Security Analysis of IEEE 802.21 Standard in Software Defined Wireless Networking

Asma Islam Swapna*, Nazrul Islam†
Department of Information and Communication Technology
Mawlana Bhashani Science and Technology University, Tangail, Bangladesh
E-mail: * asma0swapna@gmail.com, † nazrul.islam@ieee.org

***Abstract*—Software Defined Networking (SDN) is the best choice in establishing a software controlled inter-domain network. Convergence of different Wireless link technologies bring the mobile users to choose the network being in any geographical location. IEEE 802.21 is such a standard for exchanging networking information for connecting with the network being at any region in the world. Integrated with SDN wireless network this functionality of IEEE 802.21 standard can discover programmable network services with profound resource utilization. However, the information exchange should circulate through a reliable source. Hence, the security analysis of IEEE 802.21 Media Independent Handover (MIH) mechanism for Software Defined Wireless Network (SDWN) is the primary concern of this research work. This study, conducts architectural and functional analysis of MIH integrated with SDWN interface for mobility management of the wireless nodes. The outcome specifies a possible integration with future deployment opportunities in information exchange of IEEE 802.21 MIH for programmable network devices.**

Keywords*—*Software Defined Wireless Networking (SDWN), MIH, Handover Management, Handover Security, Network Security Analysis

I. Introduction

Software Defined Wireless Networking (SDWN), a branch of Software Defined Network (SDN) has been a key research technology to investigate and analyze as wireless network is growing super-fast [1] [2]. SDWN assures simple and scalable network architecture and effective mobility management for geographically expanded and standard service providing networks.

SDWN programmatically centralizes and separates the control plane (aka. Network OS) from the data plane (aka. Forwarding plane) of its wireless environment. A conventional architecture of SDWN is illustrated in Fig. 1. The whole network architecture is divided into two communication interfaces: southbound that contains the data forwarding entities and northbound consisting the service providing network applications. Both interfaces are connected with a centralized and software controlled device namely the SDN controller. In any SDWN network pane the southbound interface trains the SDN controllers to collect information about Mobile Nodes (MNs) and transmits and receives packets to and from MNs using SDWN elements [3]. For multiple controller enabled SDN network that is geographically distributed, a master controller performs master controlling of the network devices. During movement of the wireless MNs, a nearby Access Point (AP) is adjusted for seamless communication and control. During the adjustment handover of previous control session is performed and flow table is updated with handoff information and

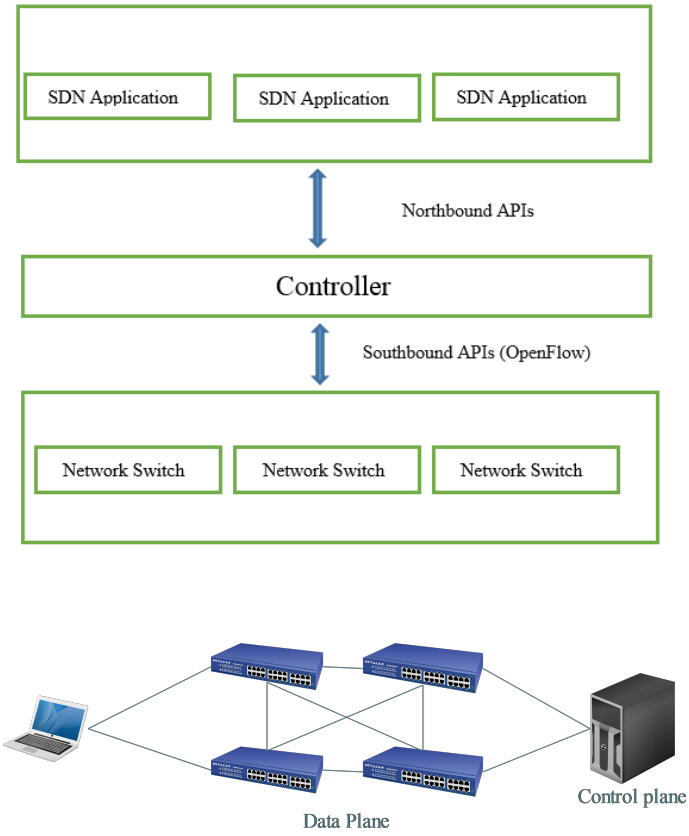

Fig. 1. SDN architecture with separated control and data plane structural and topological architecture.

newly adjusted APs information though mobility management protocol i.e. IP based mobility management. In general, a successful handover consists three phase; system discovery, handover decision and handover execution [4].

