# Balanced Scheme for Faster Authentication and Resilient Security in Vertical Handoff

**Hemavathi, S. Akhila**

***Abstract: The existing solution of channel and communication protection while performing vertical handoff is less capable to withstand potential threat. Not only this, it also results in significant forms of computational burden and increased authentication latency owing to the usage of either complex or flawed cryptographic protocols. The existing literatures were reviewed to find that studies towards faster handoff don't converge with the studies towards secure handoff at any point. Hence, a novel mathematical modeling is introduced where core emphasize was to reduce the computational burden of the encryption scheme during vertical handoff scheme with a mobile user migrating from WLAN to CDMA network. It was achieved without compromising with the security strength of the proposed authentication policy and offered a good balance between faster authentication and robust secure communication. The study outcome was found to offer superior authentication time in contrast to existing extensible transport layer security.***

***Index Terms*: *Vertical Handoff, CDMA, IEEE 802.11, WLAN, Authentication Latency, Delay.***

## I. INTRODUCTION

The usage of IEEE 802.11 standards in the form of Wireless Local Area Network (WLAN) has been increasingly used owing to its cost effectiveness in the deployment [1]. Although, it can provide a larger network but it cannot compete with the mobile networks e.g. CDMA. One of the operations that significantly differentiate them is the mechanism of handoff. A user can seamlessly perform handoff in existing mobile network without any effect on any calls on progress but the same is not so in WLAN [2 networks [4], there is no standard scheme that could ensure fast and secure vertical handoff mechanism. Some of the prime reason for this is: there is an increasing dependency of beacon exchange among the communicating nodes via an access point in IEEE ]. Hence, if a user is migrating from WLAN to CDMA network, offering faster handoff mechanism is one of the critical research problems which still have no effective solution. Irrespective of a number of research work in vertical handoff [3] and increasing number of attacks on mobile 802.11 networks that introduce potential latency in it [5].

Existing research work has witnessed usage of Predistribution and Pre-authentication-based security approaches [6]. According to such schemes, the process of repeated authentication is avoided by performing authentication of all the involved mobile nodes prior to actually perform handoff mechanism. Unfortunately, the existing schemes don't address the fact that existing WLAN is totally incapable of selecting any form of candidate access points on the basis of any standard logic [7]. There are existing techniques where location frequency of handoff operation is higher is used as the selection factor for choosing the best access point [8] and usage of neighboring graph can also be used for the similar purpose [9]. It should be noted that existence of such proactive techniques doesn't offer any form of assurance towards reauthentication. On the other hand, the area of network security has made a tremendous success and at present there are various standard protocols to claim security over mobile networks [10]. However, there still exists some problems like i) existing cryptographic protocol usage towards handoff has never been reported to be benchmarked even in homogeneous network and hence there is an exponential level of threats when it comes to heterogeneous network i.e. vertical handoff, ii) an existing mechanism of mutual authentication has reported use of either bulky cryptographic algorithm like RSA or defective security protocols (e.g. WEP, WPA, etc) [11]. It is also seen that usage of conventional encryption mechanism like Advanced Encryption Standard (AES) which is claimed to provide better authentication, encryption, and integrity is found to offer overhead in the range of 12-22 bytes [12]. Similarly, usage of frequently adopted encryption scheme e.g. HMAC and SHA are associated with 44 bytes of overhead [12]. Hence, it is really a challenging task for a mobile node being moving from WLAN to CDMA network for retaining maximum security with consistent focus on faster authentication technique.

Therefore, this work presents one such novel solution “balanced scheme for faster Authentication and resilient security in vertical Handoff” followed by a mathematical modeling for the same evolving with a solution. That is, the security potentials of proposed system are briefly analysed apart from the established faster authentication time so that a good balance between faster authentication and strong secure communication is obtained.

**Revised Manuscript Received on May 21, 2019.**

**Hemavathi**, Electronics and Communication Engineering, VTU/ AMC Engineering College/ Bangalore, India.

**S. Akhila,** Electronics and Communication Engineering, VTU/ BMS College of Engineering / Bangalore, India..

The scope of the work is to construct a fast authentication scheme by ensuring that encryption process doesn't consume much time and brief analysis of security using unique characteristics of user device during vertical handoff process. Hence, the proposed system is found to offer a good balance between network security and faster authentication principle.

The organization of the paper is as follows: Section 2 discusses existing approaches on faster handoff techniques and secure handoff techniques followed by briefing of research problems in Section 3. The next Section 4 briefs about research methodology adopted to solve the problem of faster and secure authentication in vertical handoff followed by discussion of mathematical modeling in Section 5. Result analysis is illustrated in Section 6 followed by conclusion on Section 7 to brief the study contribution.

## II. RELATED WORK

This section is a continuation of our prior study [13] where more literatures and approaches related to handoff mechanism is updated. The studies using fast handoff mechanism were initially explored in order to check the impending factors for it as well as to understand different research methodologies. From the study presented by Zhang et al. [14], claimed issues related to faster authentication in WLAN is mobility of the user device and implemented Software Defined Networking and Kalman filter in order to speed up the handoff process. However, the work doesn't offer much significance to access points. The contribution of access points plays a critical role by offering enriched list of channels to the nodes connected with it also called as requestor node. This discussion was presented by Bose and Hari [15] for similar cause of minimizing authentication delay. The limitation of this work is that it doesn't address decision formation during handoff in 802.11 networks.

