MIS Review Vol. 21, No. 1, Nos. 1/2, September(2015)/March (2016), pp. 35-50
DOI: 10.6131/MISR.2015.2101.03

Secure WLAN Handoff Scheme with Continuous Authentication

Rajeev Singh[1], Teek P. Sharma[2]
[1]G. B. Pant University of Agriculture and Technology, Uttarakhand, India;
[2]National Institute of Technology, Hamirpur (H.P.) India

ABSTRACT: *Handoffs are essential for providing continuous mobility to a wireless Station (STA) in an Enterprise LAN. An important requirement of the handoff is to establish connection of the roaming STA with a new Access Point (AP) securely and quickly such that the undergoing communication remains unaffected. We propose a novel handoff scheme for enhancing the handoff performance and security. The scheme is a lightweight and reactive method for transferring the keying material i.e., STA context to new AP. Scheme utilizes Key Hiding Communication (KHC) scheme for ongoing data communication between STA and AP. It provides continuous authentication between STA and APs. Computation and communication cost for the handoff process are calculated and security analysis is done. A comparison with other handoff schemes is also provided.*

KEYWORDS: *WLAN Security, Key Based Communication, Handoff, Lightweight Authentication.*

1. Introduction

Wireless networks supporting real time applications like Voice over IP (VOIP), e-conference etc. requires instant availability and seamless secure roaming (Bojkovic et al., 2005). This is achieved by wireless Station (STA) handoff to the new Access Point (AP). The desired properties of a good handoff are: (1) handoff should be completed within time limits as suitable for the multimedia and real time applications and (2) the handoff should be performed securely.

The communication interruption time tolerable for multimedia and real time applications during handoff is approximately 50 ms (Lee, 2010; Lee & Hunt, 2010). This is the time when mobile STA cannot send or receive data packets from its correspondent nodes. This time should be minimized such that the STA communicates with its correspondent node continuously. The 802.11i WLAN security standard provides the secure STA authentication at AP by utilizing the Authentication Server (AS) services. The secure STA authentication (default Full EAP/TLS) evolves shared secret key between STA and AP. The entire process takes time of the order of 300 ms to 4 seconds (Martinovic et

al., 2006, 2007) which make it unsuitable for the handoffs. This handoff time should be reduced while maintaining the security properties. For reducing the handoff time, pre-authentication is used where full 802.1X authentication is performed before starting the handoff. Here, STA starts EAP/TLS authentication with the candidate AP (new AP with which STA handoff is performed) through old AP connection. Old AP forwards the authentication messages to the AS. This process is termed as pre authentication. It ends when STA and new AP receive new PMK. Later, when handoff is initiated only 4-way handshake is required to complete the authentication. Involvement of AS is not required during the handoff reestablishment of trust relationship. This results in overall reduction in handoff delay and packet loss (Compton, 2008; IEEE 802.11i, 2004; Kassab et al., 2005).

Predictive authentication and proactive key distribution are proposed by the researchers to reduce time in locating and predicting the candidate AP. This involves overheads and security issues. In proactive key distribution, a group of candidate access points are determined and new shared key (i.e., PMK) is distributed among them before the handoff (Hur et al., 2007; Ling et al., 2010; Mishra et al., 2004a, 2004b; Pack et al., 2005). This introduces extra communications with all candidate APs instead of communicating with one candidate AP. In prediction based handoff techniques, if the prediction misses, the complete authentication is required for communication with the candidate AP (Chien et al., 2008; Kassab et al., 2005; Pack & Choi, 2004). This affects smooth handoff process. 802.11i also does not define candidate AP prediction as an inaccurate prediction may lead to large resource wastage. Thus, proactive key distribution is suggestive as compared to predictive authentication provided the extra communication with the group of candidate access points is lightweight and efficient. Another handoff termed as reactive method is also proposed by researchers where STA authentication is executed after the candidate AP is selected. The candidate AP is usually selected by the STA and then the security context (i.e., keying material) is transferred to this AP. For transferring security context, STA requests to AS via old AP, then AS transfers security context to the candidate AP. Security of intermediate messages that are used for authentication and transferring security context is an issue here.

For providing fast and secure handoff for the mobile STA in WLANs, standard bodies IEEE and IETF have defined protocols like Control and Provisioning of Wireless Access Points (CAPWAP), Hand Over Keying (HOKEY) and IEEE 802.11r (Task group r) (Clancy, 2008). CAPWAP supports centralized management of APs. HOKEY extends the Authentication, Authorization and Accounting (AAA) architecture to support key deriving and distribution with involving full EAP authentication. 802.11r depends upon passing credentials directly between APs for handover. Though CAPWAP takes very less time, it is more or less reauthentication with centralized Access Controller (AC), followed by key transfer to new Wireless Termination Points (WTP). HOKEY is successful in

multidomains but it takes more communication time. Among these three (CAPWAP, HOKEY and 802.11r), 802.11r is more efficient in terms of communication overheads. It still has issues concerning the safe transfer of key between APs.

