An Overview of 802.21a-2012 and Its Incorporation into IoT-Fog Networks Using Osmotic Framework

Vishal Sharma[1], Jiyoon Kim[1], Soonhyun Kwon[1], Ilsun You[1](✉),
and Fang-Yie Leu[2]

[1] Department of Information Security Engineering, Soonchunhyang University,
Asan-si 31538, Republic of Korea
vishal_sharma2012@hotmail.com, 74jykim@gmail.com, tnsgus08@gmail.com,
ilsunu@gmail.com

[2] Computer Science Department, ThungHai University, Taichung City 407, Taiwan
leufy@thu.edu.tw

Abstract. The increase in the number of devices has caused a major issue for the service providers to support the users irrespective of the type of services demanded by them. With the advent of fog computing, a near user evaluation site is available that can lower the burden on the core network by providing cloud-like services to the users. However, handling multiple IoT devices near-site requires fast and media independent handovers. This paper incorporates 802.21a-2012^{TM} into the fog network by overcoming the trust requirement and pre-registration policies of this standard using osmotic computing. The proposed framework uses an Osmotic Absorption Key (OAK) to control the handoffs between the fog layers. The proposed solution is highly flexible and inexpensive in terms of implementation cost for handling handoffs of dynamic IoT devices in Fog networks.

Keywords: Fog computing · Osmotic computing · MIH · Handovers

1 Introduction

Connecting billions of devices is not an easy task because of the difference in the make and configuration of each device. Internet of Things (IoT) aims at bridging the gap between the devices allowing them to help our everyday operations. With the number of devices increasing exponentially, it becomes important to reduce the gap between the center of operations and the requesting equipment. Fog computing, as stated by CISCO, is a unique solution for reducing the gap between the requesting device and the service providers by facilitating near-user computing [1].

The concept of fog computing has enhanced the implementation and maintenance of IoT devices. Fog computing is a self-sufficient mini-cloud near the user

Y.-B. Lin et al. (Eds.): IoTaaS 2017, LNICST 246, pp. 64–72, 2018.
https://doi.org/10.1007/978-3-030-00410-1_9

with similar facilities as that of public/private cloud for computational offloading [2]. Fogging although reduces the level of data which is shifted towards the main hub or the public cloud, yet has some complexities associated with its fully-functional deployments because of complex cloud infrastructure [3–7]. With a large number of users transmitting over the fog layers, it is evident that the number of handoffs will be very high, which needs to be tackled efficiently without leveraging excessive computational burden on the fog servers [8,9]. Further, this problem becomes severe due to the difference in the type of IoT devices, which demands handoffs between the different fog setups.

Handoffs between different media can be tackled by the use of Media Independent Handoffs (MIH) IEEE 802.21 [10]. This standard allows easy transitions between the devices operating with different media across the Point of Attachments (PoA). However, 802.21 MIH cannot assure the security during handoffs, which is extended in its lateral version under the name IEEE 802.21a [11]. Although 802.21a is efficient in providing secure MIH, yet is suffers from a disadvantage of requiring one legal network entity to support pre-established trust for every Mobile Node (MN). Also, the execution time for the handovers is high in extremely dynamic networks. In this paper, osmotic computing is considered as a solution which operates with the push key operations of the 802.21a to support unbundled media access proactive authentication. Three different handover scenarios are presented between the MN and the mobile PoA. The proposed osmotic framework provides key absorption strategy and uses an Osmotic Absorption Key (OAK) to control the handoffs between the fog layers.

2 Background to MIH Standards

This section presents an overview of 802.21 MIH and a detailed functionality of 802.21a-2012^{TM}.

2.1 802.21 MIH

Focusing on the need for seamless and media independent handovers, IEEE 802.21 standard was proposed by the internet work group. The work group for 802.21 readily resolved the issues which existed in IEEE 802.11 and 802.16 to support handoffs at high transmission rates with lower latency. 802.21 is based on the context of an MN and all other components are obtained on the basis of their relationship with the corresponding MN [12,13]. 802.21 uses a variety of service triggers to perform handoffs which include, link-up, link-down, rollback, and a handover complete, etc. All these events are triggered using MIH_SAP command. The command services are the controlling units which define the handoff policies to support MIH. Three different services are defined in MIH, namely, Information Services (MIIS), Event Services (MIES) and Command Services (MICS). The other details on the standard MIH framework can be obtained from Refs. [10,12] and [13].

