International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2018/49434 Volume 5, Issue 3, May – June (2018)

REVIEW ARTICLE

Secure and Fast Handovers Authentication Methods for Wi-Fi Based Networks: A Review Perspective

Tahadray Jean Tsitaitse
College of Computer Science and Technology, Beijing University of Technology, Beijing, China.
fahasoavajean@hotmail.com

Yongquan Cai
College of Computer Science and Technology, Beijing University of Technology, Beijing, China.
cyq@bjut.edu.cn

Shaldon Leparan Suntu
School of Computer and Communication Engineering, University of Science and Technology Beijing, China.
suntusha@yahoo.com

Muhammad Nafees Ulfat khan
School of Computer and Communication Engineering, University of Science and Technology Beijing, China.
engr_nafees@yahoo.com

Published online: 30 June 2018

Abstract – Regarding to this study, an extensive review of secure and fast handovers schemes were studied with the aim of solving security problems and authentication server computational overhead experienced in the existing schemes in wireless fidelity based networks. The complete verification scheme outlined in IEEE 802.11i network is unsuitable to be deployed so as to support the user's seamless mobility. The contribution of this paper suggested a robust delivery of handoff keys for internetworking and intranetworking schemes with a dedicated trust relationship model existing in diverse domains. Inter-access point protocol was used to transfer handover credentials in an intra-domain network. Likewise, an inter-access control-tunnelling protocol with opportunity key caching and pairwise master key caching are suggested for inter-domain security context-transfers. Man-in-the-middle attacks are tasked to break mutual authentication for wireless networks. This paper pinpoints out that the suggested fast handover authentication scheme in our study outperforms the scheme of Wang and Prasad and other schemes mentioned in the extant studies. The proposed authentication scheme prevents replay attacks, masquerading and message modification.

Index Terms – Delay, Handover, Handoff Latency, Fast Handoff, Mutual Authentication, Horizontal Handoff, Seamless User Experience.

1. INTRODUCTION

Wireless communication is the prime method of sharing information in the digital world of today [1]. The availability of handheld devices with network interface cards upsurges the use of wireless technology to interchange information through the air. Due to the flexibility of wireless communication, users need to transverse across various intranet and extranet and wish to have a continuous network connectivity [2]. Due to this, researchers continue to invent possible solutions to meet the users' demand. This can only be achieved via seamlessly user experience across multiple domains with diverse network policies as well as authentication schemes [3]. Seamless handover across networks is the de facto salient feature in Wi-Fi to support voice calls and video streaming to users roaming along these networks [4]. Largely, seamless handoff mobility between inter-domains relies on the authentication delay. Therefore, authentication is the primary step for the security of a wireless network designed to support roaming capabilities [5]. IEEE 802.1X [6] is vital authentication mechanisms for managing users' credentials in a network. The foremost role of Extensible Authentication Protocol (EAP) is to encapsulate the classified data used for the authentication [7]. EAP customarily operate between the supplicant and the authentication server, probably via a front-end authenticator [8]. The information shared by parties should not be visible to the charlatans. Internet service providers are not in a position to place several access points to increase the coverage area. In this case, the seamless user experience is required to enable the users to get good connectivity while traversing across intra-networking or internetworking domains. Security of handovers between internetworks or intra-networks needs to be considered while designing the wireless infrastructure due to its broadcasting nature that creates a space for hackers to intercept information and decrypt the session secret keys.

Particularly, wireless roaming takes place in layer 2 and layer 3. Layer 2 (L2) is a kind of IEEE 802.11 roaming where the supplicant roam out of old access point (oAP) proximity and associates with the targeted neighbour AP but both of them are in the same intranetworking [9]. It involves the transfer of connectivity of the physical layer. During the handover of the session from oAP to the target AP (tAP), there is a period of the supplicant stopping traffic passage via the oAP. This period is referred to as handover latency or delay. On the other hand, layer 3 (L3) occurs when a supplicant changes its association from oAP to the tAP in different ESS. In this type of roaming, there is a change in IP addresses between the old and the target routers.

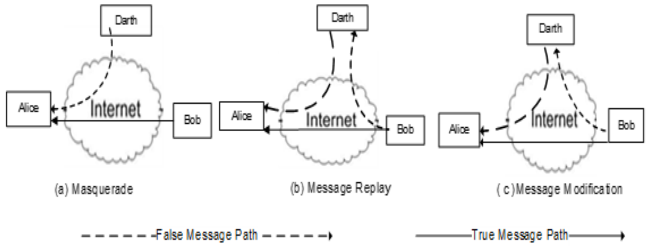
In this study, a review of fast handovers between inter-domain and intra-domain seamless handovers are extensively studied while considering the security of information sharing between their ranges. In the end, a further minimization of delay latency to the existing handover scheme is provided for both internetworking and intranetworking [10].

This study follows the following structure: section 2 Main threats against authentication mechanism, section 3 Review of authentication mechanism, section 4 Handoff techniques in WLAN, section 5 Contribution of the study, section 6 Recommendations and section 7 is the Conclusion of the study.

2. MAIN THREATS AGAINST AUTHENTICATION MECHANISM

Security in a wireless network is a challenging factor [11]. Attacks caused as a result of the man in the middle (MiTM) attack requires that both the user and the device are mutually authenticated to each other in IEEE 802.11i based networks [12]. MITM is an attacker who manages to inject himself between the guest tunnelling gateway and the mobility gateway access and impersonates the access mobility gateway to guest tunnelling gateway and vice versa [13], [14].

Categorically, threats intended to defeat mutual authentication includes; masquerading, message replay and message modification [15], [16]. These categories of MiTM are shown in Figure 1. In this scenario, Bob is the sender, Alice is the recipient and Darth is the attacker.



(a) Masquerade (b) Message Replay (c)Message Modification

Figure 1 MiTM Categories of Attacks towards Mutual Authentication

Replay Attack: A hacker passively screens transmission between the endpoints terminals. Then they retransmit the frames to mimic the genuine users. In Figure 1, Darth captures the message from Bob originally meant for Alice, and later replay it to Alice [17–19]. The packets captured by the attacker can be analysed later to decipher its contents.

Message Modification: This includes the erasure, insertion, or adjustment of information in an illegitimate way that is intended to look as if genuine to the user. Even so often, these attacks are stern to detect [19]. In Figure 1, Darth sniffs the channel and captures the message from Bob meant for Alice, perform an alteration on it and send to Alice. For instance, the message “Send 20 US dollars to John” to read send 2000 US dollars to John.