We propose a novel Secure WLAN Handoff Scheme that maintains security properties while evolving and transferring the security context (key and initial vector) to the candidate AP. The scheme is lightweight and uses reactive method for handoff. The proposed secure handoff scheme not only provides the handoff within desired time limits required by multimedia and real time data traffic but also maintains desired security using primitives like lightweight authentication, encryption and Message Integrity Code (MIC) to all the messages involved in the handshake process. Two kinds of APs are defined in the scheme: normal AP and Domain Controller AP (DCAP). STA request DCAP through normal AP by putting ID of the candidate AP. DCAP in turn distributes the STA context (key and initial vector) to the candidate AP. Thus, when STA roams into the area of candidate AP, less time is involved in the STA authentication at the candidate AP.

The rest of the paper is divided into 4 sections. Section 2 presents the related work done. Section 3 proposes the secure handoff scheme. Section 4 discusses the performance issues and comparison among the related handoff schemes. Section 5 provides security analysis while section 6 provides conclusion.

2. Related work

Several predictive and pre-authentication schemes are proposed for enhancing the handoff (Compton, 2008; IEEE 802.11i, 2004; Kassab et al., 2005). Kassab et al. (2005) proposed statistical methods for modeling the mobility pattern of the STA. As a result of the model, a set of access points are selected in the handoff region. STA can associate with any one of them and thus, STA needs to exchange fewer messages with the candidate AP. An interesting concept of neighbor graph has been introduced in (Mishra et al., 2004a, 2004b; Shin et al., 2004) that identifies the candidate access points, one of which would associate with STA. The key material is distributed to these candidate access points. New Pairwise Master Keys (PMKs) are generated using PMK trees. As the key material is received by APs before the handoff, this process is termed as proactive key distribution. Communication between AP and AS is reduced in the scheme. Still the process introduces communication overheads between the candidate access points and the AS. For further reducing this overhead, improvements like selective neighbor caching and proactive key distribution with anticipated 4-way handshake are suggested in (Hur et al., 2007; Ling et al., 2010; Pack et al., 2005). In former, the STA context is transferred to only selective neighbors. In case only one neighbor is selected, it becomes similar to reactive handoff

method. In latter, the 4-way handshake is not required at the start of handoff rather STA generates PTKs before handoff with the help of candidate AP list sent by the AS. The method is useful mainly for 802.1X based networks.

Fast AP Transition Protocol (FATP) scheme uses proactive key distribution technique to transfer existing security context to the candidate AP before handoff (Lee, 2010; Lee & Hunt, 2010). After transferring the security context, the roaming STA and candidate AP mutually verify each other's identity and derive new session keys. This does not require involvement of AS during the STA reassociasation with the candidate AP. The resulting trust relationship has same properties of full EAP/TLS authentication and has less cost in terms of latency, computational power and network traffic overhead. It implements authentication followed by reassociation. Authentication leads to establishment of trust relationships and reassociation leads to changing the AP attachment. The scheme also claims to work under DoS attacks. The issue of DoS attacks is not addressed by any other handoff solutions. Scheme defines two types of intra-domain handoff scenarios namely "R0 to R1" handoff and "R1 to R1" handoff. A secure and fast handoff technique is proposed at (Maccari et al., 2006). It is based upon the concept that when STA moves towards the candidate AP, then candidate AP request for PMK from the AS along with proving its request as legitimate. For this STA gives a token to candidate AP who forwards it to the AS, proving request as legitimate. Token generation is based upon hash calculation using PMK shared between STA and AS. The scheme works only for 802.1X based networks. Another fast authentication scheme for the wireless LAN is proposed at (Zhang et al., 2010, 2011). The scheme reduces the authentication latency during the handoff using a tunnel technique. The tunnel technique provides secure communication. Roaming STA selects the new (candidate) AP and starts the fast authentication process. The ID of candidate AP is transferred to old AP. The old AP uses MAC address of the candidate AP for generating the pair wise tunnel key. This key is then transferred to both mobile STA and the candidate AP. The roaming STA now tries to associate with the candidate AP using this temporal tunnel key. The STA packets are still transferred to old AP which then forwards them to the destination. Mean while the candidate AP starts the EAP/TLS process with STA to generate PMK and PTK. Once PTK is generated temporal tunnel key is obsoleted and the communication starts using the new PTK.