2.2 802.21a-2012^{TM}

Despite being efficient, the 802.21 is unable to provide any security mechanisms during handovers. Also, it does not consider the authentication mechanism between the MNs, PoA, and Point of Service (PoS). A variant of this standard was proposed to support the security over 802.21 with an extended name of 802.21a-2012^{TM} [11,14,15]. The new variant is capable of providing enhanced security during handoffs by defining new functions for MIH and new MIH messages. IEEE 802.21a standard focuses on providing service access security and proactive authentication in two different passes. The first pass regulates the service authentication and the second pass controls the proactive authentication and key management. With an addition of new services, this standard is capable of reducing the latency issues of earlier standards. An illustration of service authentication and proactive authentication for this standard is presented in Fig. 1(a). The PoAs are the media independent entities which are operable using different communication standards but served by a common PoS. Once an MN moves across the network, the PoS provides the handover support by overcoming the media-dependent issues allowing both services as well as proactive authentication to the requesting MN. However, there exists a gap in this standard as the source PoS is unaware of the target PoA (tPoA), which may allow loopback attacks on the network.

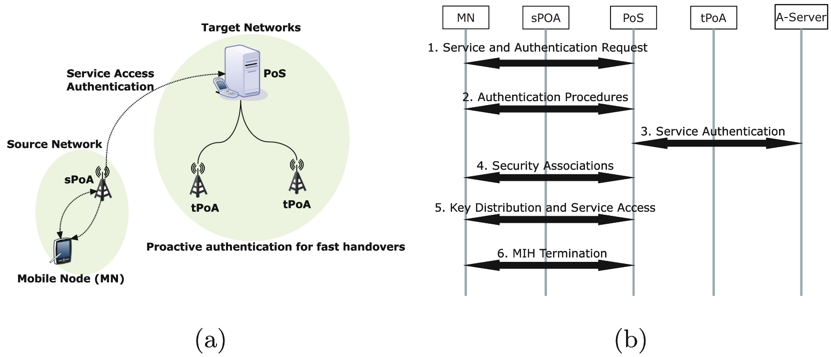
Target Networks
Service Access Authentication
PoS
Source Network
sPoA
tPoA
tPoA
Proactive authentication for fast handovers
Mobile Node (MN)
MN
sPOA
PoS
tPoA
A-Server
1. Service and Authentication Request
2. Authentication Procedures
3. Service Authentication
4. Security Associations
5. Key Distribution and Service Access
6. MIH Termination
(a)
(b)

Fig. 1. (a) Service assessment and proactive authentication for 802.21a-2012^{TM}. (b) EAP-based service protection in 802.21a-2012^{TM} [11,14].

802.21a-Service Authentication. The service security in MIH is provided either by using Transport Layer Security-based MIH or by Extensible Authentication Protocol (EAP)-based MIH. The choice of two depends on the application scenario and registration policies of MN. However, as stated in the initial draft of 802.21a, EAP-based authentication is considered for general authentication as most of the current scenarios operate on a pre-established trust over the MN.

- TLS-based Service Protection: This approach allows protected transport layer sessions for securing the MIH service messages. The security is driven by a

Master Session Key (MSK) by using a three field packet data unit. MSK is the key role player between the MN and the PoS whereas PoA has the least significant role in supporting the MN message authentication.
- EAP-based Service Protection: This approach is suitable for the scenarios where the authentication server maintains the trust of an MN with the underlying infrastructure. EAP-service authentication can be used by considering any of the existing mechanisms for service protection. In the standard 802.21a, basic EAP is used to protect the MIH services as shown in Fig. 1(b). The first step generates the service request and indicates the PoS for authentication. The second step controls the authentication phase between the MN and the PoS. The third step controls the authentication between the authentication server and the PoS. The fourth step handles the security associations. The fifth step handles the access phase for acquiring the requested services and finally, the sixth step terminates the MIH procedures [14].

802.21a-Proactive Authentication. The proactive authentication for the MIH-802.21a is provided either as an unbundled media access proactive authentication or as a bundled media access proactive authentication.

- Unbundled proactive authentication: This authentication procedure utilizes the media specific authentication by forming a tunnel between the communicating entities. The unbundled authentication can be significant in the scenarios that have a large number of MNs which are not pre-registered with the authentication server or the specific trust management entity of the network. However, the utility of unbundled proactive authentication in such scenarios requires further extension in the 802.21a standard as the requesting MN needs to be authenticated over a secure channel between the source PoS and the tPoA. Currently, such support is not provided by this standard [11,14,15].
- Bundled proactive authentication: This authentication procedure is suitable for the scenarios with a pre-established trust for every MN. Thus, considering this property, the bundled proactive authentication utilizes the EAP-based service protection in combination with the key generation operations to support proactive authentication in MIH framework. The success of security depends on the types of application and key operations used for generating the security keys. In general cases, bundled operations use Media Specific Root Key and Media Specific Pairwise Master Key along with pull or push operations [11,14].