Network information discovery is highly critical for wireless and geographically distributed scenario i.e. SDWN. For such network interface, mobility management and handover efficiency is a challenge for different link technologies. However, IEEE 802.21 or Media Independent Handover (MIH) [5]. This can be a solution for inter-domain multiple controller communication in large complex SDWN industry/campus network where handover information is secure enough for outside intrusion.

Research work in paper [6], provides the foundation for

978-1-5386-1150-0/17/$31.00 2017 IEEE

handover management analysis for SDN mobile networks lacking the wireless adaptivity. Literature in paper [7], presented a secure handover solution for inter-domain network using Media Independent Pre-authentication (MIP), however is limited to allow programmability in the network plane. Hence, the prime concern of this research activity is integrating the ideology of MIH mechanism with wireless programable network interfaces, SDWN, providing mobility support in the architecture and performing security analysis on handover message exchange with the interface.

The structure of this paper is as follows. In Section II, the background and traditional handover methodology in SDWN. Section III introduces the MIH for SDWN while section IV represents the security and architecture analysis of IEEE 802.21. Section V thereby concludes the research work and future prospects of this analysis.

II. Background and Related Work

SDN approaches empowers the network allowing packet traversing and extracting the control plane from data plane to access the network resources even more than before. With emerging wireless network demands, SDWN is integrated for OpenFlow and is adopted in a number of commercial networks and research projects.

A. Software Defined Wireless Network

SDN leverage the network separating the control plane from packet forward plane as the concept allows to run the network in a more horizontal model. Network operation including routing, forwarding and access control is interfaced with service-oriented APIs provides on demand packet transmission throughout the network plane. SDWN is oriented towards the mobile and wireless network devices and aims at the research and study of crucial technologies for the future mobile and wireless network. This SDWN architecture is composed of both North-South and East-West network dimension where East-West operates for wireless and mobile devices using inter-controller protocols such as Border Gateway Protocol (BGP) [8]. The wireless nodes using Wireless MAC processor performs changing the point of adjustment with the most viable Access Point (AP) throughout the network [2]. During the change of adjusting APs, wireless nodes perform handover of network session. Hence, security of the underlying wireless network depends on the secured session handover.

B. Media Independent Handover

IEEE 802.21 or Media Independent Handover (MIH) facilitates the heterogeneous network to perform and optimize extensible access to the network hardware. It functions with the help of MIH function (MIHF) that incorporates media independent commands, events and available Information services [5]. For efficient handover optimization MIHF uses Service Access Point (SAP) interfacing and controls link layer procedure irrespective of the technology in concern, e.g. WiFi, WiMax, 3GPP, 5G LTE or even SDWN. Researchers in [9] mentioned MIH as the potential technology to adapt with OpenFlow-based Wireless Mesh Networks since it enables query link information. Fig. 2 depicts the MIHF entities with proper location in a MIH integrated network.

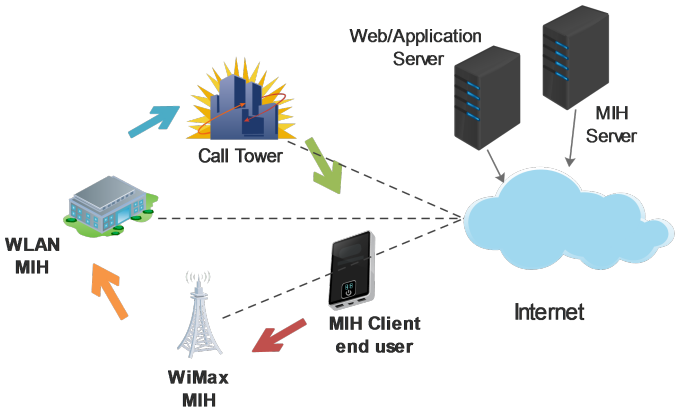

Fig. 2. MIH scenario to support handover in SDWN network infrastructure.