Study to address such limitation was carried out by Chen and Qian [16] where a unique architecture for service relaying mechanism is constructed using backbone network existing between routers in WLAN with experimental approach. Literatures have also witnessed studies towards handoff mechanism over mobile internet protocol in order to address the problems of delay. Study considering such concept was presented by Chiang et al. [17] who have introduced group-based control scheme to minimize latency. The concept uses both mobile node as well as its adjacent nodes. However, such mobility concepts are less likely to work on intelligent transportation system which demands more complex pattern of mobile node connectivity. Hence, such scheme also offers tunneling complexity as well as delay. Solution to such problems have been presented by Ryu et al. [18] which mainly emphasize on the update operation associated with node address followed by enrollment process of home agents. However this process also results in increased dependencies on mobility stack obtained from mobile node. At the same time, it also induces burden of various updates of location that may finally result in communication degradation. This problem was found addressed in the work done by Yan and Lee [19] by introducing a concept for transmitting information about state of the network between the gateways. The system contributes to minimization of location updates while performing handoff. Study towards assessing the credential of the mobile station has been presented by Fu et al. [20] where a base station performs judging of legitimacy of the mobile station using group key-based authentication mechanism. Study towards faster handoff mechanism was also presented by Lee and Wang [21] that target to minimize any events of service disruption. The technique focuses on both up/down link transmission using analytical modeling approach. Usage of multicasting-based approach for solving handoff delay has been discussed by Im and Jeong [22]. The scheme introduces a proxy mechanism for facilitating minimal interactions between communication scheme and multicast beacons. Existing techniques of faster handoff mechanism also witnessed usage of extension theory as well as accumulation concept for facilitating better decision making during handoff as seen in study of Wu et al. [23]. All these discussion techniques have good assurance of faster handoff mechanism but don't incorporate security measures.

Existing security schemes towards handoff operation is mainly associated with the implementation of cryptographic algorithms. The work carried out by Chi et al. [24] have introduces an authentication technique using IEEE 802.11s and IEEE 802.11i standard using analytical approach. However, the study has been assessed only with respect to the mesh network and hence its applicability is less on other larger and dynamic form of network. The solution towards secure handoff has been also discussed by Deng et al. [25] considering vehicle-to-vehicle communication. The study outcome has been claimed to offer better handoff latency as well as update of node location. This scheme could invoke loss of packet inspite of the fact that it minimizes overhead due to signaling. The solution to this problem has been presented by Chuang et al. [26] by introducing a password-based policy for identifying the legitimate user. The mechanism is designed for resisting intrusion in mobile networks and was claimed to offer higher degree of solution towards majority of lethal attacks with lower computational burden. However, it doesn't offer any prove that it is characterized by faster authentication process. A similar form of approach towards secure handoff has been presented by Yan et al. [27] where channel –based probing scheme using opportunistic approach has been emphasized using network-based information extracted from radio in order to minimize authentication latency. However, the major pitfall of this mechanism is its dependencies on prior information about the network topology as well as it doesn't address heterogeneous network. Ciou et al. [28] have presented an authentication policy using conventional Diffie-Hellman approach. The technique has emphasized on enhancing the flow of the generation of secret key along enhancement on conventional Extensible Authentication Protocol EAP in WLAN. Hence, although, there are various works towards secure handoff scheme, there is a lack of consideration of heterogeneous network as well as no significance achievement of minimizing faster process of vertical handoff. The next section outlines research problems.

## III. RESEARCH PROBLEMS

While working on the security of user's resources and availability of services, it is essential to ensure that encryption mechanism doesn't consume much time. The conventional usage of cryptography method calls for iterative operation which suffers from scalability problems [AR]. Considering the case of WLAN, there is a major problem associated with its Extensible Authentication Protocol EAP based approaches [AR]. Moreover, the security protocols of WLAN don't offer any 100% evidence of its resiliency to maximum attacks in wireless environment. It is also explored that existing studies are less emphasized on computational complexity as well as data privacy. However, the significant research challenge is that-If a robust access rights mechanism has been identified then it has to be executed on the user's machines which are never safe from any forms of attacks in wireless environment.

The potential challenge is to ensure a fail proof encryption towards such sensitive information that bears private information of the user as well as security algorithms. Usage of complex and iterative encryption mechanism will also consume maximum amount of time required for authenticating a requestor node. Ensuring faster authentication time with equal justification to security over access rights is quite a computational complex task yet to be seen. Hence, the research problem can be stated as *"To develop robust and secure authentication mechanism with faster response time while performing vertical handoff operation in wireless network"* The next section briefs about the research methodology followed by mathematical modeling to evolve up with a solution.

## IV. PROPOSED METHODOLOGY

The proposed research work aims to develop a secure vertical handoff mechanism without compromising the computational time associated with it in the form of authentication. Fig.1 highlights the implementation scenario of the proposed system which mainly consists of *network model* and *authentication mechanism*. The proposed system considers two network domains i.e. WLAN and CDMA which is also considered to possess a specific and respective access rights that are organized in the form of tree structure. The proposed system also introduces a mathematical modelling to execute the process of authentication on the basis of user device dynamic characteristics in order to retain maximum level of secrecy. The complete authentication process is carried out by structurization, generating security token, core security implementation with encryption and decryption, and access right organization. A new actor called as *network validator* is introduced which performs authentication of the requestor node from WLAN. The authentication is only rendered successful when the decryption key satisfies the access right organization. The prime target of the proposed system is to introduce a faster process of authentication in heterogeneous network domain. Moreover, it is also free from any dependencies of user's identity on any home networks while normal mobile user resumes its authentication just by validating the security token that is generated. The complete concept finally reduces the transmission delay without much iterative steps or any form of dependencies towards resources and hence results in faster process of encryption and decryption using simple and lightweight cryptography.

