

## SECURITY ARCHITECTURE ON WIRELESS NETWORK TRAFFIC HANDOFF : A REVIEW

Sigit Wibawa<sup>1\*</sup>

<sup>1</sup>Department of Informatic Engineering, Universitas Trilogi, Indonesia

### ARTICLE INFO

#### History of the article:

Received June 18, 2021  
Revised July 4, 2021  
Accepted July 4, 2021  
Published July 9, 2021

#### Keywords:

Handoff  
Security Protocol  
Authentication  
Systematic Literature Review

### ABSTRACT

This paper provides an overview of the wireless handoff process on wireless networks by investigating Authentication Protocol using EAP - AKA (Extensible Authentication Protocol) - Authentication and Key Agreement The EAP-AKA protocol was developed for LAN networks or mobile network devices, the authors found ineffective network procedures guaranteed that made the attacks MITM and DoS attacks may occur. In addition, we find the storage procedures and resource submissions not safe enough to withstand DoS attacks. Focusing on Both types of attacks, the authors are interested in existing security protocol methods and written by researchers, then perform Systematic Literature Review (SLR) by using international journals database ie from the IEEE organization with the use of wireless handoff attack keyword in the middle of the world and obtained some related journals which need further research to deepen the Systematic Literature review, by offering a structured, methodical, and meticulous approach to understanding the research trends of handoff security issues on wireless networks and mobile networks. The purpose of this research is to provide credible intellectual guidance for future researchers to help them identify areas in the study. Most SLR is limited to conference papers and journal articles published by IEEE from 2015 to 2021. This study reveals that the protocol, privacy and security of the handoff process are the least studied, while the operating problems, architecture, methods in the handoff process get much attention in the literature.

### Correspondence:

Sigit Wibawa,  
Department of Informatic Engineering,  
Universitas Trilogi, Indonesia,  
Email : sigit@trilogi.ac.id

This is an open access article under the [CC BY-ND](https://creativecommons.org/licenses/by-nd/4.0/) license.



### INTRODUCTION

The wireless handoff process and overview of security architecture on wireless networks by investigating Authentication Protocol using EAP-AKA (Extensible Authentication Protocol) - Authentication and Key Agreement The EAP-AKA protocol was developed by 3GPP LAN networks or mobile network devices, the authors found the initial network procedure is not effectively secure that makes any delinquent and issue [1], [2], [3]. Focusing on these investigating Authentication Protocol attacking and we propose A Systematic Literature Review of security wireless handoff security. Handoff method is used to maintain the connection. This is related to the performance due to the process of switching traffic channels automatically on the mobile station to communicate without the occurrence of termination of the connection. The main factor of success in handoff lies in the quality of service that provides different levels of service assurance

in managing and prioritizing network traffic handoff consideration.

Consideration of the need for power or signal strength required for stable communication requires stable power or signal strength. Each Access Point, BTS and Antenna Provider have user or user limits so that the user's network density must be taken care of in order to prevent jams and cause undisturbed communication.

Distance communication is far and wide so it requires handoff or handover to serve the communication needs so it is still affordable with good quality [4]. Administrative considerations are usually for the needs of the Administration of communication between the Access point or operator so that the data obtained utilized for the interests of the administration for example when done Preservation or maintenance so that users diverted to the Access Point, BTS or others antenna so required handoff [5].

**RESEARCH METHOD**

The method used in this study [6], [7] uses three stages with nine blocks or steps which will be explained as follows: the first step identifies systematic needs and the second step develops systematic needs then the third step evaluates the review protocol this stage is called the planning stage, then there are blocks or The following fifth step enters the implementation stage [8], [9], namely searching for primary studies, selecting primary studies, extracting data from primary studies, assessing the quality of primary studies and synthesizing data, for the last step is the form of reporting from research, namely the stage of distributing results as shown in Figure 1 as below.