802.21a-Key Management. Key management in 802.21a is provided by three different approaches, namely, push key, reactive pull key and optimized proactive pull key distributions. The choice of approach depends on the application scenario and type of connectivity between the PoA and the PoS. Push key and reactive pull key are used for EAP-based scenarios with reactive pull key providing a faster authentication. Optimized proactive pull key is used in the scenarios where no proactive trust exists between the entities involved in the handovers.

3 Problem Statement and Our Contribution

With the advent of security over MIH standards (802.21a), it becomes relatively easier to provide handover solutions to the mobile fog users. However, despite the capabilities of 802.21a-2012^{TM}, there are certain key issues that restrict its use for extremely mobile IoT devices that are operational under fog computing environments. The first issue is the non-correspondence between the tPoA and the PoS as 802.21a-2012^{TM} does not provide any support for the previously connected PoS and the tPoA. However, the initial draft of 802.21a-2012^{TM} aims at using EAP-based solution by considering the pre-established trust for MN as provided by the service providers for service access authentication. Although, this is an effective strategy yet does not stand well in the case of mobile PoA. The second issue is the placement of the authentication server in fog computing environments. Further, the requirement of the pre-registration of MN, as well as the mobile PoA between the PoS, is an open problem for using 802.21a-2012^{TM} in IoT-Fog environments.

The proposed approach integrates the fog computing with the virtual osmotic computing paradigm. This helps in resolving the issues related to the requirement of pre-registration of MN that otherwise prohibits the use of unbundled media access authentication of 802.21a-2012^{TM}. The proposed approach provides a framework which not only incorporates the 802.21a-2012^{TM} for supporting dynamic IoT devices in fog computing, but also reduces the overall handover time. The proposed osmotic framework is capable of handling mobile PoA and also manages the keys during the entire session which are used to relate the source PoS with the tPoA.

4 Osmotic Framework for Dynamic IoT-Fog Networks

Osmotic computing has been introduced as a new area of research for integrating the edge cloud systems [9]. Two core applications of osmotic computing are the management of services and the balancing of computational loads [2,8]. This computing is derived from the chemical osmosis process which uses a semipermeable membrane to allow the movement of solvent for balancing the concentration of the solution on its both sides. The semipermeable membrane acts as a decision support system for the movement of solvent. In this paper, osmotic computing is extended for providing 802.21a-2012^{TM}-assisted handovers in fog networks. The proposed approach is developed as an osmotic framework which is capable of resolving the problems with the unbundled media access handovers in 802.21a-2012^{TM} by virtually supporting the trust between the PoS and the PoA. The proposed approach considers three different scenarios each comprising a mobile PoA as a key entity in supporting handovers for highly dynamic MNs as shown in Fig. 2.

- The first handover scenario arises when an MN moves across the PoAs within the same PoS. Both the source PoA (sPoA) and tPoA are operated by the same PoS. Such scenario can be handled directly by using the 802.21a standard transition approach.

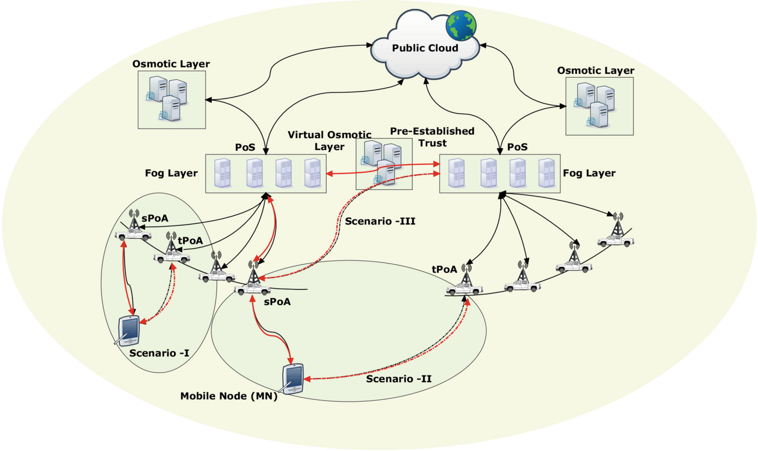

Fig. 2. An illustration of the network setup considered for analyzing 802.21a-2012 MIH using osmotic framework.