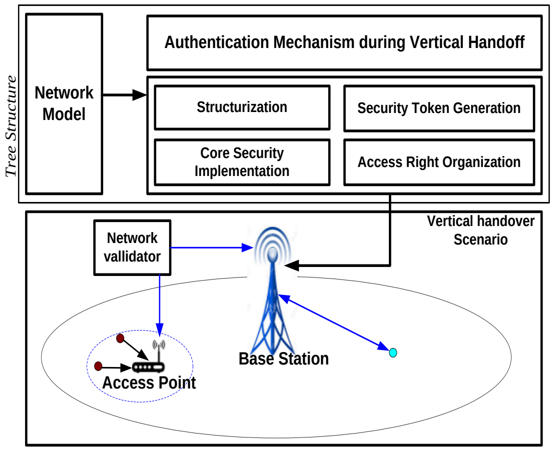

Tree Structure
Network Model
Authentication Mechanism during Vertical Handoff
Structurization
Security Token Generation
Core Security Implementation
Access Right Organization
Network vallidator
Vertical handover Scenario
Base Station
Access Point

Fig. 1 Implementation Scenario of Proposed System

## V. MATHEMATICAL MODEL

This section discusses about the simple mathematical modelling constructed in order to develop a faster authentication policy between two heterogeneous networks. The execution of the proposed system is considered to have been taken place during the spatial migration of a user from one form of network to other with different set of dependencies of each of the network. The secure authentication principle is considered during such migration from Wi-Fi network to CDMA network with supportability of routers and base station respectively. Following are the essential model description:

### A. Network Model

The network model of the proposed system is developed using graph theory where $G_1$ and $G_2$ are the graphs that corresponds to WLAN network and CDMA network respectively. Hence, the empirical expressions (1)-(2) of them are,

$$G_1 \rightarrow (V_1, E_1)^{d_1} \qquad (1)$$

$$G_2 \rightarrow (V_2, E_2)^{d_2}$$

(2)

Different from conventional tree form, the above representation of graph is flagged with its dependency parameters $d$ on each form of graph. Therefore, total number of user device η can be empirically represented as (3),

$$\eta \to (V_1)^{d_1} + (V_2)^{d_2} \tag{3}$$

In the above expression, $d_1$ and $d_2$ are also termed as network coefficient that is highly specific to $G_1$ and $G_2$ and $d_1 \neq d_2$ in every respect. Apart from this, the study also considers a new device called as network validator $\alpha$ that performs a preliminary check on the legitimacy of a node attempting to perform a new admission to its home network. In order to perform an internal assessment, the proposed technique considers analysing with different number of network validator $\alpha$ nodes. A typical implementation scenario of the proposed network model is pictorially shown in Fig.2

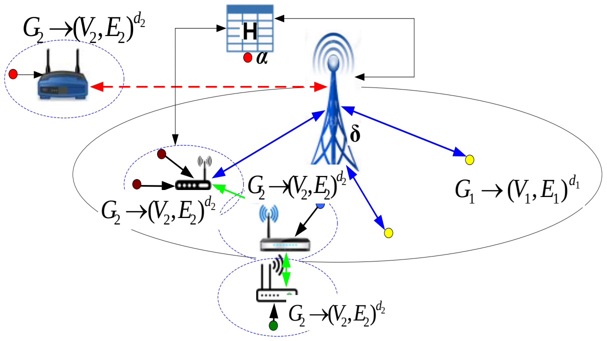

$G_2 \to (V_2, E_2)^{d_2}$
H
α
δ
$G_2 \to (V_2, E_2)^{d_2}$
$G_1 \to (V_1, E_1)^{d_1}$
$G_2 \to (V_2, E_2)^{d_2}$
$G_2 \to (V_2, E_2)^{d_2}$

**Fig. 2** Network Model

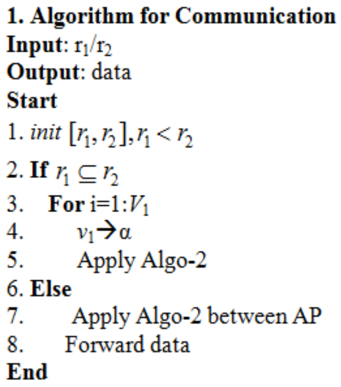
It is essential to understand more discretely about the network coefficients $d_1$ and $d_2$ in order to assists in modelling the hand-off scheme for proposed system. Referring to Fig.2, the technique considers that a sample node within WLAN is attempting to move into CDMA network with three forms of possibilities i.e. i) the *first possibility* is when a node belonging to WLAN is within the range of CDMA network, ii) *second possibility* is when a node of WLAN is out of range of CDMA network, and iii) *third possibility* is when a node of WLAN is out of range of CDMA network but is connected by its neighbouring WLAN node using multihop. Owing to various situations of the positioning of the nodes within a test environment, it is assumed that the dependable parameters of the two networks (i.e. $d_1$ and $d_2$) are executed by routers and base station respectively. In order to bring out security formulation in proposed system, the proposed security solutions are implemented within the set of characteristics drawn from the dependable parameters. The mathematical forms of this concept can be represented as (4),

$$d_1 \cap d_2 = H \tag{4}$$

Where, $H$ can be termed as security demand matrix that is exclusively a multi-dimensional matrix for catering up three specific constraints e.g. i) first constraint $c_1$ represents independent strategy constructs , ii) second constraint $c_2$ represents continuous handoff mechanism, and iii) third constraint $c_3$ represents superior access control. It will eventually mean that,

$$H \subseteq \{c_1, c_2, c_3\} \tag{5}$$

According to the above expression (5), the first constraint $c_1$ is all about invoking autonomous constructions of different access strategies for $d_1$ and $d_2$ so that secure authentication can be carried out from either side of network domain. The second construct $c_2$ should assure non-repudiation for any user when roaming to existing network domain or different network domain. The prime agenda here is to address the delay associated with the authentication of the new as well as old user very discretely. Finally, the last constraint $c_3$ is all about flagging the illegitimate attempt of accessing the network domain when the authentication attempt doesn't match with defined authentication strategy developed from either side of network domain. Hence, this completes the construction of network domain. The algorithm for communication is as follows:



```
1. Algorithm for Communication
Input: r1/r2
Output: data
Start
1. init $[r_1, r_2], r_1 < r_2$
2. If $r_1 \subseteq r_2$
3.    For i=1:$V_1$
4.       $v_1 \rightarrow \alpha$
5.       Apply Algo-2
6. Else
7.       Apply Algo-2 between AP
8.    Forward data
End
```

**Fig. 3** Algorithm for Communication

The above algorithm is responsible for performing communication by the user in mobile networks considering handoff scenario. The algorithm works on the principle that transmission range $r_1$ has to be within the transmission range of $r_2$ (Line-2). Any nodes (Line-4) within $V_1$ should first interact with validator α (Line-3) where the algorithm-2 is applied for secure authentication mechanism in order to perform data forwarding to any destination node $v_2$(Line-5). In case, source node $v_1$ stay outside $r_2$ than the authentication between the access points AP is carried out using proposed algorithm (Line-7/8). The network model is now followed by authentication model.