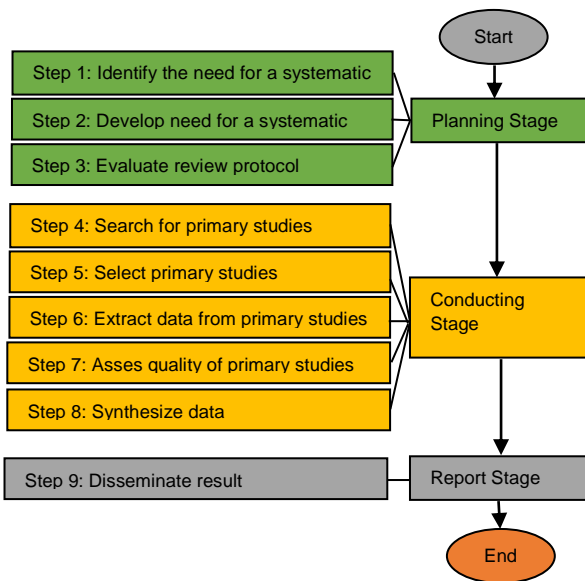


Figure 1. Prosesing Systematic Review Research

**Research Question**

The research Question (RQ) were specified to keep the review focused [10], [11]. They were design with the help of the Population, Intervention, Comparison, Outcomes, and Context (PICOC) criteria (kitchenham and Charters 2007). Table 1 shows the PICOC structure of research questions.

Table 1. Summary of PICOC

Question	Result
Population	Wireless handoffs, security, protocol, Authentication
Intervention	Wireless Handover, fault prediction, error, classification, models, methodes, techniques, authentication process
Outcomes	Prediction of the accuracy of the research area, revealing that the protocol, privacy and security of the handoff process
Context	Studies in industry and academia, small and large data sets

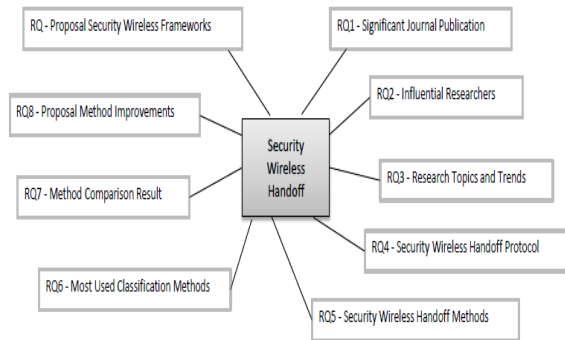


Figure 2. Basic Mind Map of the SLR on Security Wireless Handoff

The basic mind map is contained in a table which is grouped as a series of hypotheses in the form of research questions and motivation in table 2 below.

Table 2. Research Questions

ID	Research Question	Motivation
RQ1	Which Journal is the most significant security wireless handoff?	Identify the most significant journals in the security wireless handoff
RQ2	Who are the most active and influential researcher in the security wireless handoff field?	Identify the most active and influential researchers who contributed so much on are research area of security wireless handoff
RQ3	What kind of research topics are selected by researcher in the security handoff field?	Identify research topics and trend in software detect prediction
RQ4	What kind of protocols are the most used for security wireless handoff?	Identify protocols commonly used in security wireless handoff
RQ5	What kind of methods are used for security wireless handoff?	Identify opportunities and trend for security wireless handoff method
RQ6	What kind of methods are used most often for security wireless handoff?	Identify the most used methods for security wireless handoff
RQ7	Which methods performs best when used for security wireless handoff?	Identify the best method in security wireless handoff
RQ8	What kind of method improvements are proposed for security wireless handoff?	Identify the proposed method improvement for predicting security wireless handoff
RQ9	What kind of framework are proposed for security wireless handoff?	Identify the most used framework in security wireless handoff

**Search Strategy**

The search process (step 4) consists of several activities, such as selecting digital libraries, defining search strings, running pilot searches, refining search strings and retrieving

initial lists of primary studies from digital libraries that match search keywords. Before starting the search, an appropriate set of databases should be selected to increase the likelihood of finding highly relevant articles. The most popular library databases in the field are searched to have the widest possible set of studies the author determines the IEEE Xplore literature (ieeexplore.ieee.org) as reference for literature [12], [13].

The search string was developed according to the following steps:

1. Identification of the search terms from PICOC, especially from Population and Intervention
2. Identification of search terms from research questions
3. Identification of search terms in relevant titles, abstracts and keywords
4. Identification of synonyms, alternative spellings and antonyms of search terms
5. Construction of sophisticated search string using identified search terms, Boolean ANDs and ORs

The following search string was eventually used:

- **Wireless, handoff, handover, security, reliability process, wireless security authentication.**

A search string adjustment is performed, for the adjustment of the search string will dramatically increase the already extensive list an irrelevant study the search string is then adjusted to meet specific requirements. In Database searched with title, keyword and abstract. The Search is limited by the year of publication: 20015-2021. The type of publication of the journal papers and the limited Search conference on articles published in English.