C. Handover Management in SDWN

SDWN has been a key research technology for this decade and project to be implemented in near future. The separation of data and control planes in wireless architecture prompts for inter-controller session handover and AP/SAP adjustments [6]. Fig. 2 depicts some MIH entities and MIH Functions classified based on location and equipment.

Centralization of the forwarding decision combined with MIH point of service (PoS) transmit MIHF directly to the wireless terminals such as smartphones, tablets, laptops or other mobile nodes. Control Terminals decide and confronts the handover to other Access Points (AP) based on mobility function. These multimode mobile terminals hence choose the optimal wireless network to connect with based on requirements, network characteristics and application services. Therefore, handover session security over the SDN interface comes to light to be handled with much delicacy and needs of the network demands. This handover is performed in link layer 2 through a key management and an authentication procedure. A secure channel or pre-handover and post-handover key management and sharing procedure can establish a more defined MIH for concerned SDWN interface [4]. The objective here is to analyze the security aspects that urges such communication channel and authentication requirements.

III. System Architecture and Operation

SDN in wireless scenario can be distributed of three different scenarios based on data transmission and data plane variants [6]. However, the mobile terminals and controlling plane still are separated in all the variants. This section upholds operation procedure in all three SDN wireless architecture variants and thereby depicts the MIH framework empowering efficient handoff in mobility management.

A. Centralized SDWN

Centralized variant of SDWN mobile network is controlled with a single centralized controller for all mobile nodes. With less delayed communication time single controller SDWN has scalability and reliability issues in handling multiple APs and mobile nodes at the same movement time. In such network, controller operation is minimized because of no need for

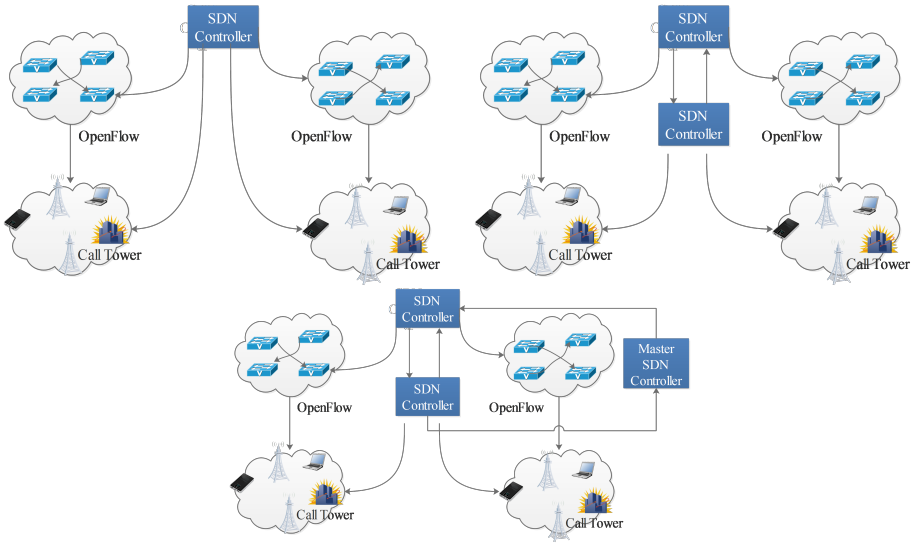

Fig. 3. Different variants of SDWN network based on controller number.

session handover among several controllers and to provide mobility through periodic node data collection and analysis.

For handover controller takes node status report and take decision on forwarding rules for available network routes. The controller hence has to have eNodeB, MME, PCRF and Mobile IP(MIP) management functionalities for handling handover [6].