## B. Authentication Mechanism During Vertical Handoff

The proposed study introduces a non-conventional form of encryption where the non-conventional user's characteristics are used. Usage of such strategy is designed keeping in mind about user friendly usage as well as incorporating high degree of privacy to the network devices that stores user's credential. The construction of this algorithm is carried out considering matrix $H$ where a tree structure for access priviledge is retained. A tree-based organization is designed that retains the strategies of access rights for users in either of the network domain. The authorization is said to be successful in this concept is when the private key of the user's device is found to satisfy the constraints imposed by the access right organization in the form of tree structure (Fig.4). The study also considers that the encrypted information is stored with the access right organization.

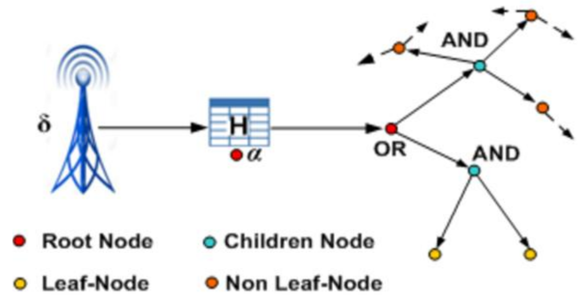


**Fig. 4** Access Right Organizations for Users

The implementation of the above mentioned scheme is carried out in multiple steps as followed:

- *Structurization*: This is the first step towards the design process that is responsible for generating a main and public secret keys i.e. $\phi_m$ and $\phi_{pu}$ respectively. Such generation is again dependent on security attributes e.g. $\beta$.
- *Security Token Generation*: This step of operation is responsible for generating a private secret key $\phi_{pr}$ by considering main secret key $\phi_m$ as well as group of user's characteristics $\gamma$.
- *Core Security Implementation*: This step mainly comprises of encryption and decryption operation of proposed system. This operation results in generated of an encrypted message $I_{enc}$ and uses multiple attributes e.g. message *msg*, access right organization $H$ and public secret key $\phi_{pu}$. The constraint imposed by the proposed technique is that if the user device is found with matched group of user characteristics γ with access right organization $H$ than only they are authorized to perform decryption. Similarly, the process of decryption is carried out on encrypted text $I_{enc}$ using group of user's characteristics γ, private secret key $\phi_{pr}$, and public secret key $\phi_{pu.}$ Hence, the empirical expression of this condition is.

$$\gamma_{requestor}=H \tag{6}$$

Hence, only after satisfying the above mathematical condition, the authorization rights are offered to the requestor node.

- *Access Right Organization*: Basically, this is a matrix that retains the network organization to offer access rights to the requesting users on the basis of legitimacy of their authentication. Similar tree structure is utilized in order to develop access right organization. The study considers leaf nodes to be depicted as user's characteristics while non-leaf node to be depicted as certain cut-off number $T$. The children nodes are considered to be $n$, and hence the relationship between cut-off value and number of children nodes is $0<T<n$. A logical concept is formed as,

$$T_{gate} = \begin{cases} AND & T = n \\ OR & T = 1 \end{cases} \tag{7}$$

In the given tree structure of Fig.5, $n_r$ represents a root node whereas $G$ represents a tree structure. According to proposed concept,

$$G_{n_r}(\gamma) \rightarrow 1 \tag{8}$$

The above expression (8) is considered to be a valid case if group of user characteristics γ is found to be satisfying the access right organization tree $G$ corresponding to root node $n_r$. The system than computes the updated cut-off value for new set of children node considering compliance with expression (8) with a condition that there should be minimum of T number of children node to return the value of 1.

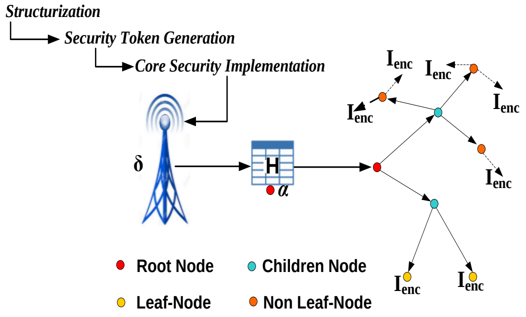


**Fig. 5** Access Right Organizations (Tree View)

The proposed system also incorporates matrix multiplication in order to generate two groups of bilinear characteristics. The study considers formation of dual cyclic groups $\sigma_1$ and $\sigma_2$ that are defined by prime order $o$. Therefore, an integrated function using these vector spaces can be mathematically represented as,

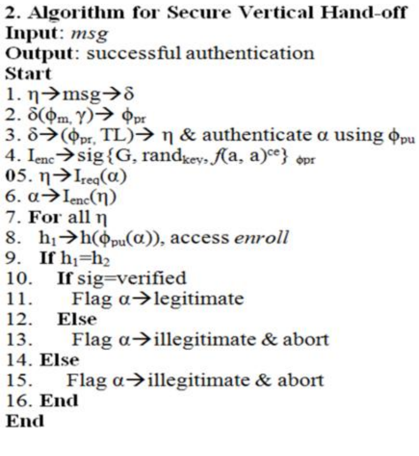
$$f(\mathrm{x}): \sigma_1 \text{ x } \sigma_2 \rightarrow \sigma_2 \tag{9}$$

The above mathematical expression of the integrated function is designed by adhering to three distinct parameters e.g. i) For all $(a, b) \epsilon \sigma_1$ and $(c, e)$ ϵ $Z_o$, $f(a^c, b^e)=f(a, b)^{ce}$. ii) $f(a, a) \neq 1$, and iii) $f(a, b)$ is computed by certain algorithm for all $(a, b) \epsilon \sigma_1$with respect to polynomial time factor. The variable $Z_o$ represents integers of order $o$. The above mentioned properties assist to ensure better form of forward and backward secrecy while performing authentication process between two network domains in vertical handoff mechanism. Hence, a network validator plays a critical role in performing secure authentication during the vertical handoff mechanism.