### Study Selection

The inclusion and exclusion criteria were used for selecting the primary studies. These criteria are shown in Table 3.

Table 3. Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Studies in academic and industry using large and small wireless handoff authentication process	Studies without a strong validation or including experimental result of wireless handoff authentication process
Studies discussing and comparing modeling performance in the wireless handoff authentication process	Studies discussing defect prediction datasets methods framework in a context other than wireless handoff authentication issue
For studies that have both	Studies not written in English

the conference and journal version only the journal version will be include, and for duplicate publication of the same study only the most complete and newest one will be included

### Data Extraction

In this study we will process research based on the characteristics of an object or called property, property is used to describe attributes related to a data structure. Property (or also called attribute) is data contained in a class it can be seen in table 4 below.

Table 4. Research Questions

Property	Research Question
Research and Publication	RQ1, RQ2 and RQ3
Research trends and topics	RQ4, RQ5 and RQ6
Wireless handoff process	RQ7
Wireless handoff authentication the middle metrics	RQ8 and RQ9

### Study Quality Assessment and Data Analysis

The study quality assessment and Data Synthesis in the of the synthesis finding and to define the strength of the elaborate inferences the goal of data synthesis is to aggregate evidence from the selected studies for answering the research question. A single piece of evidence might have small evidence force but the aggregation of many of them can make a point stronger [14]. The data extracted in this review include both quantitative data and qualitative data. Different strategies were employed to synthesize the extracted data pertaining to different kinds of research questions. As a Rules the narrative synthesis method was used the data were tabulated in manner consistent with the questions. Some visualization tools including bar charts and tables were also used to enhance the presentation of distribution of wireless handoff authentication in the middle methods, reliability also one of method to examine or observese [15].

## RESULTS AND DISCUSSION

### Significant Journal Publication

In order to carry out activities such as those listed on the scope with the results as expected on the purpose of this activity and accompanied by effective cost utilization, the methodologies for carrying out such activities shall be so designed that all the variables and indicators who are involved in the review are fulfilled, therefore the methodology for carrying out this study is carried out as follows:

Table 5. Result Keyword in Journal

Keyword	Result
Wireless handoff	3274
Wireless handover	3862
Wireless handoff Process	921
Wireless handover Process	984
Wireless handoff attack	25
Wireless handover attack	49
Wireless handoff security authentication	4
Wireless handover security authentication	5

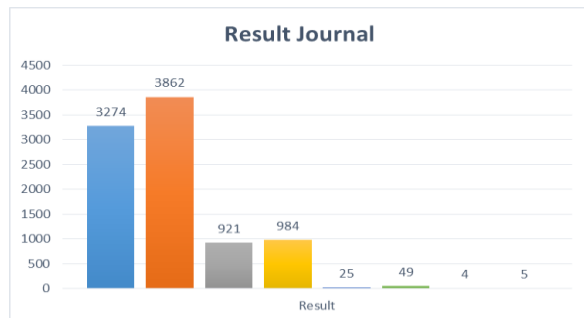


Figure 3. Result Journal by Keyword

**Methods Used in wireless handoff**

Conducting systematic review to know the position of research by doing the use of keywords literature studies on previous studies to obtain the analysis gap.

Table 6. Conducting Journal

Title	Researchers	Discussion
A Secure Certificate Based Authentication to reduce Overhead for Heterogeneous wireless networks	M.Prasad, R. Manoharan, Pondicherry Engineering College, India	Authentication algorithm signed also resists against man-in-the-middle-attack and replay attack
Secure 3GPP-WLAN authentication protocol based on EAP-AKA	"Shruti S. Patkar, Dayanand D. Ambawade, Dept. of Electronics & Telecommunication Sardar Patel Institute of Technology Mumbai, India"	Authentication Protocol using EAP -AKA (Extensible Authentication Protocol) - Authentication and Key Agreement The EAP-AKA protocol was developed by 3GPP
Secure handover in WSN using FLAP	"Manpreet Kaur, Simarpreet Kaur, Kamaljit Singh Saini, Dept. of Comp. Sci. and Engg. Chandigarh University Mohali, India"	Authentication protocol using FLAP (Frame Layer Protocol)

Secure and efficient uniform handover scheme for LTE-A networks

Zaher Haddad, Mohamed Mahmoud, Imane Aly Saroit, and Sanaa Taha, Al-Aqsa University, Gaza, Palestine Tennessee Tech University, USA University, Cairo, Egypt"

LTEA Long Term Evolution-Advance scheme and use Home Subscriber Server (HSS)