Ideally, MiTM attacks inject themselves between legitimate communications, performs the indented malicious attacks, and retransmit the information to the legitimate user without the sender or receiver cognizance [18].

3. REVIEW OF AUTHENTICATION MECHANISM

Authentication refers to the process through which the user and the device are legitimized before accessing network and its resources. This lead to the development of various secure and fast authentication methods to thwart malicious attacks arising from MiTM acts.

Zhu [20] proposed a flexible and secure authentication scheme to authenticate APs across multiple organizations. The scheme adopted a certificate based standard utilizing x.509 format. The scheme consists of four components: the certificate authority, AP, AS and the users. The APs are connected to the server to authentic users. Both the AS and the user applies for personal certificates from the certificate authority. The scheme utilizes two certificates for multiple authentication within various APs scenario. The users are verified by other APs connected to the AS by using an associate certificate that is verified and validated.

Bargh et al.[21] the authors applied inter-access point protocol [22] and Seamoby to push context information from home AS to the targeted AS to achieve the inter-domain seamless roaming. In addition, trust relationship and roaming agreement must exist between the APs and AS(s) across the inter-domains technology.

Hassan et.al [23] studied a scheme to reduce the handoff delays experience in the course of substantiation process. The nearby share secret keys for the supplicant roaming in between them. The authors applied Markovian trust model labelled that even with the straightforward implementation, the average number of full-authentications required for a roaming client declines linearly as the probability of two neighbouring APs creating

Bhargava and Sichitiu [24] presented an authentication scheme that positively defends attacks rising from the parking lot and detect intruders basing on location. This tactic depends on received strength of the signal from the location. The imposter‘s location can be estimated by deploying a Bayesian model.

Li et al. [25] recommended a style for authenticating multimedia information conveyed over two dissimilar networks and in addition to security trepidations in audio-cum-visual applications. This shield a channel from uneven substantiation interferences.

Roos et al. [26] examined the authentication design of hierarchical, centralized, and distributed and demonstrated that centralized method requires at least an intelligence authentication concept, the path length can be reduced by distribution method and the hierarchical scheme is suitable for puzzling and robust authentication.

Xiao et al. [27] studied a verification method at the lowest layer grounded on channel searching and proposition analysis to establish the in progress and past transmissions tried by an individual. This scheme permits legitimate users to access the internet resources while thwarting illegitimate users.

Yu et al. [28] presented a physical layer authentication mechanism based on tag computation from a message and then computed tag transmits to the Bob along with the information. A shared secret key between Bob and Alice computes a tag, if Bob endorses the message with tag then success message otherwise a failure message occurs.

Capkun et al [29] propose an authentication method basing on the integrity-region to enable protection integrity of information exchange between principals where mutual authentication is not needed. This method prevents MiTM from unscrambling the pre-shared key between principals. Ultrasonic hardware is used to detect MiTM attacks.

Table 1 shows some extant studies conducted by various authors to enhance mutual authentication during the handoff process.

Table 1summary of other existing authentication mechanisms

Author/ Reference	Main Idea	Recommendations
Jing et al.[30]	The author proposed a signature proxy method to authenticate MN and AP while eliminating the third party. Their scheme achieved both forward and backward perfect secrecy.	• Well-organized in terms of overhead transmission and cost computation.
Choi and Jung [31]	The authors proposed a chameleon hashing authentication handover method basing on credentials. The credentials are generated via a collision-resistant hash function between the MN and AP minus the AS whenever handover occurs.	• Provide robust key exchange and effective authentication scheme
Soltwisch et al. [32]	The authors designed a protocol to forward the keys from the serving router to the targeted router in line with the trust relationship between the access routers	• Minimalized message exchange at the wireless link and fast message authentication key exchange
Zhu et al. [33]	The scholars present a secure confined to a small area substantiation and charging standard to address security and performance regarding to system flexibility, internetworking session handoff delay and roaming of broker.	• Achieve secure roaming and billing options in the metropolitan area in wireless mesh network practically in terms of compromised by hackers
Han et al. [34]	This article suggests an improved authentication and key treaty mechanism for Home Node B that acclimates proxy signature and proxy signed signature for mutual verification to prevent an unauthorized access to the network.	• Prevent varied threats and met minimum range from user-tolerable verification delay.
Chang and Tsai [35]	The authors proposed a self-substantiated mobile model with a novel structural design of servers to eliminate the storage of pre-shared keys.	• Elimination of overhead computation since no keys are stored.
Qiu et al. [36]	The scholars apply the proxy-based signature authentication method for the handover long-term evolution networks referred to the as elliptic curve	• Efficient cost reduction scheme and minimalized handover delay.

	discrete logarithm for verification	
He et al. [37]	In this article, the authors pinpoint a Hash-Hand handover authentication method that update session keys regularly to eliminate security vulnerabilities	• More robust regarding to security and low servers' overhead computations
Tang and Wu [38]	The paper proposes an authentication scheme that calls for a solo elliptic-curve crypto on a delegation technique to compute a passcode for a roaming client visiting a foreign network.	• Enjoys both communication and computation efficiency. • It lacks basic security requirement.
Iddris et al. [7]	The authors presented a local authentication method EAP- fast authentication key agreement (FAKA) to simplify the authentication process. They achieved fast authentication scheme by applying EAP-AKA by combining both symmetric and asymmetric algorithms.	• Eliminates MiTM by using one-time-key
Rekik et al [39]	Researchers propose a seamless authentication protocol to secure the mobile stream-control transmission protocol handover. Their scheme deploys security protocol-analyser automated authentication of internet-security protocol and applications tool.	• Transmissions encryption of information between nodes is shielded hence prevent MiTM attacks.
Shrestha et al. [40]	Authors based their notion on designing WLAN access control regardless of the administrative domain. Kerberos authentication protocol was proposed to manage keys and issue tokens for session protection to enhanced roaming for home network and formerly visited network.	• Low latency attained. • Prevention of MiTM attacks

4. HANDOFF TECHNIQUES IN WLAN

Roaming clients can change their point of attachment through handoff process. An MN is attached to one AP at a time. Fast handoff roaming is necessary to support video or voice quality [41]. Frequent handoffs lead to excessive consumption of network bandwidth leading to poor quality of service.

Handoff can be fragmented into vertical and horizontal handoffs [42]. Vertical handoff (inter-network/heterogeneous) is a handoff between different types of networks [43]. At all handover operation is a three-phase process that includes the transfer of radio link, handoff decision and channel allocation [44]. According to Paul [45], handoff management includes three crucial steps; the measurement, decision, and execution.