3. Proposed secure WLAN handoff scheme

There are two types of APs involved in the scheme: Domain Controller Access Point (DCAP) and normal Access Points (AP1, AP2, ..., APn). There is only one domain controller AP in a particular domain while there are several normal APs in the domain. It is assumed that domain controller AP has high computation capacity. The main functionality

of domain controller is to authenticate wireless stations and access points. Hence, this role can even be performed by the authentication server (AS) in a domain. Apart from this, DCAP not only evaluates fresh communication key for STA but also forwards refreshed key to the new AP during handoff. The STA performs handoff among normal APs. The proposed scheme has initialization and communication phases similar to Key Hiding Communication (KHC) scheme (Singh & Sharma, 2013a); in addition it has handoff phase.

3.1 Initialization phase

Each wireless station and access point initially authenticates itself to the DCAP and evolves shared master key for communication. For this initial authentication, STA and AP utilize the initialization phase of the Key Hiding Communication (KHC) scheme proposed by Singh and Sharma (2013a). During KHC initialization phase, pair of communicating nodes evolve master key (MK) between them. Using the KHC process, STA is initially authenticated at DCAP and then a master key ($MK^{STA\text{-}DCAP}$) is evolved at the STA and DCAP. Similarly, normal APs evolve secret master key ($MK^{AP1\text{-}DCAP}$, $MK^{AP2\text{-}DCAP}$, ..., $MK^{APn\text{-}DCAP}$) with the domain controller AP. $MK^{STA\text{-}DCAP}$ is termed as MK of the STA. DCAP transfers STA MK securely by encrypting using $MK^{AP1\text{-}DCAP}$ to the current communicating AP (say AP1). Using MK of the STA, initial parameters i.e., CD_0, C0 and C1 are shared between STA and AP. Such initial parameters are also shared between normal APs and domain controller AP. Thus, after initialization each pair of devices has its own set of K_0, IV_0, C0 and C1 required for secure communication. The naming conventions used in the paper are mentioned in Table 1. The wireless handoff scenario along with keys and parameters evolved after the initialization process is shown in Figure 1. As a station may perform frequent handoff, extra memory and computation overheads are involved at nodes. Hence, we assume 128 bit shared master key, 64 bit K0, 64 bit IV0, 64 bit C0 and 64 bit C1 in the KHC scheme.

3.2 Communication phase

After initialization, the communication between STA and AP1 is performed like KHC communication phase. In communication phase of KHC, key refreshing and hiding concept for sharing the symmetric secret key (K_i) and initial vector (IV_i) is introduced. Key and IV refreshing are done using MK. After refreshing, the secret encryption key and IV are protected by XORing with counters C0 and C1 respectively. The key and IV are then mixed with each other before transferring them to the receiver. For mixing, the new byte locations for placing the K_i and IV_i in the CD_i are calculated with the help of existing K_{i-1}. Mixed key and IV is termed as Codeword (CD_i). This codeword is added to the transmitted frame and delivered to the recipient. Corresponding frame MIC is calculated using K_{i-1}. The recipient extracts the key from the codeword, compares it with its own evaluated key, thereby authenticating the sender. Key (K_i) along with IV_i, is then used to

encrypt the data frame to be transmitted next. The key verification at the receiver also provides authentication per frame. The authentication is lightweight as key verification involves operations like increment, XOR and modulus evaluations. MIC of only the authenticated frames is checked. The verified key is utilized to encrypt the data and evaluate MIC for the next frame.

Table 1 Naming Convention

Domain Controller AP: DCAP	*Codewords*
Device Identifiers	New codeword: CD_i
STA identifier: IDSTA (64 bits)	STA-domain controller: $CD^{STA\text{-}DCAP}$
APi identifier: IDAPi (64 bits)	APi-domain controller: $CD^{APi\text{-}DCAP}$
Domain Controller identifier: IDDC (64 bits)	STA-APi: $CD^{STA\text{-}APi}$
Shared Keys	*Initial Vector*
Master Key: MK	Previous IV: IV_{i-1}
Previous Key: K_{i-1}	New IV: IV_i
New Key: K_i	STA-domain controller: $IV^{STA\text{-}DCAP}$
STA-domain controller: $K^{STA\text{-}DCAP}$	APi-domain controller: $IV^{APi\text{-}DCAP}$
APi-domain controller: $K^{APi\text{-}DCAP}$	STA-APi: $IV^{STA\text{-}APi}$
STA-APi: $K^{STA\text{-}APi}$	

Thus, for transferring data between STA and AP in the proposed scheme, first refreshing of key and IV is done then key and IV protection is done which is then followed by key and IV mixing i.e., codeword (CD_i^{STA}) formation. The CD_i^{STA} is sent as extra bytes in the WLAN header. AP verifies codeword and hence authenticates the STA. The contents within the frame body are encrypted using K_{i-1} and IV_{i-1}. Each frame is protected via MIC addition to frame. The receiver verifies the K_i and IV_i from the received codeword (CD_i^{STA}) using protection and mapping. This verification provides per frame authentication. K_i and IV_i are then used to encrypt next frame. Thus, encryption key for each successive data frame is refreshed in this process. Similar key refreshing and verification also takes place between other two pairs i.e., AP and DCAP; STA and DCAP.