- The second handover scenario arises when an MN moves across the PoAs which are served by different PoS. In traditional 802.21a, such scenarios are suggested to use the ERP-based MIH proactive authentication. However, this solution requires pre-registration of MN, thus, cannot be directly applied to the second scenario.
- The third handover scenario arises between the mobile PoA and the PoS. The PoAs are considered to be moving at a high speed in a network between the PoSs.

IEEE 802.21a does not support the handover in the second and the third scenario and is resolved with the help of the proposed osmotic framework.

4.1 Key Management

The virtual osmotic layers help in managing the keys which are to be used for authenticating the mobile PoA across the PoS. For the first scenario, the standard push key solution of 802.21a can be applied. The virtual osmotic layer of each fog layer provides the keys for authentication, and all the push key operations are handled by the osmotic layer. The first scenario is exactly the one considered in the standard implementation of 802.21a. For second and third scenarios, the osmotic layer has way more role than mere an authentication server. It operates as the new entity and the source PoS and target PoS are cooperated by a pre-established trust which is maintained by tunneling one osmotic layer to the other osmotic layer. These operations are secured by absorption policies of the osmotic computing. The proposed approach uses an OAK to validate each osmotic layer as well as the PoS. OAK facilitates the use of unbundled proactive authentication by overcoming the communication issue between the source PoS and the tPoA which is not handled in the traditional 802.21a. The osmotic layer pushes the OAK into the network which helps in identification of the controlling PoS. This allows control over the IoT devices which are moving at a very high speed and do not offer much time to execute handovers.

4.2 Mobility-Aware Handoffs

For service access authentication with highly mobile PoA, it is not suitable to use the standard solution as EAP-based authentication requires pre-establishment of trust. Also, the unbundled approach does not guarantee the security since there is no facility for securing connectivity between the source PoS and the tPoA. The proposed osmotic framework pushes an OAK into the network via osmotic layer which facilitates the connectivity between the every entity in the network and the trust is maintained instead of assuming it. Once the MN reaches a terminal PoA, the PoS makes a key request to the osmotic authentication server, which relies on pushing the OAK in the network. It also shares an identical key with the tunneled osmotic layers. Once an MN communicates with the tPoA, it shares the new key which is generated using the previous OAK. This new key is transferred to an osmotic server of the target PoS which validates the new key by generating its source key and matching it with the one shared by the source osmotic layer. This procedure involves management of multiple keys by each osmotic authentication server as it may be tunneled to multiple layers at the same instance.

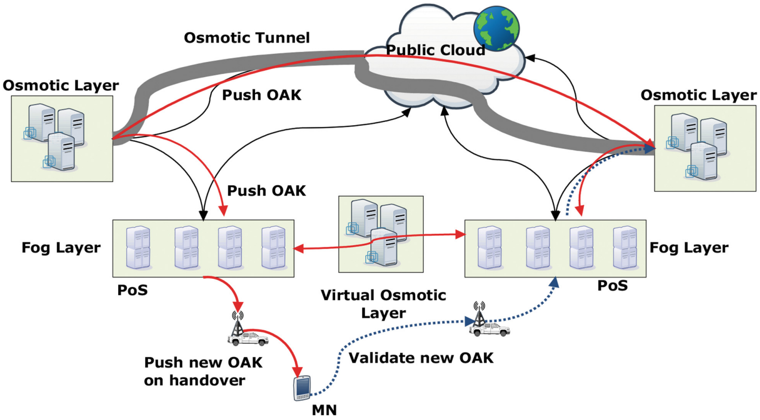

Fig. 3. An illustration of osmotic tunneling for OAK push operations.

5 Performance Case Study

The proposed approach overcomes the trust establishment issues with the 802.21a and allows an osmotic facility to incorporate it for handovers in dynamic

IoT-Fog networks. The mobile PoA can be authenticated between the source PoS and the target PoS by an OAK which is used to tunnel source and target osmotic layers. This allows the sharing of context as well as key information over the secured channel as shown in Fig. 3. The performance of the proposed osmotic framework is studied for two aspects, namely, cost and flexibility. The details of which are as follows:

- Cost: The cost of operation in the proposed approach varies with the scenario. The first scenario with IoT devices operates with the same cost as that of 802.21a standard and does not vary despite the target application. However, for the other two scenarios, the osmotic layer plays an important role by periodically pushing an OAK whenever a handover is initiated. The cost of operation for handovers of PoA and MN depends on the time consumed in maintaining a tunnel between the source and the target osmotic layer and the time taken in generation and validation of OAK. The unbundled authentication is strengthened by the proposed solution by providing secure communication between the source PoS and tPoA, however, it may cause some latency if the device overlaps with the multiple handover contexts at the same time. In the normal case, this communication depends only on the time taken by the PoA in absorbing the OAK from the tunneling source.
- Flexibility: The proposed approach is extremely flexible in implementation. In the proposed solution, the osmotic framework is considered which operates over a virtual layer that is created by using the servers from the fog layer. However, the proposed approach can be easily extended by deploying an independent osmotic network as suggested by the initial definition of osmotic computing. The virtual osmotic layer is considered to reduce the time in generation and acquisition of OAKs.