According to Jain and Tokekar [46], horizontal handoff (intra-network/homogeneous) same subnet APs. Mobility Management has been studied in [47]–[54] regarding to IPv4 and IPv6 to improve management of the roaming users.

Table 2 shows a description of handoff mechanisms in a WLAN environment

Table 2 Summary of existing handoff mechanisms in a WLAN environment

Author/ Reference	**Main Idea**	**Recommendation**
Zekri et al. [55]	The authors proposed an intelligent context-aware solution to cater for both users and services constraint basing on a progressive decision mechanism such as fuzzy and analytic hierarchy procedures.	High user's consideration and flexibility
Choi et al. [56]	In this article, the authors propose handoff mechanisms that deliver seamless mobility. Pre-registration and pre-authentication take place prior to L2 handoff. This mechanism uses pre-registration to achieve low latency.	Offers low latency and packet loss reduction

Yan et al. [57]	The authors design an old-dual thresh handover method studied by the author of [58] to stipulate a vertical based authentication method.	Provide a shorten latency period
Yang et al. [59]	The authors proposed a handover scheme to provide user concealment and un-traceability	Accomplishes outstanding features of security and efficacy
Cao et al. [60]	Cao et al. proposed an artless robust and secure handoff model to fit in the entire mobility domain in long-term evolution networks. The model affords sturdy perfect forward secrecy and user concealment.	- Secure against several malicious attacks - Provide robust efficiency regarding communication cost and computational cost
He et al. [61]	He et al proposed PairHand which deploys pairing based cryptography to safeguard handover procedure. This scheme incorporates a batch-signature authentication scheme.	- Attains high efficacy and also practicable in real applications

5. CONTRIBUTION OF THE STUDY

In this section, a novel handover fast hash authentication scheme (FHAS) design to solve the problem of handover latency arising during the mobility between intra-domain and inter-domain roaming in the homogeneous environment; particularly IEEE802.11 based networks (Wi-Fi-based networks). Homogeneous mobility handoff mechanism has been extensively surveyed in [44]. The standard network layer solution, MIP is simple to administer but has several issues, such as triangular routing, high global signalling load, and high handoff latency [62].

RSNA has been defined by 802.11i and it contains six phases to include (phase 1) network and security ability discovery, (phase 2) association and authentication of 802.11, (phase 3) EAP/RADIUS/802.1X authentication, (phase 4) The 4-way handshake, (phase 5) the group key handshake and (phase 6) protected communication for the client to associate to the network. The first five phases cause a long delay time that leads to severe loss of packets, thus causing unstable network connection which does not support video or voice calls.

$$Handoff\ Latency = Phase1 + Phase2 + Phase3 + Phase4 + Phase5 \quad (1)$$

Basing on equation (1), some of the phases need to be skipped in order to minimize the handoff latency. The authors in reference [63]–[65] has proposed handoff latency authentication schemes but still, their schemes have some problems in computational overhead or security concerns as describe below.

Mishra et al. [63] propose a scheme that performs authentication one step ahead of a roaming client to minimize latency. This method is well organized in delay reduction but it burdens the administrative by causing computational overhead during the pairwise master key (PMK) generation. Similarly, no proof of robust re-authentication from the client or AP is shown in this model in case AS mislays traces of the supplicant due to interference since the AS is mandated to trigger authentication process.

Wang and Prasad [64]proposed a scheme for authentication using an exchange of arbitrary number between the supplicant and the AP. The oAP sends an exclusive OR secret key concatenated with an indiscriminate number to a client and a target-AP. Then the two nodes exchange nonces and compute a novel PMK from nonces and key components acknowledged from the oAP. In this scheme, communication is simple since no AS is required after full authentication. Security problems arise if an imposter obtained an exclusive-OR secret key from a rogue AP[66]. Likewise, the imposter can get clear-text of nonces which aid in the computation of new PMK.

Patrick and Choi [65] suggested a predictive frequent handoff region (FHR) selective authentication method. This scheme looks for FHR comprising a set of neighbouring AP basing on the movement pattern of client and the APs sites using multiple to all APs using substantiation information of a secret-key. This model fails in consecutive handoff and the pre-shared key can be revealed if a compromised AP is installed along with the legitimate APs.

This paper considers researches by Mishra et al, Wang and Prasad and Patrick and Choi work and solves the existing problems shown in their studies concerning security problems and computation overheads of AS.

5.1. Intranetworking Roaming

The 802.11i protocol, the AP requires the supplicant to undergo authentication using the local AS to access the network by performing the preliminary full verification with the AP and the AS. This will allow the supplicant and the AP to compute a common origin and compute PMK_0 meant for safeguarding the channel between the supplicant and the oAP as follows:-

$$\mathrm{PMK_0} = \mathrm{PRF}(\mathrm{PMK_{PRIMARY}}\ |\mathrm{AP_{MAC}}\ |\ \mathrm{SUPPLICANT_{MAC}}) \quad (2)$$

In authenticating the device, $\mathrm{PMK_0}$ is computed from the primary PMK, the AP_{MAC} and the $\mathrm{SUPPLICANT_{MAC}}$using the pseudo-random function (PRF). Primary authentication-key (PAK) is collectively communal between the AS and the supplicant without the knowledge of the AP.

Similarly, the oAP and tAPs conducts the pre-verification process for decreasing authentication latency time during the handoff of the supplicant before the supplicant roams to one of the tAPs. The oAP transfers the hand-over key (HoKi) to the tAPs using inter-access point protocol (IAPP). The oAP using the formula (5) performs a HoKi for each tAP as follows:-

$$\mathrm{HoKi} = \mathrm{PRF}(PMK_{i-1}\ |\mathrm{tAP_{MAC}}|\mathrm{SUPLICANT_{MAC}}) \quad (3)$$

$\mathrm{HoK_i}$ implies the order of handoff of the session of the supplicant from 1 to n in contradiction of each handoff of it. HoKi offers mutual authentication at MAC layer by means of $\mathrm{AP's_{MAC}}$ and $\mathrm{SUPPLICANT's_{MAC}}$ addresses to supports a faultless forward perfect secrecy to the oAP by means of PRF since tAPs or it is hard for the imposter to calculate the contemporary PMK between the oAP and Supplicant from the HoKi. Figure 2 is the oAP distribution of the HoKi to each of the tAPs in a one-hop adjacent ring comprising of tAPs in one-hop distance from the oAP. The supplicant served by the oAP can roam to the only one tAP in the one-hop adjacent ring. T is the group of the tAPs:-

$$\mathrm{T} = \{\mathrm{tAP_{\_1}}, \mathrm{tAP_{\_2}}, \mathrm{tAP_{\_3}}, \mathrm{tAP_{\_4}}, \mathrm{t\,AP_5}, \mathrm{tAP\_6}, \mathrm{tAP\_7}, \mathrm{tAP\_8}\}$$