Two kinds of frames are used in the proposed handoff scheme: communication frames and handoff frames. The frame types and their corresponding contents are shown in Figure 2. Communication frames are same as that of the KHC scheme with the exception that the codeword size is now 128 bits only. Three different handoff frames are required in the following: between STA and AP1 (current AP); between AP1 and DCAP; and between DCAP and AP2 (new/candidate AP). This implies that 2 bits are required in frame header for indicating the frame type. We consider the proposed implementation strategy by Ren et al. (2004) and use bits B3 and B4 of the data frame control field for frame identification.

For AP1 and DCAP communication

Master Key (128 bit): $MK^{AP1\text{-}DCAP}$

Codeword (128 bit): $CD_0^{AP1\text{-}DCAP}$

Initial Key (64 bit): $K_0^{AP1\text{-}DCAP}$

Initial Vector (64 bit): $IV_0^{AP1\text{-}DCAP}$

Counters (64 bit each): $C0^{AP1\text{-}DCAP}$, $C1^{AP1\text{-}DCAP}$

For STA and DCAP communication

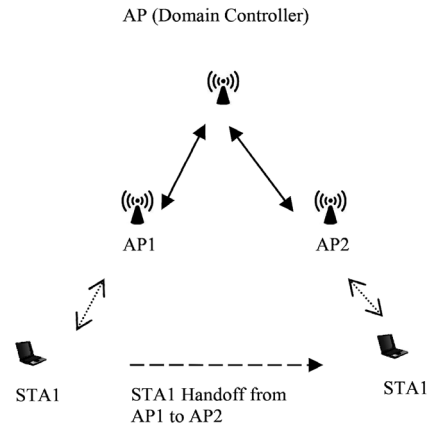
Master Key (128 bit): $MK^{STA\text{-}DCAP}$

Codeword (128 bit): $CD_0^{STA\text{-}DCAP}$

Initial Key (64 bit): $K_0^{STA\text{-}DCAP}$

Initial Vector (64 bit): $IV_0^{STA\text{-}DCAP}$

Counters (64 bit each): $C0^{STA\text{-}DCAP}$, $C1^{STA\text{-}DCAP}$



For STA and AP1 communication

Master Key (128 bit): $MK^{STA\text{-}AP1}$

Codeword (128 bit): $CD_0^{STA\text{-}AP1}$

Initial Key (64 bit): $K_0^{STA\text{-}AP1}$

Initial Vector (64 bit): $IV_0^{STA\text{-}AP1}$

Counters (64 bit each): $C0^{STA\text{-}AP1}$, $C1^{STA\text{-}AP1}$

Figure 1 WLAN Handoff Scenario along with Keys and Parameters

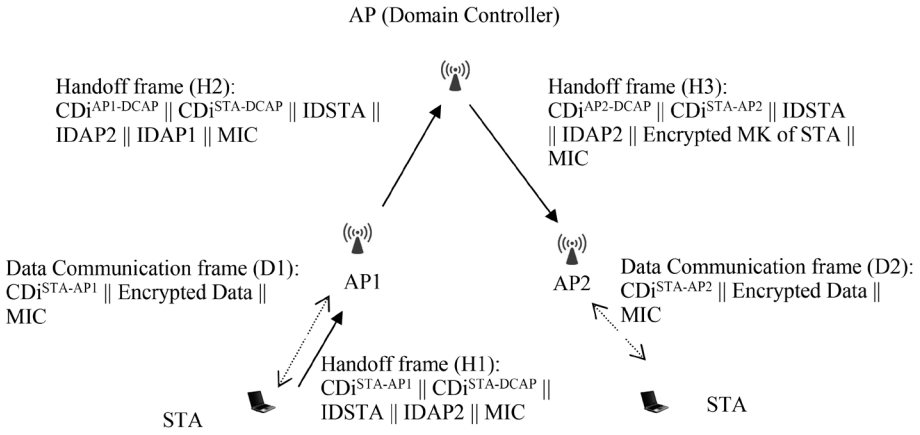
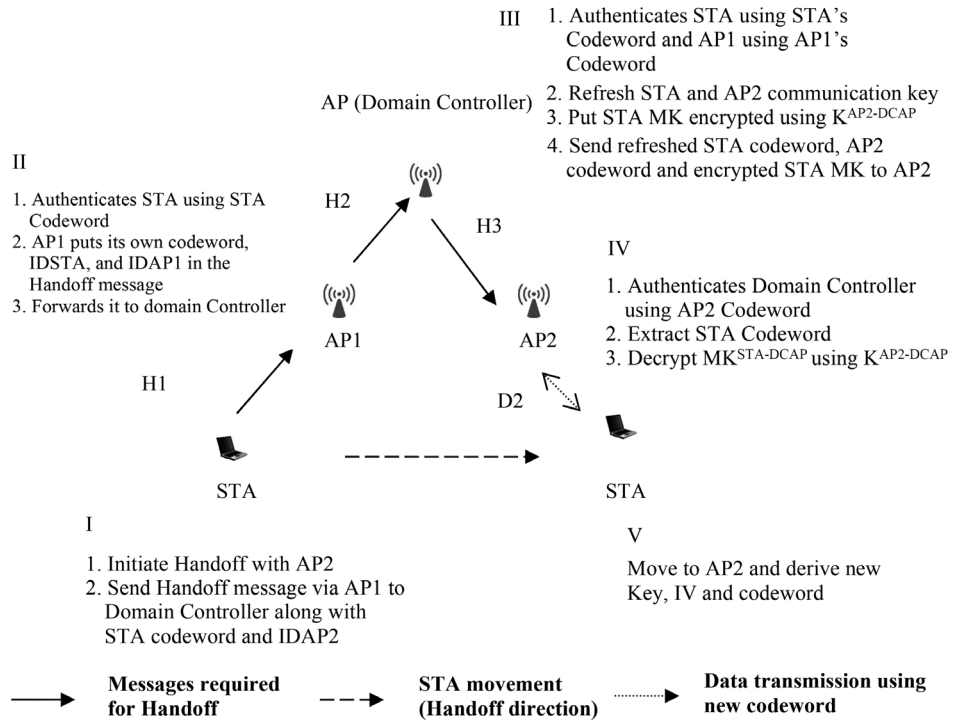