6 Conclusion and Future Directions

This paper presents an overview of security solutions for media independent handovers by considering 802.21a-2012^{TM} standard. An osmotic framework is presented which provides a strategy for incorporating 802.21a-2012^{TM} into the dynamic IoT-Fog networks. Three different handover scenarios are presented considering the MN and mobile PoA. The proposed osmotic framework provides key absorption strategy which operates similar to the push key but uses an Osmotic Absorption Key (OAK) to control the handoffs between the fog layers. The proposed solution is highly flexible and capable of handling extremely dynamic nodes by providing a handoff security even between the source PoS and tPoA. Further investigations and detailed implementation of the osmotic-assisted handovers in IoT-Fog networks using 802.21a-2012 will be presented in the future reports.

Acknowledgement. The work is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2016R1D1A1B03935619) as well as the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2014R1A1A1005915).

References

1. Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the Internet of Things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16. ACM (2012)
2. Sharma, V., Srinivasan, K., Jayakody, D.N.K., Rana, O., Kumar, R.: Managing service-heterogeneity using osmotic computing, arXiv preprint arXiv:1704.04213 (2017)
3. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data, pp. 37–42. ACM (2015)
4. Sbeyti, H., Malli, M., Al-Tahat, K., Fadlallah, A., Youssef, M.: Scalable extensible middleware framework for context-aware mobile applications (SCAMMP). Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. (JoWUA) **7**, 77–98 (2016)
5. Baiardi, F., Tonelli, F., Isoni, L.: Application vulnerabilities in risk assessment and management. J. Wirel. Mob. Netw. Ubiquitous Comput. Depend. Appl. (JoWUA) **7**, 41–59 (2016)
6. He, Q., Dong, Q., Zhao, B., Wang, Y., Qiang, B.: P2p traffic optimization based on congestion distance and DHT. J. Internet Serv. Inf. Secur. (JISIS) **6**, 53–69 (2016)
7. Jiang, X., Ge, X., Yu, J., Kong, F., Cheng, X., Hao, R.: An efficient symmetric searchable encryption scheme for cloud storage. J. Internet Serv. Inf. Secur. (JISIS) **7**, 1–18 (2017)
8. Sharma, V., You, I., Kumar, R., Kim, P.: Computational offloading for efficient trust management in pervasive online social networks using osmotic computing. IEEE Access **PP**(99), 1 (2017)
9. Villari, M., Fazio, M., Dustdar, S., Rana, O., Ranjan, R.: Osmotic computing: a new paradigm for edge/cloud integration. IEEE Cloud Comput. **3**, 76–83 (2016)
10. De La Oliva, A., Banchs, A., Soto, I., Melia, T., Vidal, A.: An overview of IEEE 802.21: media-independent handover services. IEEE Wirel. Commun. **15**(4), 96–103 (2008)
11. Marin-Lopez, R., Bernal-Hidalgo, F., Das, S., Chen, L., Ohba, Y.: A new standard for securing media independent handover: IEEE 802.21a. IEEE Wirel. Commun. **20**(6), 82–90 (2013)
12. de la Oliva, A., Melia, T., Vidal, A., Bernardos, C.J., Soto, I., Banchs, A.: IEEE 802.21 enabled mobile terminals for optimized WLAN/3G handovers: a case study. ACM SIGMOBILE Mob. Comput. Commun. Rev. **11**(2), 29–40 (2007)
13. Lim, W.-S., Kim, D.-W., Suh, Y.-J., Won, J.-J.: Implementation and performance study of IEEE 802.21 in integrated IEEE 802.11/802.16 e networks. Comput. Commun. **32**(1), 134–143 (2009)
14. 802.21a-2012 - IEEE standard for local and metropolitan area networks: media independent handover services - amendment for security extensions to media independent handover services and protocol. IEEE 802.21a, May 2012
15. Park, H., Lee, H.H., Lee, S.-H.: IEEE 802 standardization on heterogeneous network interworking. In: 2014 16th International Conference on Advanced Communication Technology (ICACT), pp. 1140–1145. IEEE (2014)