The complete specification of access right organization is provided by the network validator corresponding to the encrypted message that is also called as encrypted strategy. Hence, the final part of algorithm construction of security token generation is carried out considering 4 specific devices, i.e. i) user device η, network validator *α*, access points AP, and base station *δ*. It is assumed that all the network validator *α* is initially authenticated by base station *δ*. The enrollment of the nodes with their respective identity *P* is carried out within base station,

$$enroll \rightarrow \{P \| h(\phi_{pu})\} \qquad (10)$$

The above mathematical expression for enrolment is specific for specific network domain. This enrolment list is consistently updated for faster and reliable handoff authentication. The algorithm for secure vertical hand-off is as shown in Fig.6. The complete stage of secure authentication process is carried out in two stages viz. stage-1 is associated with initiation stage while stage-2 is associated with handoff stage of communication. A specific message *msg* consisting of location information of η and importance of η is forwarded by the user device to the base station (Line-1). An algorithm for security token generation (Fig.7) is used for generating private secret key $\phi_{pr}$ using main key $\phi_m$ and group of user characteristics γ (Line-2).



```
2. Algorithm for Secure Vertical Hand-off
Input: msg
Output: successful authentication
Start
1. $\eta \rightarrow msg \rightarrow \delta$
2. $\delta(\phi_{m,} \gamma) \rightarrow \phi_{pr}$
3. $\delta \rightarrow (\phi_{pr,} TL) \rightarrow \eta$ & authenticate $\alpha$ using $\phi_{pu}$
4. $I_{enc} \rightarrow sig\{G, rand_{key}, f(a, a)^{ce}\}_{\phi pr}$
05. $\eta \rightarrow I_{req}(\alpha)$
6. $\alpha \rightarrow I_{enc}(\eta)$
7. For all $\eta$
8.   $h_1 \rightarrow h(\phi_{pu}(\alpha))$, access enroll
9.   If $h_1 = h_2$
10.     If sig=verified
11.       Flag $\alpha \rightarrow$ legitimate
12.     Else
13.       Flag $\alpha \rightarrow$ illegitimate & abort
14. Else
15.       Flag $\alpha \rightarrow$ illegitimate & abort
16. End
End
```

**Fig. 6** Algorithm for secure vertical hand-off

The algorithm calls the *Structurization* process for constructing the public secret key $\phi_{pu}$ as well as main key $\phi_{m\ in}$ in following process:

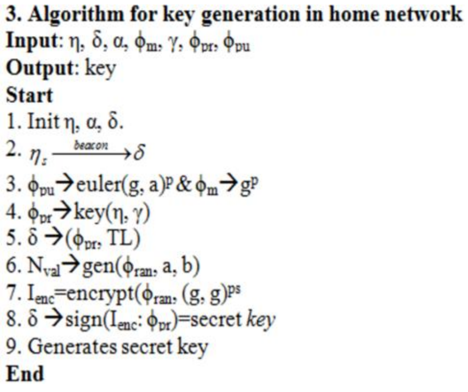
$$\phi_{pu} \rightarrow (\sigma_o, a, b=a^k, f(a, a)^k)$$
$$\phi_m \rightarrow (l, a^k) \qquad (11)$$

In the above expression, *k* and *l* are random integer number of order *o*. The next step of the algorithm is to generate a private key $\phi_{pr}$ by the base station after identifying group of user characteristics γ. This process is carried out by selecting an arbitrary value followed by defining γ and generation of random user characteristics. So the computation of secret key $\phi_{pr}$ is carried out by,

$$\phi_{pr} \rightarrow a(k+w)/l \qquad (12)$$
$$\forall T \in \gamma : (\phi_{pr})_T = a^w . h(T)^{w_T} \qquad (13)$$

In the above expression, *w* is considered as any arbitrary integer. The next part of the algorithm forwards the private key $\phi_{pr}$ by the base station along with information bearing legitimated nodes (i.e. user device) TL (Line-3). The public key $\phi_{pu}$ is made available to the network validator that executes the encryption mechanism. The encryption is carried out by generating certain arbitrary values i.e. $rand_{key}$ and γ (Line-4). The computation of the encrypted information $I_{enc}$ is carried out by considering complete graph G, $rand_{key}$, and a set of linear vector space $f(a, a)^{ce}$. Finally, the base station provides its signature on the encrypted data (Line-4).

The next part of the algorithm implementation is associated with handoff operation. The request for encrypted information $I_{req}$ is forwarded to the network validator by the user device (Line-5). Instantly, the network validator forwards the encrypted information to the user device in order to initiate authentication process (Line-6). The user device then executes following process in order to perform authentication: i) it computes the hash of public key $\phi_{pu}$ of the network validator α (Line-6). It also refer TL in order to check the presence of network validator information on *enroll* matrix followed authenticating it (Line-8). If the generated hash matches with the hash value of specific network domain then it performs the signature verification (Line-9). Otherwise, the network is considered as untrusted and connection is aborted owing to failure of signature verification.



```
3. Algorithm for key generation in home network
Input: $\eta, \delta, \alpha, \phi_{m;} \gamma; \phi_{pr;} \phi_{pu}$
Output: key
Start
1. Init $\eta, \alpha, \delta$.
2. $\eta_z \xrightarrow{beacon} \delta$
3. $\phi_{pu} \rightarrow euler(g, a)^p$ & $\phi_m \rightarrow g^p$
4. $\phi_{pr} \rightarrow key(\eta, \gamma)$
5. $\delta \rightarrow (\phi_{pr;} TL)$
6. $N_{val} \rightarrow gen(\phi_{ran;} a, b)$
7. $I_{enc} = encrypt(\phi_{ran;} (g, g)^{ps}$
8. $\delta \rightarrow sign(I_{enc}: \phi_{pr}) =$ secret key
9. Generates secret key
End
```