Figure 2 Frame Types and Contents

Combination "00" indicates communication frame between STA and normal AP, "01" indicates handoff request from STA to AP, "10" indicates handoff request by old AP (AP1) to domain controller AP, "11" indicates handoff response from domain controller AP to new AP (AP2).

3.3 Handoff phase

STA which is currently under AP1 (old AP), sends handoff request to the AP1whenever handoff with AP2 (candidate AP) is required. STA sets the handoff bits in the frame header as "01" and puts its own ID as well as ID of AP2 in the frame body. New codewords ($CD_i^{STA\text{-}AP1}$ and $CD_i^{STA\text{-}DCAP}$) and MIC are appended to it. On receiving this handoff request, AP1 removes



Node Processing: I (At STA), II (At AP1), III (At Domain Controller), IV (At AP2), V (At roaming STA)

Handoff Messages: H1, H2, H3, H4

All the messages sent by any of the node are protected using the MIC evaluated using its own Key

Figure 3 STA Handoff with AP2

$CD_i^{STA\text{-}AP1}$ and verifies authenticity of the STA through STA codeword. AP1 then appends IDSTA, its own IDAP1 and codeword ($CD_i^{AP1\text{-}DCAP}$) in the frame body along with

MIC. This request is forwarded to the domain controller. Domain controller authenticates STA and AP1 by verifying their codewords ($CD_i^{STA\text{-}DCAP}$ and $CD_i^{AP1\text{-}DCAP}$). It generates new codewords for AP2 ($CD_i^{AP2\text{-}DCAP}$) and STA ($CD_i^{STA\text{-}AP2}$), puts them in response frame to AP2. Domain controller also puts the encrypted MK for the current STA session. On receipt of response frame, AP2 extracts its own codeword, authenticates domain controller and extracts the STA codeword ($CD_i^{STA\text{-}AP2}$). The roaming STA request is verified using this extracted codeword. AP2 also extracts the MK of the STA session by decryption using $K_{i-1}^{AP1\text{-}DCAP}$. With the help of MK, AP2 further performs key refreshing and safe key transfer with STA. This accomplishes STA handoff with AP2. The entire handoff process the shown in Figure 3.

The computation and communication costs are involved in the proposed handoff scheme Three handoff messages i.e., H1, H2, H3 are exchanged among STA, AP1, DCAP and AP2. Scheme is reactive and therefore context/keying material is not supplied to all APs as done in proactive schemes, rather only one candidate AP is given STA communication key. The scheme provides secure communication as all the 3 handoff messages are protected by MIC and mutual authentication exists among all parties i.e., STA, AP1, DCAP and AP2 via codeword verification. The scheme also provides protection to handoff against DoS attacks at AP2. Before the handoff message H3 is received at AP2 all the DoS attack packets are dropped. Once STA's communication message i.e., D2 is received at the AP2, the entire process is nothing but the KHC communication and is safe under DoS attack.

4. Performance evaluation

For the proposed scheme, we calculate communication cost, network overload and computation cost required for performing the handoff and compare them with CAPWAP, HOKEY, IEEE 802.11r and FATP.