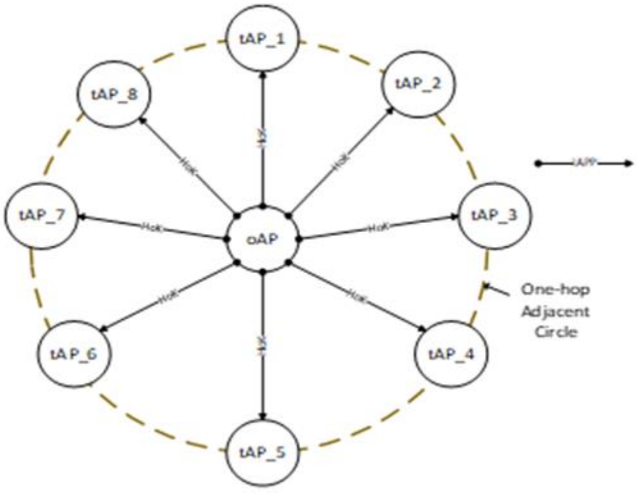


Figure 2 Distribution of handover Secret-Keys

Fast handoff context delivers service between APs is performed by IAPP. IAPP information exchanged is deemed secured when a robust trust relationship between APs and include $\mathrm{SUPPLICANT_{ID}}$, $\mathrm{SENDER_{ID}}$, and security framework holding the handover key, an index of authentication key (AK) information, and cryptosystem procedures for scrambling the data and substantiation information code used in the oAP.

When the oAP completes the handoff, the AS transmit a new AK to the tAPs so that each AP may compute PMK as the comprehensive AK. Nevertheless, for a seclusion of the AK in advance and prior to the handover process, the AS must work out a substitute of series PAK to be shared for the complete preliminary authentication process. PAK subkey generation entails two techniques as preferred in this study. The foremost model is deployed for immediate calculation of the supplicant's handover AK. $\mathrm{PAK_0}'s$ value is similar to the PAK, as portrayed in Figure 2. N and N_i are twofold dissimilar PRF. $\mathrm{AK_{INDEX}}$ means the series of the handover of the supplicant and AS consecutively utilizes the similar index from 1 to n in contradiction of each conferal of it.

The other model is utilized in the pre-computation of a series of AK, and the series key as presented in Figure 3 will be put in storage by the supplicant as well as the AS. The aforementioned pre-computation is just after the execution of the full substantiation initially conducted. In this model, $\mathrm{PAK_n}$ is the same value with PAK as represented in Figure 3 After the full authentication process, the supplicant and the AS independently generate the hash-key series from $\mathrm{PAK_n}$ and $\mathrm{AK_1}$ on either side. The AS uses $\mathrm{AK_1}$ as AK for the initial handover of the supplicant and transmits it to the tAPs. This second technique burdens the AS computational overhead during the initial full verification mechanism. The first method is ideal to be used to enhance fast handoff.

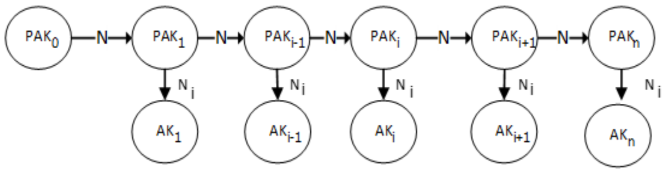


Figure 3 Instantaneous Calculation of the Supplicant's handover AK

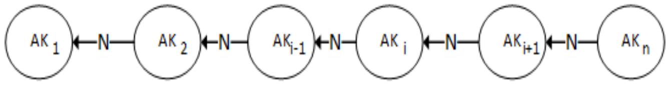


Figure 4 Pre-computation of AK Series

oAPs → AS: After swapping the messages of IAPP, the tAP which receives the context security, directly requests the AK to the AS using the request message of the AK with oAP_{ID}, its ID and $AK_{\ i}$ data as displayed in Figure 5.

AS → tAPs: In the meantime, the AS by now has the PAK pre-shared key with the supplicant in the preliminary full substantiation process, after generating the $\mathrm{AK_i}$, AS just sends the response message of AK with $\mathrm{AK_i}$, to the tAP.

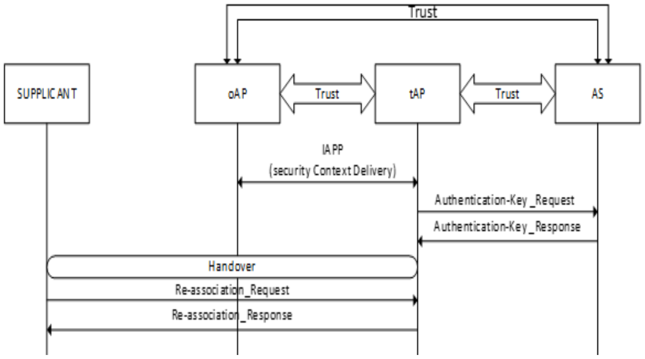


Figure 5 Pre-authentication Trust model for the intra-domain

In the circumstance of AK pre-computation mechanism, the $\mathrm{AK_i}$ is send by AS to the storage. The form of AK rests on AK computation mechanism aforementioned previously. In this procedure, the AS is responsible for transferring$\mathrm{AK_i}$, to the adjacent APs except for the oAP, since the oAP may generate new PMK between the supplicant and the tAP in case it has handover key and $\mathrm{AK_i}$. The supplicant plays a crucial title role of transmitting the information of the oAP. After swapping AK messages, each adjacent AP finally computes $\mathrm{PMK_i}$ for the supplicant and itself by means of the $\mathrm{HoK_i}$ and $\mathrm{AK_i}$ with PRF as pointed out in equation (4):

$$\mathrm{PMK_i} = \mathrm{PRF}(\mathrm{HoK_i}\ |\mathrm{AK_i}) \quad (4)$$

The complete circle of the APs store the key for sometimes and if the handoff does not take place, the keys are dropped by the APs. When the supplicant roams to the tAP and computes $\mathrm{PMK_i}$.

