlow-based forwarding as well as traditional forwarding, which makes it easy for enterprises and introduce OpenFlow based SDN technologies, even in multi-vendor network environments.

Messages in Open Flow protocol:

The Open flow protocol consists of three types of messages: controller-to-switch, synchronous and symmetric.

1. Controller-to-switch messages are to

- Specify, modify or delete flow
- Request for information on switch capabilities
- Retrieve information such as, counters from the switch.

2. Asynchronous messages are sent by the switch to:

- Send the controller a packet. The packet that does not match an existing flow of mobility.
- Inform the controller that a mobility flow has been removed
- Inform the controller that there is an error has occurred on the switch or a change in port status.

3. Symmetric messages can be sent by both the switch and the controller and are used for:

- Hello messages exchanged between the controller and the switch.
- Echo messages determine the latency of the switch-to-controller connection and also verify that the controller-to-switch connection is still operative or not operative.

SDN and DMM

DMM architecture with SDN concept for routing Optimization:

The purpose of this concept is to make optimized routing path from the DMM architecture [7].

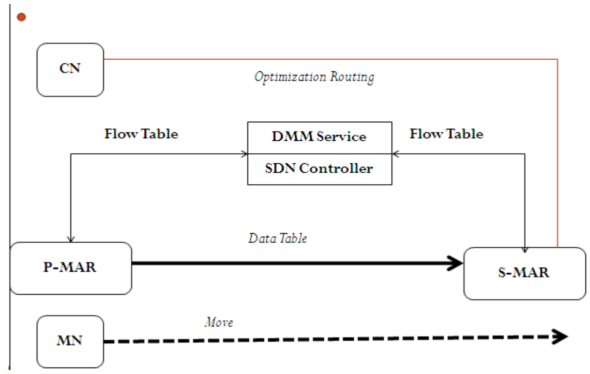

Figure. 4 SaDMM

If data path is controlled by SDN controller in the DMM architecture with a DMM service that stored mobile node status, mobile node data path which is possible to set up by optimized path. Tunneling is not necessary when receiving data from previous router. The architecture of method is shown in the figure 4.

A. Handover process and potential optimization routing:

In the architecture, mobile node is supported mobility management by binding update to controller with DMM service. As in a Figure 4, as soon as mobile node attaches to initiate router, P-MAR sends a Packet in Message which includes MNs ID, for registration to the controller. On accepting this Packet in Message, a Packet out Message is sent by the controller and controller stores mobile node information in binding cache entry. For set up the data path, a Flow Modify message is sent by the controller to set up the flow table in the P-MAR. If the mobile node moves e.g. to the S-MAR, the S-MAR sends a Packet in Message which includes mobile nodes ID, new location of mobile node(S-MAR). As soon as the controller receives packet in message, it will check and update BCE. On receiving this Packet in Message, a Flow Modify message is sent by the controller to P-MAR, S-MAR to set up the new data path. On receiving flow modify messages, the S-MAR and P-MAR will update their routing tables. Then the data session will flow to new S-MAR from P-MAR and finally to the mobile node.

B. Advantage of DMM architecture with SDN

SDN which has a very flexible way to set up data flow can provide a solution to support efficient route in the DMM architecture.

1. Routing optimization

2. No need to control the Data

C. Problem Statement: What is missing in OpenFlow?

1. Flow processing: Change of address from network switches or routers would disrupt flow processing i. e has a mobility problem.
2. Secure session management: Change in an IP address also destroy active SSL/TCP sessions.
3. Secure handover: Problem of support mobility and mutual authentication also certificate exchange is not desirable for fast moving Open Flow clients.
4. Flow rule management: since flow rules must be updated frequently, change of IP address to solve latter issue causes additional overhead.

D. *Secure SaDMM:*

In this work we are going to focus on the two problems, which have described briefly in the following section. Also it is explaining about the solution of the same.

Mobility Issue:

In SDN architecture, the centrally managed control layer in a software-based controller maintains the overall view of the network. The controller grants the flexibility to manage, configure, secure the software, and also help to optimize network resources via dynamic and automated software programs. One such realization of SDN is OpenFlow that exploit new opportunities over the existing networking. OpenFlow at the current stage is not able to support mobility [8]. This is a critical limit of OpenFlow. Current SDN architecture inhabited critical issues in robust multipath connectivity for fault tolerance. This is even more essential when the switch or the controller is mobile. In one hand, number of channels between the controller and the switch can guarantee a certain level of assurance for consistent or smooth connectivity. Mobile routers, mobile switches mobile base stations, mobile, mobile clouds and server migration are some of the powerful reasons why mobility is insisted in SDNs. This would cover and extend SDN benefits into mobile environments such as moving buses, moving trains, buses, flights and other moving automobiles.

E. Secure handover issue:

Problem of cannot support mobility and mutual authentication and certificate exchange is not preferable for moving clients of OpenFlow.

Solution:

The fig. 6 below will illustrate the system architecture where the routers and switches configured on the fly. The flow control agents (FCA) on the mobile routers and switches are very essential on mobile switch or routers and updating the software controller of the new location information which is helpful in location based services. The flow rules built on top the newly introduced cryptographic global identifiers which remain unchanged over time. Thus, updatation of the flow rules due to mobility is no longer useful. This would reduce the processing overhead and control traffic overhead due to dynamic address configuration because of mobility and thus, flow processing. Over more, it reduces overhead in the PCRF i.e. policy charging and rules function and improve the flexibility with QoS management and network configurations.