4.1 Communication cost and network overload

STA requires a total network overload of four messages i.e. H1, H2, H3 and D2 to perform the handoff successfully with AP2. For simplification, we assume that the transmission latency between STA and AP is same as that of between AP and Domain Controller. The transmission time between two nodes using an IP socket (using UDP datagram) between two systems averages to 1.9796 milliseconds (Singh and Sharma, 2013b). In proposed handoff scheme, four such communications are required: between STA and AP1 (old AP); between AP1 and domain controller; between domain controller and AP2 (candidate AP); between STA and AP2.

Therefore, communication cost of our proposed handoff scheme is equal to 4 × 1.9796 ms = 7.9184 ms.

Table 2 Computation Cost of the Proposed Handoff Scheme

Device	Processing/Computations	Number
STA	Key and IV refresh	03
	Key protection and Key mapping	03
	Encryption	01
AP1	Key and IV refresh	02
	Key protection and Key mapping	02
Domain Controller AP	Key and IV refresh	04
	Key protection and Key mapping	04
	Encryption	01
AP2	Decryption	02

4.2 Computation cost

The proposed scheme involves computations at the STA, old AP (AP1), domain controller AP (DCAP) and candidate AP (AP2). The computations involved are listed in Table 2. Key protection and key mapping is done using XOR and modulus operations, respectively while Key and IV are refreshed using hash calculations. Both XOR and modulus are mathematical operations and takes negligible time as compared to cryptographic primitives. Therefore, we can ignore them from calculations. We consider the average time taken for hash calculation as 0.1256 ms (Singh & Sharma, 2013b). Total number of key and IV refreshing required are 09 while number of encryptions and decryptions required are 02 respectively. As key refreshing and IV refreshing both require hash calculation, 18 hash calculations are required for handoff. For maintaining integrity, MIC computation and verification is required for each of the 4 frames. Thus, computation time for the handoff process is:

$18 \times 0.1256 + 2 \times 0.1223 + 2 \times 0.0533 + 4 \times 0.193 = 3.3834$ ms

Total time required for handoff = communication time + computation time = 7.9184 ms + 3.3834 = 11.3018 ms (<< 50 ms)

Hence, the proposed scheme is well suited for multimedia and real time applications.

4.3 Comparison with other secure handoff schemes

We compare proposed scheme with the existing handoff schemes and standards like CAPWAP, HOKEY, IEEE 802.11r and Fast AP Transition Protocol (FATP) in Table 3.

Table 3 Comparison of Our Scheme with Other Secure Handoff Solutions

Secure Handoff Solutions	Change Required in 802.11	Fresh Session Key	Fresh Traffic key	Communication overhead	Issues
CAPWAP	No change in 802.11 but requires operations at IP layer	Not derived	Yes, AC executes 4-way handshake with STA and delivers new traffic keys for WTP	$4(T_w + T_c) + T_c = 85$ µsec	Fresh session keys are not evolved in the handover
HOKEY	No change in 802.11 but requires operations at IP layer	Yes	Yes	$2(T_w + T_a) + 4T_w =$ 130 µsec	Communication overhead is a concern
IEEE 802.11r	Yes, change in 802.11 protocol itself	Yes, initial AP (R0KH) generates session keys for other APs as PMK-R1, PMK-R2 etc.	Yes, Derived using PMK-R1, PMK-R2 etc.	$2T_w + 2T_c + 2T_w =$ 70 µsec	Caching of PMK by First Authenticator (PMK-R0), Key management involving key transfer between R0KH and R1KH will require $O(n^2)$ keys to be managed between n APs
FATP	Yes, termed as extended authentication frame format	Yes, using PMK-R0	Yes, Derived using PMK-R1	$2T_w + 4T_c^* = 50$ µsec	Caching of PMK is required. Scheme still suffer under DoS attacks.
Proposed scheme	Yes, change in frame formats required	Yes, By Domain controller	Yes, per frame by calculating hash	$2T_w + 2T_c = 40$ µsec	Scheme requires modifications in 802.11 frame formats

Note. * considering secure inter Access Point communication requires only two messages and the handoff takes place from R0 to R1 AP

CAPWAP and HOKEY do not change the existing 802.11 frame structure. All except CAPWAP scheme generates fresh session keys. Fresh traffic keys are generated by all the schemes. Communication overhead in our scheme is less as compared to any other scheme. For calculating communication overhead, we assume in a typical network: transmission latency (T_w) between STA and AP is equal to 15 μsec, latency (T_c) between any two relative close devices including AP to AP and WTP to AC is equal to 5 μsec and latency (T_a) between infrastructure components and local AAA server is equal to 20 μsec (Clancy, 2008).

5. Security analysis

The proposed handoff scheme shortens the handoff latency by initiating a key transfer process prior to moving to the new AP and performing handoff. The security properties of the scheme are analysed in this section.