The supplicant moves to any of the tAP after pre-authentication and performs the four-way handclasp with the tAP after the re-association to validate the legitimacy of the supplicant's and AP's key information. This is necessary to test the credibility of the handover process. Utilizing the exchange of the $\mathrm{AK_i}$ information in this manner, the supplicant and AS endorse the harmonization of the subkeys of the PMK and AK. If the supplicant roams swiftly to the tAP prior to the arrival of the HoK via IAPP or connects up to the tAP that is not next to oAP due to connectivity issues, it will not connect to the tAP. In this case, the new AP receives the re-association and computes it key as follows:-

$$\mathrm{PMK_i} = \mathrm{PRF}(\mathrm{AK_i}|\mathrm{AP_{MAC}}|\mathrm{SUPPLICANT_{MAC}}) \quad (7)$$

Nevertheless, since the supplicant is not aware to the AP's state of affairs, AP can inform parameters of PMK generation to the supplicant using a four-way handclasp as stated beforehand. The cryptographic suite between the AP and supplicant can be also attained via the four-way handshake.

5.2. Internetworking Roaming

IEEE 802.11i defined that supplicant must obtain a new IP address if it enters into a different subnet. This implies that the 802.11i initial full authentication process should be required whenever a supplicant enters into another domain. This will cause unnecessary rekeying of credentials from time to time. This causes high handoff latency and rapid loss of packets thus sensitive high latency applications are dropped.

To overcome this problem, a vendor based opportunistic key caching is required between the internetworking networks to force the key materials to the tAP in the new domain through the Inter-AC tunnelling protocol (IACTP) as depicted in Figure 6. This enables the supplicant to wander through an area of multiple inter-domain networks without changing the IP address thus reducing latency to support video and voice calls.

However, the keys are harmonized by the current AC1 to the other available ACs in the mobility administrative group via the central distribution centre. If the client wanders across the mobility administrative group, the targeted AC utilizes the stowed client's info to validate the supplicant while omitting the 802.1X authentication method and conducts the 4-way handclasp to validate the process. This lowers the handoff latency between the inter-domain handovers.

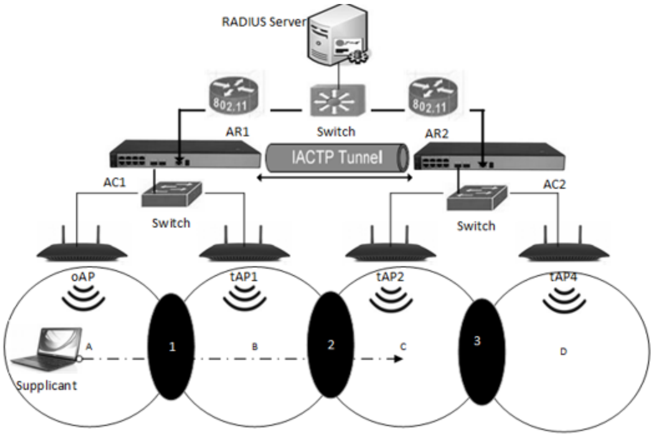


Figure 6 IAPP and IACTP Handover Scheme Using OKC and PMK Caching

In Figure 6, the supplicant goes into the area coverage of oAP marked *A* and an initial 802.1x authentication scheme is executed. When the user's device makes a displacement towards tAP1 and first enters into the area marked *B* it first enters into the brick plane area labelled. In this plane, a handoff is mandatory, basing on the signal threshold of tAP1 and all the protected information are transmitted to tAP1 minus the glitch of the client's awareness [67], [68] using IAPP or context transfer protocol.

When the supplicant roams from tAP1 to tAP2, the supplicant must perform another full authentication according to IEEE 802.11i. However, in this study, IACTP is utilized to exchange information between two distinct domains so long as the trust model exists between the two-internet service providers AR1 and AR2.

In Figure 8, the AS preferable the RADIUS server was introduced to the network in order to create a trust relationship in the middle of the interlinked network components. Neighbouring network APs were linked via security slab to enable them to interchange the info by being aware of the policy agreement of the internetworking agreement policy as displayed in Figure 7. In this case, twofold significant issues ought to be considered:-

(i) The supplicant is aware of the AS and the oAP to which it is associated with,

(ii) The supplicant mistrusts all tAPs in which verification did not take place [69].

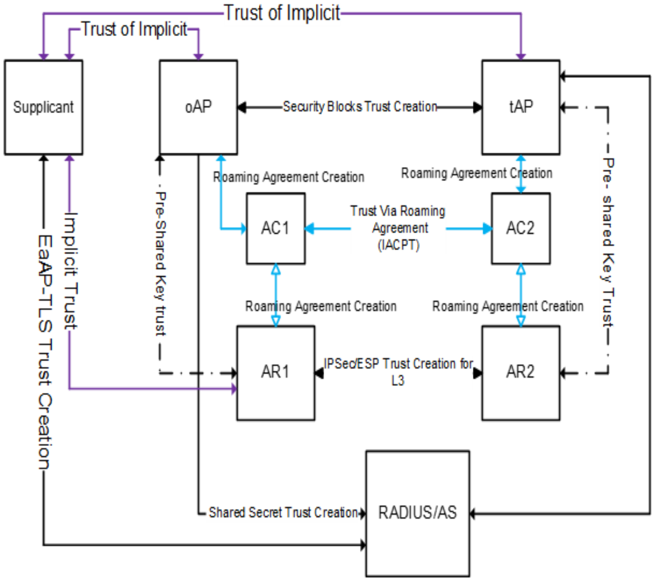

Trust of Implicit
Trust of Implicit
Supplicant
oAP
Security Blocks Trust Creation
tAP
Roaming Agreement Creation
Roaming Agreement Creation
AC1
Trust Via Roaming Agreement (IACPT)
AC2
Roaming Agreement Creation
Roaming Agreement Creation
AR1
IPSec/ESP Trust Creation for L3
AR2
Implicit Trust
EaAP-TLS Trust Creation
Pre-Shared Key trust
Pre- shared Key Trust
Shared Secret Trust Creation
RADIUS/AS