**Fig. 7** Algorithm for security token generation

**Table I** List of Notation

| Notation | Meaning |
|---|---|
| $\delta$<br>$\alpha$ | Base Station<br>Network validator |
| $d_1$, $d_2$ | Dependency parameter (network coefficient) |
| H | User device |
| H | Access Right Organization |
| $r_1$, $r_2$ | Transmission range of WLAN and CDMA |
| B | Security Attribute |
| $\phi_m$ | Main Secret key |
| $\phi_{pu}$/ $\phi_{pr}$ | Public Secret key, Private Secret key` |
| $I_{enc}$ | Encrypted data |
| T | Cut-off value |
| N | Children nodes |
| G | Tree structure |
| $n_r$ | Root nodes |
| Γ | User-Defined Characteristic |

The robustness of the proposed authentication mechanism is that its complete dependable parameters for performing encryptions are consistently dynamic in nature and hence it results in unique encryption outcome. Owing to consistent update of access right organization, the proposed system offers faster authentication irrespective of the any level of mobility of the user. It primarily targets man-in-middle attack as well as collusion attack whenever a node attempts to enter a foreign network. Usage of hashing also makes the authentication not only light weighted but also faster in operation for user migration in heterogeneous network domain. The next section discusses about the result analysis. Table I gives the list of notation used in the paper.

## VI. RESULT ANALYSIS

From the prior section of mathematical modelling, it is now clear that proposed system introduces a novel authentication mechanism while performing vertical handoff as well as it equally emphasize on faster execution of the entire authentication process. The scripting of the proposed concept was carried out on MATLAB considering performance parameters of i) time for generation of secret key, ii) encryption time, and iii) decryption time. Majority of the performance parameters considered for analysis is related to time in order to assess the scale of effectiveness in minimizing / controlling authentication time. The best means of gauging the effectiveness of proposed security solution is to compare it with standard and frequently adopted schemes in wireless network. The proposed technique compares its results with conventional Extensible Authentication Protocol EAP that is widely used for ensuring security while accessing systems under WLAN. The RFC4017 [29] is implemented in order to code EAP in our test environment with defined time-based performance parameters Following are discussion of result analysis obtained after implementing the algorithm.

### C. Analysis Strategy

In order to perform analysis, the proposed model initiates with the different numbers of network validator (2-7) and user devices (1-10) over the simulator area. The complete analysis was carried out over 500-1000 iteration considering different forms of user characteristics. In order to keep the analysis simple, the presence of any 5 random user characteristics are considered. Different characteristics assumed for this purpose are dynamic position of user device, priority assigned to user device, different form of sub-networks, various edges, assignment of an intermediate node in order to construct multihop. However, the value of user device characteristics could be further increased or decreased based on any upcoming future security demands and computational needs. The computation of the authentication time is carried out by fixing the position of base station as well as network validator while arbitrarily keeping the user device mobile between the access points of WLAN and base station of CDMA network. The compilation of the proposed logic was carried out on 32 bit core-i3 processor in windows platform. Hence, a very simple strategy was maintained in order to check that applying of public cryptographic techniques doesn't really adversely affect the authentication time. The prime agenda is to check for lightweight features of proposed authentication scheme while performing vertical handoff.

### D. Comparative Analysis

The outcome shown in Fig.8 highlights that proposed system offers faster response for secret key generation in less than 1.5s in presence of 5 different user's device characteristics. The prime reason for this trend of proposed system is that the generation of the private key by the base station takes place in random order corresponding to the group of user device characteristics. Moreover usage of hash function on the cut-off value also results in minimization of size of the storage resulting in less complexity from computational operation. On the other hand, the existing system of EAP-TLS was not found to cater up the lower time demands for generating secret keys. Although, with increase of number of user device characteristics there is a decrement of time for key generation for EAP TLS, but it is comparatively higher than proposed system whose trend is quite predictably linear.

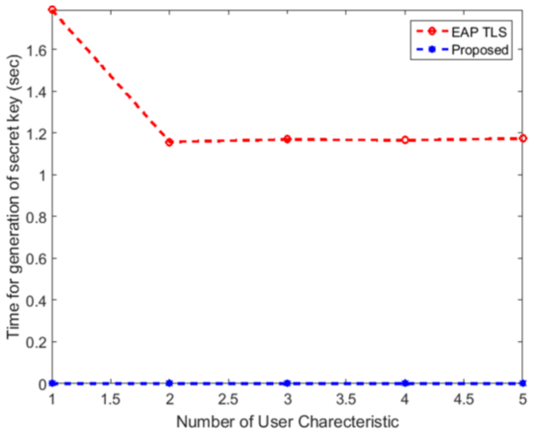


**Fig. 8** Comparative Analysis of Time for generation of Secret Key (y-axis)

This trend of time consumption for key generation for proposed system has various inference viz. i) it is quite deterministic in nature owing to its less occurrences of variances in its peak in time and hence its time factor is quite reliable as compared to existing system, ii) lower and static trend of time consumption also shows the scalability capacity of proposed system where uniformity of the performance (i.e. key generation time) is found never effected even by increase of random values of user characteristics, and iii) the outcome also shows a good supportability to the next part of the algorithm following key generation i.e. encryption and decryption. Hence, a uniform and minimized consumption trend of time for key generation significantly contributes towards faster authentication time.