5.1 Protects STAs from re-associating to malicious APs

As all the packets bear the codeword for authenticating a frame, no malicious STA is able to associate with the normal AP. AP1 authenticates STA by verifying its codeword ($CD_i^{STA\text{-}AP1}$). Domain controller authenticates STA and AP1 by verifying their codewords ($CD_i^{STA\text{-}DCAP}$ and $CD_i^{AP1\text{-}DCAP}$). New AP (AP2) authenticates domain controller by verifying AP2's codeword ($CD_i^{AP2\text{-}DCAP}$). On receipt of communication frame from STA, the codeword of the STA is also verified. Thus, all the frames used in the handoff are authenticated. This protect STAs from re-associating to Malicious APs.

5.2 Evolves fresh keys even during handshake

At old AP (AP1), STA communicates using KHC and hence fresh key and IV are evolved per frame. On performing the handoff, STA refreshes its key and IV. Using key and IV, STA derives fresh codeword for communication with the new AP (AP2). Once codeword is verified, STA's communication with AP2 proceeds further with evolving fresh key and IV.

5.3 Continuous authentication is provided

At old AP (AP1) STA communicates using KHC and hence enjoys continuous authentication. On performing the handoff, STA refreshes its key and IV. Using key and IV it derives a fresh codeword for communication with the new AP (AP2). For each frame, STA authentication process is continued with AP2. Hence, STA enjoys continuous authentication.

5.4 Protection against DoS attacks

In KHC scheme the computational DoS attack has less impact on AP1. AP1 protected by KHC scheme is able to maintain its communication under the computational DoS attack by verifying the codeword followed by MIC verification. This method of verifying codeword before MIC verification helps in protection against computational DoS attack. We realized that AP2 behavior under DoS attack while performing the handoff is same as that of KHC behavior. In handoff situation, STA1 moves to AP2 while communicating with STA2. During this period AP2 is under DoS attack and the attacker's objective is to hamper the handoff process at AP2. None of the attack packets are considered for processing till AP2 gets message H3 for STA handoff. This means all attack packets are dropped till H3 is received. After AP2 gets message H3 for handoff of STA, AP2 starts accepting the packets of the attacker node and STA1. Once the STA packet i.e., D2 is authenticated, the remaining process is same as that for an access point protected by KHC scheme under DoS attack. Thus, the proposed scheme enjoys enough security during the handoff.

6. Conclusion

In this paper, we propose a reactive handoff scheme. As the scheme is reactive, the security context (key and initial vector) is not supplied to all APs rather only one candidate AP is given STA communication key and initial vector. Thus, when STA roams into the area of candidate AP, less time is involved in the STA authentication at the candidate AP. The proposed scheme maintains security properties while evolving and transferring the security context to the candidate AP. The scheme is lightweight and provides continuous per frame authentication. All the handoff messages used in the scheme are protected. As frames are protected using MIC, frame modification is not possible. The proposed handoff scheme has low computation and communication cost (<50ms). This makes it suitable for real time scenarios with frequent handoffs. As compared to other secure handoff schemes, the proposed handoff scheme requires fewer messages, has less communication cost and is secure.

References

Bojkovic, Z., Turán, J. and Ovseník, L. (2005), 'Towards to multimedia across wireless', *Journal of Electrical Engineering*, Vol. 56, No. 1-2, pp. 9-14.

Chien, H.Y., Hsu, T.H. and Tang, Y.L. (2008), 'Fast pre-authentication with minimized overhead and high security for WLAN handoff', *WSEAS Transaction on Computers*, Vol. 7, No. 2, pp. 46-51.

Clancy, T.C. (2008), 'Secure handover in enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11r', *IEEE Wireless Communications*, Vol. 15, No. 5, pp. 80-85.

Compton, S (2008), '802.11 denial of service attacks and mitigation', available at: http://www.sans.org/reading_room/whitepapers/wireless/80211-denial-service-attacks-mitigation_2108 (accessed 26 November 2014).

Hur, J., Park, C., Shin, Y. and Yoon, H. (2007), 'An efficient proactive key distribution scheme for fast handoff in IEEE 802.11 wireless networks', *Proceedings of the International Conference on Information Networking*, Estoril, Portugal, pp 629-638.

IEEE 802.11i (2004), 'IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements-part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: amendment 6: medium access control (MAC) security enhancements', available at: https://standards.ieee.org/findstds/standard/802.11i-2004.html (accessed on 20 November 2014).

Kassab, M., Belghith, A., Bonnin, J.-M. and Sassi, S. (2005), 'Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks', *Proceedings of the Wireless Multimedia Networking and Performance Modeling*, Quebec, Canada, pp. 46-53.

Lee I. (2010), 'A novel design and implementation of Dos-resistant authentication and seamless handoff scheme for enterprise WLANs', Unpublished master thesis, University of Canterbury, Christchurch, New Zealand.