B. Semi-Centralized SDWN

Semi-centralized SDWN carries multiple controller indifferent of different geographical regions. Each controller is divided and serves as a centralized SDWN controller for the perspective geographical region. Therefore, each dividend centralized SDWN network operates in the above-mentioned manner. Mobile nodes use a domain membership unique to every node and communicate with the centralized dividend controller for handover operation [10]. The controllers will pass the user node information, domain status and session details to the new controller in case of inter-controller communication and session handover. New controller can request to end the old session involving several MMEs. Higher latency and inter-domain session information exchange will be prone to security vulnerabilities in case of several frequent handover operations.

C. Hierarchical SDWN

Hierarchical SDWN lies in multiple semi-centralized SDWN controller layers and a complex evolution of Semi-centralized SDWN architecture. A controller on the upper layer of the architecture controls other distributed layer of controllers as a master SDWN controller. During handovers of SDWN interface sessions and mobility sessions all semi-centralized SDWN controllers have to exchange other session information with the master SDWN controller and ahead for handoff execution. In case of approved and completion of proper information update to the master SDWN controller a new controller for mobile nodes is initiated in the lower layers which ensures secure SDWN interface on geographically distributed hierarchical SDWN network. However, one drawback is the complexity of handover management and session information encryption during handoff [11].

All the variants are depicted in the Fig. 3 side-by-side for efficient comparison and understanding. Keeping in mind of above-mentioned scenarios, IEEE 802.16 (MIH) is proposed for analysis on different variants of SDWN network in inter-controller handoff moments [12]. The proposed handover framework for OpenFlow based SDWN provides a set of optimization facilities and functionalities in exchange of handover information for mobility scenarios. MIH allows network information flows and controls allowing to be deployed in any PoAs, APs, MNs, WLANs, WiMAX and even any link technologies [13].

The proposed framework is depicted in Fig. 4 featuring the SDWN controllers or Points of Service (PoSs) , Points of Access/Switches and MNs:

1) SDWN Controllers / PoSs: Points of Service or controllers performs routing decision making task and updates forwarding table and handles and configure the mobility procedures. Handover decisions hence controlled by the PoSs in IEEE 802.16 or MIH integrated SDWN. These functionalities are integrated with Mobility Management Module (MMM) in MIHF while communicating with the MNs on SDWN interface.

2) SDWN PoSs / Switch: PoAs executes data packet forwarding operations as instructed by the PoS controllers and based on flow table information. SDWN switches provide link connectivity and can integrate with MMM to provide MIH integrated functionalities to any link technologies.

3) Mobile Nodes: MNs are coupled with MIHF to along with SDWN interface towards the access links and Link SAPs. MN sends status information on change of PoAs to take decision on MIH handoff by PoSs during its movement over the geographical regions.

As the MNs move through the SDWN interface and

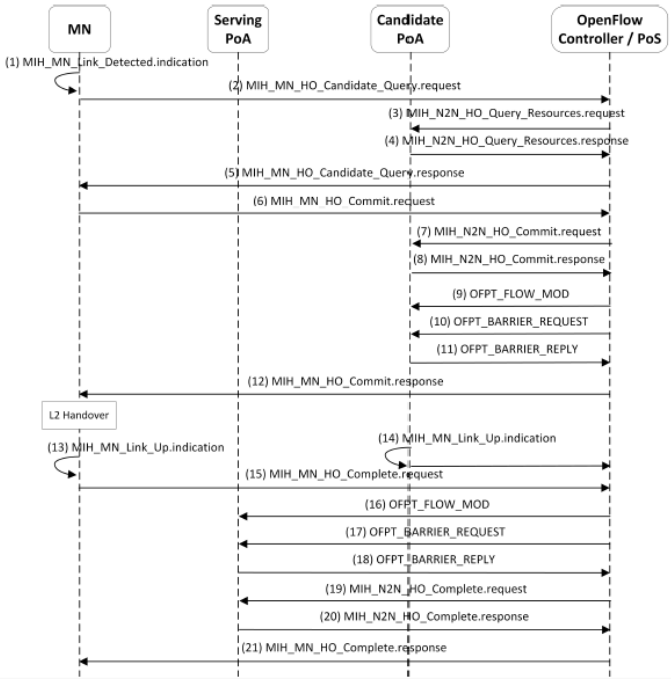

Fig. 4. SDWN integrated IEEE 802.21 MIH handover signaling and information exchange [15].