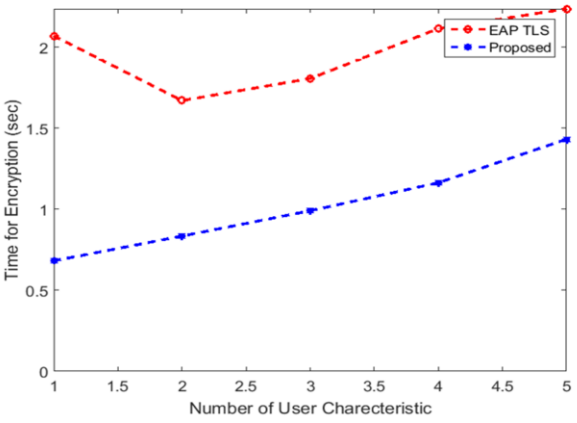


**Fig. 9** Comparative Analysis of encryption

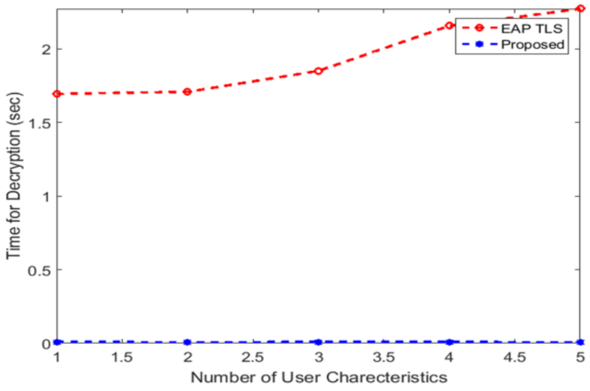


**Fig. 10** Comparative Analysis of Decryption Time

In order to construct a fast authentication scheme, it is essential to ensure that encryption process doesn’t consume much time. The outcome of encryption performance time in Fig.9 shows that there is an increase in encryption time with increase of number of user device characteristics. However, there is a less fluctuation of encryption time for proposed system as compared to existing EAP-TLS. The prime reason behind this is the presence of network validator node eases the work of authentication as it maintains and accesses complete information of trusted list TL from the base station upon receiving any form of request from any node. This results in significantly faster encryption process. This process also minimizes the mutual authentication time that conventionally exists between any two communicating nodes. Hence, migration becomes faster while performing vertical handoff with approximately 20-30% improvement in encryption time in presence of any form of dynamic traffic condition with in WLAN or in CDMA network system. Normally, there is no much significant difference between encryption and decryption performance time. But a closer look into the outcomes shown in Fig.9 and Fig.10 will show that proposed system has minimized decryption more than the encryption time. There is a solid reason for this as normally the decryption technique has specific criteria that are generally initiated during the roaming process of the user device. The dependency of decryption operation is the encrypted information $I_{\text{enc}}$ and secret key $\phi_{\text{pr}}$. The complete decryption process actually uses only one major process which is to check if the group of user device characteristics matches with the structure of the access right organization. After the response of the encrypted information is forwarded back to the network validator, later checks for its legitimacy. The authorization is only offer after the disclosure of positive legitimacy. The computation of response of the encrypted information is carried out by concatenating time stamp with an arbitrary key and further subjecting it to hash function. This process not only makes the decryption faster but potentially contributes to minimizing authentication time. Hence, a fair authentication time is a combination of cumulative time encapsulated in time to generate key, encryption and decryption time respectively.

### E. Security Analysis

In this section, the security potentials of proposed system are briefly analysed apart from the established faster authentication time. The proposed system is found to be robust against any intrusion arising from *rogue access points*. The encrypted information is transmitted from the network validator to the user device by the access point in WLAN. It is already known by now that public secret key is required to perform encryption for the information to be forwarded and the trusted networking domain is only assigned this public secret key. Hence, it is not feasible for any existing access point to become rogue or any rogue access point. Apart from this, the proposed system is also resistive against a rogue user device. It is because a user device must be capable of decrypting the encrypted message if it wants to experience the roaming privilege by the base station. If any user device becomes rogue, by any chance, then it will not be assigned private key by the network validator as the rogue user device will have chance in its characteristics that are not updated in *enroll* list. Similarly, the proposed system is also resilient against any form *eavesdropping attack*. It is because once the system performs successful authentication during the roaming process the complete wireless traffic system with edges subjected to encryption with an aid of arbitrary secret keys. Hence, there is no possibility of any external information to breach inside the secure channel or any possibility of leakage of encrypted information to other nodes inspite of destined nodes. The proposed system is also resilient against collusion attack as well as denial-of-services. Hence, the proposed system offers a robust mechanism to resists against multiple forms of attacks just by using the same authentication principle with faster vertical handoff operation.

## VI. CONCLUSION

The proposed study has offered a novel solution towards secure communication scheme by the means of secure handoff mechanism during migration of mobile user from WLAN to CDMA networks. The significant contribution of the proposed system is i) the system offers cumulatively 20-30% improvement in encryption time and approximately 75-80% of decryption time in contrast to existing EAP protocol, ii) The complete mechanism of encryption is designed using less number of iterative steps and more number of progress steps that results in lowering of storage complexity too along with minimal time complexity, iii) with the introduction of unique characteristics of user device, the proposed system performs encryption on the access right organization to offer maximum coverage of security to the entire topology in spite of securing only communicating nodes. Hence, the proposed system is found to offer a good balance between network security and faster authentication principle.

The future work will be in the direction of enhancing the speed of vertical handoff between WLAN and CDMA network considering decision delay and optimize the utilization of maximum radio resources for further minimizing the authentication delay.