Figure 7 Inter-Domain Trust Relationship Model for Multiple APs Scenario

5.3. Security Analysis

The primary objective of the fast handover authentication scheme (FHAS) is to enhance the robust security. FHAS bolsters the feebleness of the security context from the oAP using authentication key. Since oAP stills hold the pre-shared computed key materials after handoff of the supplicant, the secure context-transfers method is attained by IAPP. Wang's method utilizes arbitrary number also suffers from a security problem. When the supplicant moves from one inter-domain to the other the security context-transfer is done via IACTP which provide a secure tunnel for the exchange of credentials materials. FHAS delivers the authentication key of the AS into security context-transfer method and answers the security concerns of the available schemes. Ordinarily, APs are installed in public domain and the imposters can decipher the secret in the memory. FHAS provides seamless forward confidentiality using AS. If the imposter decodes the current PMK used between the supplicant and the oAP, he cannot be able to compute a novel PMK without having an authentication key from the home AS since the home AS only transfers authenticating key to APs bearing a trusted relation with him distant to oAP. FHAS supports backward confidentiality using PRF and the PMK caching while forward confidentiality to the inter-domain is done by the OKC. In case the imposter gets HoK and authentication key of the tAP, he cannot compute the already used PMK from HoK as per the cryptanalytic personality of the PRF. The imposter is unable to generate $\mathrm{AK}_{\mathrm{i}-1}$ or $\mathrm{AK}_{\mathrm{i}+1}$ from AK_{i}, because each i index of AK was sequestered by N_i. Since credentials are transferred in a wired distribution architecture, it is not possible for the imposter to eavesdrop the packets for him to perform an attack.

6. RECOMMENDATION

To ensure proper security of fast handover schemes, an intrusion detection prevention scheme (IDPS) for Wi-Fi devices should be designed to meet users' seamless mobility without rampant attacks emanating from a MitM. IDPS should be able to perform the following duties:

1. Prevention of unauthorized access
   - Monitoring phase of authentication
   - Detection of unauthorized device
   - Device removal from the network
2. Malicious attack and Intrusion detection
   - Detection of attack
   - Source tracking and detection of the imposters
   - Recovery of the network after the attack
3. Rogue AP detection
   - Rogue AP identification in the network coverage area.
   - Provide an alert information to users
   - Remove the rogue AP from the network zone.

Figure 8 is a representation of the recommended security monitoring system for the Wi-Fi network and its devices emanating from the points highlighted above.

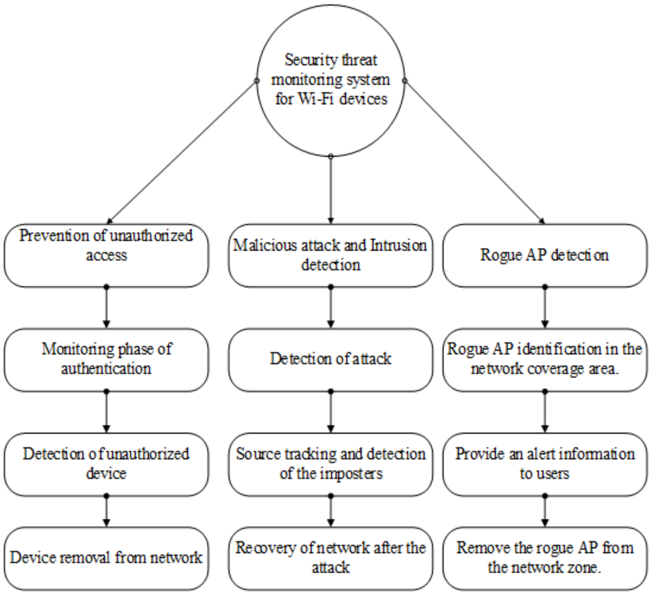

Security threat monitoring system for Wi-Fi devices
Prevention of unauthorized access
Malicious attack and Intrusion detection
Rogue AP detection
Monitoring phase of authentication
Detection of attack
Rogue AP identification in the network coverage area.
Detection of unauthorized device
Source tracking and detection of the imposters
Provide an alert information to users
Device removal from network
Recovery of network after the attack
Remove the rogue AP from the network zone.

Figure 8 Security Threat Monitoring System for Wi-Fi Devices

7. CONCLUSION

In this study, FHAS tunnel based methods for fast and secure handover in Wi-Fi has been proposed to moderate delay for intranetworking and internetworking. In intranetworking, the IAPP context transfer technique was used to securely transfer credentials to the target AP. On the other hand, IACTP has been deployed with OKC and PMK Caching to achieve the transfer of credentials from one domain to the other domain. This method enables the inter-domain networks to create a trust relationship with each other thus avoiding frequent pre-authentication processes. This study introduces the concept of chain hashing of keys to lessen the computational overhead of the AS. This scheme is suitable for both inter-domain and intra-domain mechanisms by creating a model of trust between the network components. This method can be protracted to support heterogeneous for fast handovers of mobile users.

REFERENCES

[1] M. Shi, X. (Sherman) Shen, J. W. Mark, D. Zhao, and Y. Jiang, “User authentication and undeniable billing support for agent-based roaming service in WLAN/cellular integrated mobile networks,” *Comput. Networks*, vol. 52, no. 9, pp. 1693–1702, 2008.

[2] J. J. Baek, J. S. Song, and S. H. Seo, “Multiple preauthentication schemes based on fast channel switching in public wireless LANs,” *2009 Int. Conf. Innov. Inf. Technol. IIT ’09*, pp. 16–20, 2009.

[3] Y. W. Lee and H. Lee, “Evaluation of authentication Interworking methods among multiple WLAN service Providers,” *Int. J. Commun. Syst.*, pp. 515–531, 2007.

[4] M. Long, C. H. J. Wu, and J. D. Irwin, “Reducing communication overhead for wireless roaming authentication: Methods and performance evaluation,” *Int. J. Netw. Secur.*, vol. 6, no. 3, pp. 331–341, 2008.

[5] Z. Zhang, R. W. Pazzi, and A. Boukerche, “Design and evaluation of a fast authentication scheme for WiFi-based wireless networks,” *2010 IEEE Int. Symp. “A World Wireless, Mob. Multimed. Networks,”* pp. 1–6, 2010.

[6] H. Hyunuk, J. Gyeok, S. Kiwook, and P. Sangseo, “A study on MITM(Man in the Middle) vulnerability in wireless network using 802.1X and EAP,” *Proc. Int. Conf. Inf. Sci. Secur. ICISS 2008*, pp. 164–170, 2007.

[7] Y. Idrissi, N. Zahid, and M. Jedra, “Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA,” *…Technology (FGCT), 2012 …*, pp. 137–142, 2012.

[8] N. Asokan, V. Niemi, and K. Nyberg, “Man-in-the-Middle in Tunneled Authentication Protocols,” *IETF Draft. Tunneled Authentication Protoc.*, pp. 1–15, 2002.

[9] Y. Lee, “VOIP Handoff Method Complemented With 802.11 BSS Network Table to Effectively Reduce the Handoff Delay on 802.11 Networks,” *IEEE Access*, pp. 1–5, 2006.