detects a new PoA nearby, handover is initiated and triggers MIH_MN_HO_Candidate_Query.request towards controller PoSs. PoSs find the resource availability and issues to commit the handover. The requested PoA if selected and acknowledged about the handover and incoming MNs connection request, sends OFPT_FLOW_MOD message to the PoS for initiating handover information. Without the acknowledgement message the handover is not initiated. Again, PoS controller does not approve any handover without acknowledging all other PoAs about the new PoS update for the concerned MN. The sequence of this message is irregular in each exchange. The exchanged handover information is performed in encrypted format using Elliptical Curved Discrete Logarithm Problem (ECDLP) and Elliptic curve diffie-Helman (ECDH) [14]. Keys are generated The IEEE 802.16 MIH integration with SDWN interface as depicted in the Fig. 4.

IV. Result Analysis

This section evaluates the security concern of handover information exchange between PoSs, PoAs and MNs in any SDWN interface and inter-controller communication. For comparison, Li et els scheme [16] has been taken for the follow-study among the different handover procedures. On that scheme, certain terms, Mutual Authentication, Privacy Preservation, Forward and Backward Security, Reply Attack resistance, Forgery Attack Resistance etc. are taken into consideration for analysis metrics. Table 1 in below upholds the comparative security analysis of IEEE 802.16 MIH integrated with SDWN that operates as above-mentioned.

1) Mutual Authentication: Mutual authentication ensures the participating components conducts communication with verified and legal interface. In MIH integrated SDWN interface, PoSs, MNs and PoAs communicates exchanging handover and node reports after acknowledgement of each other. PoSs recognize the MNs with unique domain identification information within the same hierarchy. On the other hand, MNs are acknowledged of PoSs and newly attached PoA with OFPT_FLOW_MOD and MIN_MN_HO_Candidate_Query.response messages.

TABLE I. Security Comparison of IEEE 802.21 MIH integrated with SDWN.

Security Requirement	Li et. al.	IEEE 802.21	Securing Feature
Mutual Authentication	Yes	Yes	OFPT_FLOW_MOD and MIN_MN_HO_Candidate_Query.response messages
Privacy Preservation	No	Yes	OFPT_FLOW_MOD
Forward and Backward Security	No	Yes	ECDLP, ECDH
Reply Attack resistance	Yes	Yes	ECDLP, ECDH
Forgery Attack Resistance	No	Yes	MIIS

2) Privacy Preservation: In the MIH integrated SDWN, handover is initiated after receiving the OFPT_FLOW_MOD and commit instruction receival by the both PoSs and MNs. This reserves the privacy of each participating components in any link technologies operated through SDWN interface.

3) Forward and Backward Security: In order to satisfy this security requirement, the protocol IEEE 802.16 should satisfy that during the handover information exchange in encrypted form, no outside entity and interface gets access of the key generated and shared among the SDWN components (PoSs, MNs, PoAs). In this integrated SDWN interface, the handover keys are unique for each session and protected by ECDLP, ECDH.

4) Reply Attack Resistance: Attacker may find some information regarding the exchange handover messages and replay the attack in future using such unprotected information. However, in this case, ECDLP and unique irregular message sequence for each exchange.

5) Forgery Attack Resistance: Unauthorized modification in the handover message sequence can lead to gain attached to vulnerable PoSs and beyond the control or SDWN PoSs where new untrusted entity can gain attached to the selected PoAs inside the interface. Hence, handover message sequence should have proper integrity. MIH provides encryption and random sequence which reduces security vulnerabilities relating to forgery attacks and resist the handover authenticity throughout the session in every layer of the SDWN controller interface.