## REFERENCES

1. K. J. Kim, N. Joukov, Mobile and Wireless Technologies, Springer, 2017
2. E. Hossain, M. Rasti, L. Bao Le, Radio Resource Management in Wireless Networks: An Engineering Approach, Cambridge University Press, 2017
3. A. Ahmed, L. M. Boulahia and D. Gaiti, "Enabling Vertical Handover Decisions in Heterogeneous Wireless Networks: A State-of-the-Art and A Classification," in IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 776-811, Second Quarter 2014.
4. D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," in IEEE Access, vol. PP, no. 99, pp. 1-1.
5. A. Mahmood, H. Zen, A. K. Othman and S. A. Siddiqui, "An optimized travelling time estimation mechanism for minimizing handover failures from cellular networks to WLANs," 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF), Harbin, 2015, pp. 28-33.
6. H. F. Zmezm, S. J. Hashim, A. Sali K. A. Alezabi, “Pre-Authentication Design for Seamless and Secure Handover in Mobile WiMAX”, International Review on Computers and Software, vol.10, No.7,2015
7. D. Gong and Y. Yang, "On-Line AP Association Algorithms for 802.11n WLANs with Heterogeneous Clients," in IEEE Transactions on Computers, vol. 63, no. 11, pp. 2772-2786, Nov. 2014.
8. S. Pack and Y. Choi, "Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems", Communications IEE Proceedings, Vol. 151, Issue 5, Aug. 2004 pp. 489-495.
9. A. Mishra, et al., "Proactive Key Distribution Using Neighbor Graphs", IEEE Wireless Communications, Vol. 11, Issue 1, Feb. 2004 pp. 26-36.
10. T. Yang, R. Zhang, X. Cheng and L. Yang, "Graph based resource allocation for physical layer security in full-duplex cellular networks," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.
11. Y. Suga, "SSL/TLS Status Survey in Japan - Transitioning against Renegotiation Vulnerability and Short RSA Key Length Problem," 2012 Seventh Asia Joint Conference on Information Security, Tokyo, 2012, pp. 17-24.
12. T. Feller, Trustworthy Reconfigurable Systems: Enhancing the Security Capabilities of Reconfigurable Hardware Architectures, Springer, 2014
13. Hemavathi and S Akhila. Article: An Insight towards Trends and Effectiveness of Vertical Handoff Mechanism. Communications on Applied Electronics 4(5):35-41, February 2016. Published by Foundation of Computer Science (FCS), NY, USA
14. B. Zhang, X. Wen, Z. Lu, T. Lei and X. Zhao, "A fast handoff scheme for ieee 802.11 networks using software defined networking," 2016 19th International Symposium on Wireless Personal Multimedia Communications (WPMC), Shenzhen, 2016, pp. 476-481.
15. K. R. Bose and K. K. K. Hari, "Mobile Information Centre -- An Approach to Fast Handoff," 2011 International Conference on Ubiquitous Computing and Multimedia Applications, Daejeon, 2011, pp. 60-62.
16. X. Chen and D. Qiao, "HaND: Fast Handoff with Null Dwell Time for IEEE 802.11 Networks," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.
17. M. S. Chiang, C. M. Huang and D. D. Tuan, "Fast handover control scheme for multi-node using the group-based approach," in IET Networks, vol. 4, no. 1, pp. 44-53, 1 2015.
18. S. Ryu, K. J. Park and J. W. Choi, "Enhanced Fast Handover for Network Mobility in Intelligent Transportation Systems," in IEEE Transactions on Vehicular Technology, vol. 63, no. 1, pp. 357-371, Jan. 2014.
19. Z. Yan and J. H. Lee, "State-Aware Pointer Forwarding Scheme With Fast Handover Support in a PMIPv6 Domain," in IEEE Systems Journal, vol. 7, no. 1, pp. 92-101, March 2013.
20. A. Fu, Y. Zhang, Z. Zhu and X. Liu, "A Fast Handover Authentication Mechanism Based on Ticket for IEEE 802.16m," in IEEE Communications Letters, vol. 14, no. 12, pp. 1134-1136, December 2010.
21. L. S. Lee and K. Wang, "Design and Analysis of a Network-Assisted Fast Handover Scheme for IEEE 802.16e Networks," in IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 869-883, Feb. 2010.
22. I. Im and J. Jeong, “Cost-Effective and Fast Handoff Scheme in Proxy Mobile IPv6 Networks with Multicasting Support”, Mobile Information Systems, vol.10, Issue 3, pp. 287-305, 2014
23. C-F. Wu, “Research Article A Handoff Algorithm of Dynamic Decisions with Extenics for Wireless Cellular Networks”, Journal of Electrical and

Computer Engineering, pp. 5, 2010

24. K. H. Chi, Y. C. Shih, H. H. Liu, J. T. Wang, S. L. Tsao and C. C. Tseng, "Fast Handoff in Secure IEEE 802.11s Mesh Networks," in IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 219-232, Jan. 2011.
25. Y. Deng, G. Wang, J. Cao and X. Xiao, "Practical secure and fast handoff framework for pervasive Wi-Fi access," in IET Information Security, vol. 7, no. 1, pp. 22-29, March 2013.
26. M. C. Chuang, J. F. Lee and M. C. Chen, "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks," in IEEE Systems Journal, vol. 7, no. 1, pp. 102-113, March 2013.
27. Y. Yan, Y. Qian and R. Q. Hu, "A Novel Channel Probing/Scanning Scheme for Secure Fast Handoff in IEEE 802.11-Based Wireless Networks," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston, TX, USA, 2011, pp. 1-6.
28. Y-F. Ciou, F-Y. Leu, Y-Li Huang, and K. Yim, “A Handover Security Mechanism Employing the Diffie-Hellman Key Exchange Approach for the IEEE802.16e Wireless Networks”, Mobile Information Systems, vol. 7, pp. 241-269, 2011
29. https://www.ietf.org/rfc/rfc4017.txt

## AUTHORS PROFILE

**Hemavathi,** received her Bachelors in Electronics and Communication Engineering in the year 2000 from Adi Chunchanagiri Institute of Technology, Kuvempu University and her Masters in Digital Communication Engineering from Acharya Institute of Technology, Visvesvaraya Technological University (VTU), India in the year 2012. She is currently working towards her Ph.D degree at B M S College of Engineering, Bangalore, India. She is working as a Assistant Professor at AMC Engineering College in the department of Electronics and Communication Engineering. She is a life member of Indian Society for Technical education (ISTE) since 2018. She has published papers in 4 International Journals, 1 International Conference and 4 National conferences.

**Dr. Akhila. S** received her Bachelors in Electronics in the year 1988 and her Masters in Electronics in the year 1994 from University Visvesvaraya College of Engineering, Bangalore, India. She has completed her Ph.D. in the year 2013 from the Visvesvaraya Technological University (VTU) in Wireless Communication. Since 1995, she has been with B M S College of Engineering, where she is working as a Professor in the Electronics and Communication Engineering Department. She is a life member of Indian Society for Technical education (ISTE). She has published papers in more than 4 National conferences, 6 International Conference and 25 International Journals.