[10] O. Alfandi, H. Brosenne, C. Werner, and D. Hogrefe, “Fast re-authentication for inter-domain handover using context transfer,” *2008 Int. Conf. Inf. Networking, ICOIN*, pp. 1–5, 2008.

[11] S. Kanawat and P. Parihar, “Attacks in Wireless Networks,” *… Smart Sensors Ad hoc Networks (…*, no. 1, pp. 113–116, 2011.

[12] Z. Chen, S. Guo, K. Zheng, and H. Li, “Research on man-in-the-middle denial of service attack in SIP VoIP,” *Proc. - Int. Conf. Networks Secur. Wirel. Commun. Trust. Comput. NSWCTC 2009*, vol. 2, pp. 263–266, 2009.

[13] H. Sun, J. Song, and Z. Chen, “Survey of Authentication in Mobile IPv6 Network,” *IEEE Commun. Soc. IEEE CCNC 2010 Proc.*, pp. 10–13, 2010.

[14] M. Conti, S. Member, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Commun. Surv. TUTORIALS, VOL. 18, NO. 3, THIRD Quart. 2016*, vol. 18, no. 3, pp. 2027–2051, 2016.

[15] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Commun. Surv. TUTORIALS*, pp. 1–26, 2016.

[16] K. Park, Y. Park, Y. Park, and A. G. Reddy, “Provably Secure and Efficient Authentication Protocol for Roaming Service in Global Mobility Networks,” *IEEE Access*, vol. 5, pp. 25110–25125, 2017.

[17] P. Singh, M. Mishra, and P. N. Barwal, “Analysis of Security Issues and Their Solutions In Wireless LAN,” *Inf. Commun. Embed. Syst. (ICICES), 2014 Int. Conf. (pp. 1-6). IEEE*, no. 978, pp. 1–6, 2014.

[18] M. Ordean and M. Giurgiu, “Towards securing client-server connections against man-in-the-middle attacks,” *2012 10th Int. Symp. Electron. Telecommun. ISETC 2012 - Conf. Proc.*, pp. 127–130, 2012.

[19] M. M. Khan, M. Bakhtiari, and S. Bakhtiari, “An HTTPS approach to resist man in the middle attack in secure SMS using ECC and RSA,” *Int. Conf. Intell. Syst. Des. Appl. ISDA*, pp. 115–120, 2014.

[20] W. Zhu, “A Secure and Flexible WLAN Authentication Scheme for Organizations,” *2015 2nd Int. Conf. Inf. Sci. Secur.*, pp. 1–4, 2015.

[21] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, and P. Schoo, “Fast authentication methods for handovers between IEEE 802.11 wireless LANs,” *Proc. 2nd ACM Int. Work. Wirel. Mob. Appl. Serv. WLAN hotspots - WMASH ’04*, pp. 51–60, 2004.

[22] C. T. Chou and K. G. Shin, “An enhanced inter-access point protocol for uniform intra and intersubnet handoffs,” *IEEE Trans. Mob. Comput.*, vol. 4, no. 4, pp. 321–334, 2005.

[23] J. Hassan, H. Sirisena, and B. Landfeldt, “Trust-Based Fast Authentication for Mobile IPv6 Networks,” *IEEE Trans. Mob. Comput.*, vol. 7, no. 2, pp. 1–5, 2008.

[24] V. Bhargava and M. L. Sichitiu, “Physical Authentication through Localization in Wireless Local Area Networks,” *IEEEGlobecom*, pp. 1–5, 2005.

[25] Z. Li, Q. Sun, Y. Lian, and C. W. Chen, “Joint source-channel-authentication resource allocation and unequal authenticity protection for multimedia over wireless networks,” *IEEE Trans. Multimed.*, vol. 9, no. 4, pp. 837–850, 2007.

[26] A. Roos, S. Wieland, A. T. Schwarzbacher, and B. Xu, “Time

behaviour and network encumbrance due to authentication in wireless mesh access networks," *IEEE Veh. Technol. Conf.*, pp. 1219–1223, 2007.

[27] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," *IEEE Int. Conf. Commun.*, pp. 4646–4651, 2007.

[28] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-Layer Authentication," *IEEE Trans. Inf. Foresics Secur.*, vol. 3, no. 1, pp. 38–51, 2008.

[29] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," *IEEE Trans. Mob. Comput.*, vol. 9, no. 11, pp. 1608–1621, 2010.

[30] Q. Jing, Y. Zhang, A. Fu, and X. Liu, "A privacy preserving handover authentication scheme for EAP-based wireless networks," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 1–6, 2011.

[31] J. Choi and S. Jung, "A handover authentication scheme using credentials based on chameleon hashing," *IEEE Commun. Lett.*, vol. 14, no. 1, pp. 54–56, 2010.

[32] R. Soltwisch, X. Fu, D. Hogrefel, and S. Narayanan, "A Method for Authentication and Key Exchange for Seamless Inter-Domain Handovers," *IEEE Panasonic Technol.*, no. 2, pp. 463–469, 2004.

[33] H. Zhu, X. Lin, R. Lu, P. H. Ho, and X. S. Shen, "SLAB: A secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 10, pp. 3858–3868, 2008.

[34] C. K. Han, H. K. Choi, and I. H. Kim, "Building femtocell more secure with improved proxy signature," *GLOBECOM - IEEE Glob. Telecommun. Conf.*, pp. 1–6, 2009.

[35] C. Chang and H. Tsai, "Transactions Papers An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 11, pp. 3346–3353, 2010.

[36] Y. Qiu, M. Ma, and X. Wang, "A proxy signature-based handover authentication scheme for LTE wireless networks," *J. Netw. Comput. Appl.*, vol. 83, no. February 2015, pp. 63–71, 2017.

[37] D. He, S. Chan, and M. Guizani, "Handover authentication for mobile networks: security and efficiency aspects," *IEEE Netw.*, vol. 29, no. 3, pp. 96–103, 2015.

[38] C. Tang and D. O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 4, pp. 1408–1416, 2008.

[39] M. Rekik, A. Meddeb-Makhlouf, F. Zarai, and M. S. Obaidat, "A MSCTP-Based Authentication Protocol: MSCTPAP," *2015 IEEE Int. Conf. Data Sci. Data Intensive Syst.*, pp. 617–623, 2015.

[40] A. P. Shrestha, D. Y. Choi, G. R. Kwon, and S. J. Han, "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network," *Comput. Math. with Appl.*, vol. 60, no. 2, pp. 245–255, 2010.