A secure Media Independent Information Service (MIIS) reduces the most of the attack probabilities. It performs through handover signaling mechanism as depicted in Fig. 4 above with several different phases.

V. Conclusion

In this paper, the main characteristics and security aspects of IEEE 802.21 integrated SDWN is discussed and analyzed. The integrated SDWN meets security requirement in several

different aspects including Mutual Authentication, Privacy Preservation, Forward and Backward Security, Reply Attack resistance, Forgery Attack Resistance etc. The comparative study shows an imminent possibility of adopting IEEE 802.21 in inter-domain multiple controller communication in more complex and large SDWN network. Along with security and big industry adaptivity, MIH provides mobility management in IP based wireless link technologies.

The future prospects of this SDWN integrated IEEE 802.16 MIH protocol and prospective security analysis will lead to persistent research on assessment of SDWN appliance in data center, cognitive networks and mobile communication. This study will lead the security mechanism deployment over the analyzed protocols to ensure a less vulnerable SDWN architecture. In the future, more detailed information exchange between nodes, including simulations of the analyzed concepts will be done.

REFERENCES

[1] L. M. C. Carlos J Bernardos, Antonio De La Oliva and H. Jin, "An architecture for software defined wireless networking," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 52–61, 2014.

[2] M. R. Sama, L. M. Contreras, J. Kaippallimalil, I. Akiyoshi, H. Qian, and H. Ni, "Software-defined control of the virtualized mobile packet core," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 107–115, 2015.

[3] J. B. You Wang and K. Zhang, "Design and implementation of a software-defined mobility architecture for ip networks," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 40–52, 2015.

[4] I. Saadat, F. Buiati, D. R. Cañas, and L. J. G. Villalba, "Overview of ieee 802.21 security issues for mih networks," in *ICIT 2011: Proceedings of the 5th International Conference on Information Technology*, 2011.

[5] E. Piri and K. Pentikousis, "Ieee 802.21: media independent handover services," *The Internet Protocol Journal*, vol. 12, no. 2, pp. 7–27, 2009.

[6] S. Kukliński, Y. Li, and K. T. Dinh, "Handover management in sdn-based mobile networks," in *2014 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2014, pp. 194–200.

[7] A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez, and H. Schulzrinne, "Media-independent pre-authentication supporting secure interdomain handover optimization," *IEEE Wireless Communications*, vol. 15, no. 2, pp. 55–64, 2008.

[8] N. A. Jagadeesan and B. Krishnamachari, "Software-defined networking paradigms in wireless networks: a survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 27, 2015.

[9] P. Dely, A. Kassler, and N. Bayer, "Openflow for wireless mesh networks," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*. IEEE, 2011, pp. 1–6.

[10] P. Dely, A. Kassler, L. Chow, N. Bambos, N. Bayer, H. Einsiedler, C. Peylo, D. Mellado, and M. Sanchez, "A software-defined networking approach for handover management with real-time video in wlans," *Journal of Modern Transportation*, vol. 21, no. 1, pp. 58–65, 2013.

[11] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4g lte/sae networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 2, pp. 457–468, 2014.

[12] H. Kim and N. Feamster, "Improving network management with software defined networking," *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013.

[13] C. Guimarães, D. Corujo, R. L. Aguiar, F. Silva, and P. Frosi, "Empowering software defined wireless networks through media independent handover management," in *2013 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2013, pp. 2204–2209.

[14] J. Hur, H. Shim, P. Kim, H. Yoon, and N.-O. Song, "Security considerations for handover schemes in mobile wimax networks," in *2008 IEEE wireless communications and networking conference*. IEEE, 2008, pp. 2531–2536.

[15] G. Yi and S. Lee, "Fully distributed handover based on sdn in heterogeneous wireless networks," in *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication*. ACM, 2014, p. 70.

[16] C. Li, U. T. Nguyen, H. L. Nguyen, and N. Huda, "Efficient authentication for fast handover in wireless mesh networks," *computers & security*, vol. 37, pp. 124–142, 2013.