Reliability Analysis of Wireless 802.11 Networks with Reliability Block Diagram

Sigit Wibawa Mudrik Alaydrus Department of Electrical Engineering Universitas Mercu Buana Jakarta, Indonesia

Security holes in wireless technology were found in the management framework process handoff specifically when devices were first interconnected

**CONCLUSION AND FUTURE WORK**

This article is expected to make it easier to discovery the best wireless network, because we can also mapping the coverage of wireless networks by knowing the value of system reliability for components with series configurations written the value of success is successful on the system while for parallel components the value of failure is written on the system, In the future, our suggestions and proposals are to prepare wireless devices in this case study, Security Analysis of Handoff Process with Why we need security on handoff process allows users to use alternative passwords such as fingerprints, retina identifiers, face recognition and voice recognition to authenticate so that users no longer need to remember passwords to enter the system and are relatively more resistant to phishing because it is not easy to duplicate.

**REFERENCES**

- [1] M. Prasad, R. Manoharan, "A Secure Certificate Based Authentication to Reduce Overhead for Heterogeneous Wireless Network," International Conference on Advanced Computing and Communication Systems (ICACCS) 2017.
- [2] Shruti S. Patkar, Dayanand D. Ambawade "Secure 3GPP-WLAN Authentication Protocol Based on EAP-AKA," IEEE International Advance Computing Conference (IACC) 2015.
- [3] Manpreet Kaur, Kamaljit Singh Saini, "Secure Handover in WSN using FLAP," IEEE 2<sup>nd</sup> International Conference on Next Generation Computing Technologies (NGCT) 2016.

- [4] Olabisi E. Falowo, Olugbenga Taiwo "Consensus-Based Algorithm for Making Network Selection Decisions in Heterogeneous Wireless Networks," IEEE 26<sup>th</sup> International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): Mobile and Wireless Networks 2015.
- [5] Amit Kumar, Hari Om L. Stein, "A Secure Seamless Handover Authentication Technique for Wireless LAN," IEEE International Conference on Information Technology 2015.
- [6] Piotr Pacyna, Rafał Chrab aszcz, "Evaluation of EAP Re-authentication Protocol," 17<sup>th</sup> International telecommunications networks strategy and planning symposium (Networks) 2016
- [7] Nandi Zhang, Marvin A. Sirbu, Jon M. Peha, "A Comparison of Migration and Multihoming Support in IPv6 and XIA," International symposium on networks computer and communications (ISNCC) 2017.
- [8] Alican Ozhelvaci, Maode Ma, "Secure and Efficient Vertical Handover Authentication for 5G HetNets," IEEE International Conference on Information Communication and Signal Processing (ICSP) 2018.
- [9] Naif Alamri, C. Edward Chow, Amer Aljaedi, Abdelhamid Elgzil, "UFAP: Ultra-Fast Handoff Authentication Protocol for Wireless Mesh Networks," IFIF Wireless Day 2018.
- [10] Alisson Puska, Michele Nogueira, Aldri Santos, "Confidentiality-Aware Decision on Handoffs under Uncertainty on Heterogeneous Wireless Networks," IEEE Symposium on Computers and Communications (ISCC) 2018.
- [11] Jianjun Jiang, Shilian Zheng "Joint Delay and Maintenance Optimization for Spectrum Handoff in Cognitive Radio Networks Using Binary Shuffled Frog Leaping Algorithm, IEEE 19<sup>th</sup> International Conference on Communication Technology 2019
- [12] Sigit Wibawa, Mudrik Alaydrus "Reliability Analysis of Wireless 802.11 Networks with Reliability Block Diagram" IEEE International Conference on Informatics and Computing (ICIC), 2019.
- [13] Wen Qiang, Li Jiying, Yang Yonghong, Li Ya "The Research of LTE-R handoff algorithm based on fuzzy Prediction," 11<sup>th</sup> International Conference on Measuring Technology and Mechtronics Automation (ICMTMA) 2019.
- [14] Xinhang Ding, Zhilong Zhang, and Danpu Liu, "Low-delay Secure Handover for Space-air-ground Integrated Networks," IEEE 31<sup>st</sup> Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 2020.
- [15] T. Hidayat and R. Mahardiko, "A Review of Detection of Pest Problem in Rice Farming by using Blockchain and IoT Technologies," J. Comput. Networks, Archit. High-Performance Comput., vol. 3, no. 1, pp. 89–96, Mar. 2021.