[41] H. Ahmed and H. Hassanein, "A Performance Study of Roaming in Wireless Local Area Networks Based on IEEE 802 . 11r," *24th Bienn. Symp. Commun.*, vol. 2, no. 3, pp. 1–5, 2008.

[42] N. S. V Shet, K. Chandrasekaran, and K. C. Shet, "Implementation of Handoff through wireless access point Techniques," *J. Telecommun.*, vol. 2, no. 2, pp. 143–146, 2010.

[43] J. Mcnair and F. Zhu, "Vertical Handoffs in Fourth-Generation Multinetwork Environments," *Ieee Wirel. Commun.*, no. June, pp. 8–15, 2004.

[44] I. F. Akyildiz, J. McNair, J. Ho, H. Uzunalioglu, and W. Wang, "Mobility Management in Next Generation Wireless Systems," *Proc. IEEE*, vol. 87, no. 8, pp. 1347–1384, 1999.

[45] L. C. Paul, "Handoff/Handover Mechanism for Mobility Improvement in Wireless Communication," *Glob. J. Res. Eng. Electr. Electron. Eng.*, vol. 13, no. 16, pp. 1–9, 2013.

[46] A. Jain and S. Tokekar, "Application Based Vertical Handoff Decision in Heterogeneous Network," *Procedia Comput. Sci.*, vol. 57, pp. 782–788, 2015.

[47] S. Park, P. Kim, and B. Voz, "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)," *Netw. Work. Gr.*, pp. 1–10, 2005.

[48] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs," *MobiWac '04 Proc. Second Int. Work. Mobil. Manag. Wirel. access Protoc.*, pp. 19–26, 2004.

[49] H. Yokota, a. Idoue, T. Hasegawa, and T. Kato, "Link layer assisted mobile IP fast handoff method over wireless LAN networks," *Proc. 8th Annu. Int. Conf. Mob. Comput. Netw.*, pp. 131–139, 2002.

[50] K. El Malki, "Low-Latency Handoffs in Mobile IPv4 Status," *Netw. Work. Gr.*, pp. 1–64, 2007.

[51] R. Koodli, "Fast Handovers for Mobile IPv6 Status," *Netw. Work. Gr.*, pp. 1–42, 2005.

[52] R. Koodli, "Mobile IPv6 Fast Handovers," *Starent Networks*, pp. 1–48, 2008.

[53] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "Fast-handoff Schemes for Application Layer Mobility Management," *IEEE 15th Int. Symp. Pers. Indoor Mob. Radio Commun.*, vol. 3, pp. 1527–1532, 2004.

[54] E. Gustafsson, A. Jonsson, and C. E. Perkins, "Mobile IP Regional Registration," *Mob. IP Work. Gr.*, pp. 1–35, 2001.

[55] M. Zekri, B. Jouaber, and D. Zeghlache, "Context aware vertical handover decision making in heterogeneous wireless networks," *IEEE Local Comput. Netw. Conf.*, pp. 764–768, 2010.

[56] H.-H. C. H.-H. Choi, O. Song, and D.-H. C. D.-H. Cho, "A seamless handoff scheme for UMTS-WLAN interworking," *IEEE Glob. Telecommun. Conf. 2004. GLOBECOM '04.*, vol. 3, pp. 1559–1564, 2004.

[57] Z. Yan, H. Zhou, H. Zhang, H. Luo, and S. Zhang, "A dual threshold-based fast vertical handover scheme with authentication support," *Proc. Int. Conf. Mob. Technol. Appl. Syst. - Mobil. '08*, p. 1, 2008.

[58] 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 Wirel. Commun.*, no. April, pp. 55–64, 2008.

[59] X. Yang, Y. Zhang, J. K. Liu, and Y. Zeng, "A trust and privacy preserving handover authentication protocol for wireless networks," *Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Proce*, 2016.

[60] J. Cao, M. Ma, and H. Li, "An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 10, pp. 3644–3650, 2012.

[61] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wirel. Commun.*, vol. 11, no. 1, pp. 48–53, 2012.

[62] C. Perkins, "IP Mobility Support for IPv4," *Netw. Work. Gr.*, pp. 1–99, 2002.

[63] A. Mishra, M. Shin, and W. A. Arbaush, "Context caching using neighbor graphs for fast handoffs in a wireless network," *Ieee Infocom 2004*, vol. 1, pp. 351–361, 2004.

[64] H. Wang and A. R. Prasad, "Fast Authentication for Inter-domain Handover," in *Telecommunications and Networking - ICT 2004*, 2004, pp. 973–982.

[65] S. Patrick and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *IEE Proc. Commun.*, vol. 151, no. 5, pp. 489–495, 2004.

[66] B. Alotaibi and K. Elleithy, "Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions," *Wirel. Pers. Commun.*, vol. 90, no. 3, pp. 1261–1290, 2016.

[67] S. Bangolae, C. Bell, and E. Qi, "Performance study of fast BSS transition using IEEE 802.11r," *Proceeding 2006 Int. Conf. Commun. Mob. Comput. - IWCMC '06*, p. 737, 2006.

[68] A. A. Tabassam, H. Trsek, S. Heiss, and J. Jasperneite, "Fast and seamless handover for secure mobile industrial applications with 802.11r," *Proc. - Conf. Local Comput. Networks, LCN*, no. October, pp. 750–757, 2009.

[69] B. Aboba, “IEEE P802.11 Wireless LANs: IEEE 802.1x Pre-Authentication,” *One Microsoft W.*, no. June, p. 10, 2002.

Authors

Tahadray Jean Tsitaitse received the Bachelor degree in computer science and Technology 2011 and Master degree 2014 at Beijing University of Technology. Now he is PHD student in Beijing University of Technology. His current research interest include wireless sensor networks and Market analysis for improving network security.

Yongquan CAI is a professor and doctoral supervisor in the College of Computer Science and Technology, Beijing University of Technology. His research interests include information security, computer network, cryptographic protocols analysis and formal methods in cryptography.

Shaldon Leparan Suntu received his Bachelor Degree in Information and Technology in 2012 from Kenyatta University, Kenya and Master Degree in Information and Communication Engineering in 2018 from University of Science and Technology Beijing, China. His area of interest include; Wireless Communications, Networking, Databases, Web Design, Data Privacy.

Muhammad Nafees Ulfat khan received his degree of Bachelor of Science in Electronics and Communication in 2013 from University of Lahore, Pakistan and Master Degree in Information and Communication Engineering in 2018 from University of Science and Technology Beijing, China. His research area is Light fidelity (Li-Fi) and visible light communication (VLC).