Lee, I. and Hunt, R. (2010), 'A novel design and implementation of Dos-resistant authentication and seamless handoff scheme for enterprise WLANs', *Proceedings of the 8th Australian Information Security Management Conference*, Perth, Australia, pp. 49-61.

Ling, T. C., Lee, J. F. and Hoh, K. P. (2010), 'Reducing handoff delay in WLAN using selective proactive context caching', *Malaysian Journal of Computer Science*, Vol. 23, No. 1, pp 49-59.

Maccari, L., Fantacci, R., Pecorella, T. and Frosali, F. (2006), 'Secure, fast handoff techniques for 802.1X based wireless network, Communications', *Proceedings of the IEEE International Conference on Communications*, Istanbul, Turkey, pp. 3917 - 3922.

Martinovic, I., Zdarsky, F.A., Bachorek, A. and Schmitt, J.B. (2007), 'Measurement and analysis of handover latencies in IEEE 802.11i secured networks', *Proceedings of the European Wireless Conference* (EW2007), Paris, France, pp.1-7.

Martinovic, I., Zdarsky, F. A., Bachorek, A. and Schmitt, J.B. (2006), 'Intro. of IEEE 802.11i and measuring its Sec. vs. performance tradeoff', Technical Report 351/06, Distributed Computer Systems Lab, University of Kaiserslautern, Kaiserslautern, Germany.

Mishra, A., Shin, M.H. and Arbaugh, W.A. (2004a), 'Context caching using neighbor graphs for fast handoffs in a wireless network', *Proceedings of the IEEE conference on Computer Communications*, Hong Kong, China, pp. 351-361.

Mishra, A., Shin, M.H., Petroni, N.L., Clancy, T.C. and Arbaugh, W.A. (2004b), 'Proactive key distribution using neighbor graphs', *IEEE Wireless Communications*, Vol. 11, No. 1, pp. 26-36.

Pack, S. and Choi, Y. (2004), 'Fast handoff scheme based on mobility prediction in public wireless LAN systems', *IEE Proceedings Communications*, Vol. 151, No. 5, pp. 489-495.

Pack, S., Jung, H., Kwon, T. and Choi, Y. (2005), 'A selective neighbor caching scheme for fast handoff in IEEE 802.11 wireless networks', *Proceedings of the International Conference on Communications*, Seoul, Korea, pp. 3599-3603.

Ren, K., Lee, H., Han, K., Park, J. and Kim, K. (2004), 'An enhanced lightweight authentication protocol for access control in wireless LANs', *Proceedings of the 12th IEEE International Conference on Networks*, Singapore, pp. 444-450.

Shin, M., Mishra, A. and Arbaugh, W. (2004), 'Improving the Latency of 802.11 hand-offs using neighbor graphs', *Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services*, Boston, MA, pp. 70-83.

Singh, R. and Sharma, T.P. (2013a), 'A key hiding communication scheme for enhancing the wireless LAN security', *Wireless Personal Communications*, Vol. 77, No. 2, pp. 1145-1165.

Singh, R. and Sharma, T.P. (2013b), 'A secure WLAN Authentication Scheme', *IEEK Transactions on Smart Processing and Computing*, Vol. 2, No. 3, pp. 176-187.

Zhang, Z., Boukerche, A., Hussam M. and Ramadan, S. (2011), 'TEASE: a novel tunnel-based secure authentication scheme to support smooth handoff in IEEE 802.11 wireless networks', *Journal Parallel Distributed Computing*, Vol. 71, No. 7, pp. 897-905.

Zhang, Z., Pazzi, R.W. and Boukerche, A. (2010), 'Design and evaluation of a fast authentication scheme for WiFi-based wireless networks', *Proceedings of the IEEE International Symposium on World of Wireless Mobile and Multimedia Networks*, Quebec, Canada, pp. 1-6.

About the authors

Rajeev Singh received his M. Tech. degree in computer science & engineering from Indian Institute of Technology, Roorkee, India in 2008 and his PhD degree from National Institute of Technology, Hamirpur, India in 2014. Currently, he is working as an assistant professor with the Department of Computer Engineering, Govind Ballabh Pant University of Agriculture & Technology, Uttarakhand, India. His research interest includes computer networks and network security.

Corresponding author. assistant professor, Department of Computer Engineering, Govind Ballabh Pant University of Agriculture & Technology, Uttarakhand, India 263145. Tel: +91-5944233338. E-mail address: rajeevpec@gmail.com

Teek Parval Sharma received his PhD degree from Indian Institute of Technology, Roorkee, India in 2009 in the area of wireless sensor networks. He is an associate professor at National Institute of Technology, Hamirpur, India. He has published numerous high quality research papers in international/ national journals and conferences, and has also contributed in various books of standard international publishers. His research interest includes distributed systems, wireless sensor networks, mobile Ad hoc networks, and wireless networks. E-mail address: teekparval@gmail.com