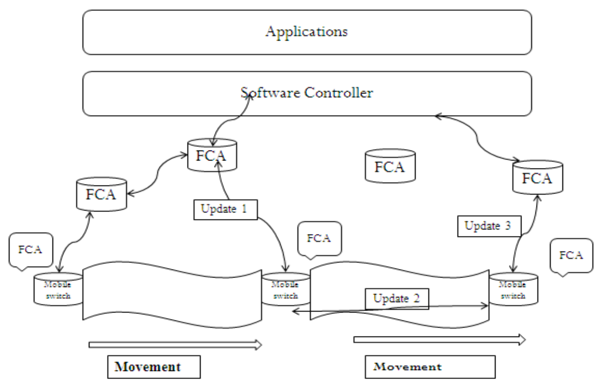

Figure 5 Secure SaDMM Scenario

The present technique of SSL over TCP begins new security threats known as TCP-level attacks. There are several serious security weaknesses or flaws inherent in the protocol e.g. SYN attacks, sequence prediction attack, reset attack, ICMP attacks and DoS attacks. The OpenFlow routes and switches connect to the remote control processor, viz. the controller handles the TCP requests. Therefore, an attacker's aim is to seek to break or change into the controller. Thus, if the attacker found any security related weaknesses in the controller the attacker will penetrate into the network. TLS implementations do not currently check certificates of client. If a similar approach is used with OpenFlow, it will vulnerable to any man-in the- middle attack. The specifications do not provide the certificate format also not indicate what fields in the certificate are used for naming. OpenFlow pertain the use of TLS without specifying a version number or a reference number. This would result in non-interoperable implementations if different implementations of OpenFlow use different versions.

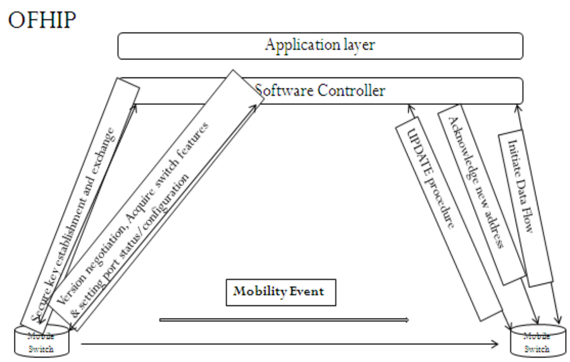

Figure. 6: Secure Handover-update procedure

Comparisons and Analysis

We have done comparison work on three existing methods of Mobility Management which is a CMM, DMM, SaDMM with our forth new technique i.e. Secure SaDMM. With considering the issues related handover

Delay, tunneling, Scalability issues etc explained detailed study on all techniques. The TABLE I below entitled the same.

POINTS TECHNIQ	HANDOVE	DELAY	TUNNELING	DATA PROCESSING	SCALABILITY ISSUES	NETWORK ISSUES
CMM	IP Address changes so session will be broken	High	Fixed tunneling for each node	Yes	Yes	-Optimal Routing issues -Costly for Service Provider -Single pt. of failure
DMM	Separating the session Identity	Medium	Temporary	Yes but diminished	Diminished More (In case of lots of MN)	- Admin level issue -Self configuration
SaDMM	Controller will update the involved forwarding tables	Low	No Tunneling	No	No	-Securing the controller -Visibility loss -OPENFLOW can't support Mobility
Secure SaDMM	Secure Handover	Low	No Tunneling	No	No	Though it provides security, SDN's Controller cannot check the client certificate.

Table 1. Comparison Table

CONCLUSION

Mobility management is used to trace physical user and subscriber locations to provide mobile phone services, like calls and Short Message Service (SMS)UMTS and GSM are each made up of separate cells (base stations) that cover a specific geographical area .The mobility management related information is maintained in the distributed controllers, which are organized in different domains rather than centralized controller like CMM. By modifying the Flow Tables at the involved gateways, the routes can be optimized inherently. A SaDMM is an efficient mechanism for mobility management oriented to the future mobile network architecture as SDN uses Open flow protocol which does not support mobility and has issue of secure handover, mutual authentication. The new architecture i.e Open flow HIP layer protocol for these issues of Open flow, presents the architecture that enables Open Flow switches to change their IP addresses securely during mobility.

REFERENCES

1. H. A. Chan, Distributed Mobility Management with Mobile IP,IEEE ICC 2012 Workshop on Telecommunications: from Research to Standards, June 2012, Ottawa

2. P Bertin, S Bonjour, J Bonnin" Distributed or Centralized Mobility?" Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, 1-6

3. Yuhong Li; Haimeng Wang; Ming Liu; Bofan Zhang; Huanqu Mao, "Software defined networking for distributed mobility management," Globecom Workshops (GC Wkshps), 2013 IEEE , vol., no., pp.885,889, 9-13 Dec. 2013

4. Nunes, B.A.A.; Mendonca, M.; Xuan-Nam Nguyen; Obraczka, K.; Turletti, T.,"A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," Communications Surveys Tutorials, IEEE , vol.16, no.3, pp.1617,1634, Third Quarter 2014

5. Zuniga, J.C.; Bernardos, C.J.; de la Oliva, A.; Melia, T.; Costa, R.; Reznik, A., "Distributed mobility management: A standards landscape," Communications Magazine, IEEE , vol.51, no.3, pp.80,87, March 2013

6. Requirements of distributed mobility management draft-ietf dmm-requirements-01 H. Chan (Ed.) Huawei Technologies July 12, 2012.

7. Hyunsik Yang, Younghan Kim Soongsil University "Routing Optimization with SDN" draftyang-dmm-sdn-dmm-01.txt October 2014 April 22, 2014

8. OPENFLOWhttps://www.sdncentral.com/sdn-essentials-primer/cisco-openflow.