FAVH: A Novel Technique of Faster Authentication in Vertical Handoff in WLAN and CDMA Network

Hemavathi[1], S. Akhila[2]
[1]Dept. of ECE, AMCEC
Bangalore, India
[2]Dept. of ECE, BMSCE,
Bangalore, India

Abstract— Incorporation of complex cryptographic protocol calls for more recursive encryption which degrades the handoff mechanism in heterogeneous wireless network. After reviewing the existing literatures about the handoff with respect to security and fast authentication protocols, various problems have been surfaced that loses to keep sustainable balance between security and handoff delay. Hence, this paper proposes a novel approach called as FAVH or Fast Authentication in Vertical Handoff which uses a dynamic feature-based encryption mechanism during the handoff between Wireless Local Area Network (WLAN) and Code Division Multiple Access (CDMA) network. The study outcome shows FAVH outperforms the most frequently used Extensible Authentication Protocol using Transport Layer Security (EAP-TLS) with respect to key generation time, encryption time, decryption time and computational complexity.

Keywords- Vertical Handoff, Heterogeneous Wireless Network, Security, WLAN, EAP, Handoff Delay

1. INTRODUCTION

Basically, handoff mechanism can be stated as a technique to ensuring that a mobile node stay connected when they move out from transmission range of one access point and move in to the range of new access points. This is the only mechanism to extend the coverage and connectivity services in the area of mobile networks [1][2]. The entire process of handoff takes place in three stages. In the first stage, a network agent or a user (i.e. mobile device) or a network with changing condition should initiate handoff. In the second stage, there is a generation of novel connectivity from different access point. In this stage, the new resources in the new connection should be explored in order to get the mobile node connected in new networking group. In the third stage, the data packet flows from prior to new network group depending upon the allocated privilege of the user. Theoretically, there are two types of handoff viz. horizontal handoff in homogeneous network and vertical handoff in heterogeneous network [3]. The prime reason of horizontal handoff is because of lowered signal strength while the reason for vertical handoff is due to the mobility of the user. Vertical handoff may also occur when the user chooses to select another network for getting the services [4]. However, different from theory, the next generation of wireless network encounters significant level of challenges due to i) demands of increased QoS, ii) communication overhead, iii) optimization of network usage, iv) trust worthiness etc. [5]. However, in this entire demanding success factor, there is one common thing, which is authentication. It is a process by which the newly entering node in new network group must be authenticated to each other. As there are various forms of rogue access points posing a significant security threats to the mobile nodes, it is necessary for both the access points as well as mobile nodes to get authenticated to each other [6]. During authentication, a mobile node furnishes their factors of authentication to the server in order to get it verified. In case of positive verification, the user is provided with access to the privileged resources. It is highly important that a WLAN to validate the incoming mobile nodes and generate a highly secured communication channel with all the mobile nodes complying the standard of IEEE 802.11. Normally, a WLAN uses some security standard called as WEP (Wireless Equivalent Privacy), WPA (Wi-Fi Protected Access), TKIP (Temporal Key Integrity Protocol), etc [7]. Unfortunately, all these standards are not 100% secured [8] against majority of the lethal threats in wireless networks. This problem has substantially gained an attention from the research community where an extensive research work has been dedicated just to ensure security in WLAN. Various research techniques have been evolved in due course of time where mainly cryptography was a dominant player. Usage of cryptography is always safe and there is large number of potential cryptographic algorithm with wide ranges of security. Unfortunately, such implementation introduces a delay which cannot be tolerated during the handoff mechanism. Such delay significant affects not only the QoS factors but also give rise to potential security threats e.g. DoS. As majority of encryption and decryption

performed on wireless networking are based on public key-based approach, they are normally recursive in nature. Hence such operation always ensures a handoff latency and delay.

Although, there has been a significant level of research work being carried out minimizing handoff delay in heterogeneous network, but less work is found to keep a balance between delay and security potentials. Hence, this paper discusses about a solution to overcome such problems of delay and security in vertical handoff in heterogeneous wireless network. Section 2 discusses about the review of literature highlight contribution of prior researchers followed by problem identification after reviewing the existing system in Section 3. The proposed system is discussed in Section 4 followed by discussion of research methodology in Section 5. Discussion of algorithm implementation for proposed FAVH is carried out in Section 6 and result discussion in Section 7. Finally, the summary of the contribution is briefed in Section 8.

2. RELATED WORK

This section discusses about the existing techniques that has been introduced in the past for strengthening the vertical handoff mechanism. This section will update our findings from the prior review work [9]

Study towards Wireless Local Area Network (WLAN) security system has meet extensive research work in the past. One of the recent work carried out by Pandey et al. [10] have focused on presenting a unique authentication technique in WLAN using Extensible Authentication Protocol (EAP) in order to speed up the process of key delivery. The study outcome was compared with conventional system to find reduced delay in authentication. Similar direction of the work has also been carried out by Patkar and Ambawada [11] towards securing WLAN. The study has used EAP as well as Elliptical Curve Cryptography for generating keys during vertical handover between 3GPP networks to WLAN. The study outcome was found to posses minimal consumption of channel capacity as well as successfully reduce delay upto 9.56% compared to existing system. Zhu et al. [12] have also presented a technique of securing WLAN infrastructure using authentication mechanism. The study has presented a certificate-based policy where a digital certificate was utilized to sign the transacted messages in WLAN. The certificate was used to authenticate the server and user's identity. However, the exact implementation and analyzed outcomes are not much discussed in this paper. Study towards WLAN security and authentication was also presented by Ali and Owens [13]. The study has discussed that existing security protocols exercised in WLAN are not safe enough and recommended more level of security features to be incorporated e.g. authentication between server and user, computation of extraction of secure keys, protecting identity of user, faster mechanism of connecting to network, scalability etc.

Bassoli et al. [14] have presented a study that has discussed an authentication mechanism considering two different types of network i.e. WLAN and Evolved Packet System (EPS). The technique uses direct IP access strategies and security incorporations are carried out using homomorphic encryption. The encryption was carried out using different entities e.g. IMSI number, secret key, public key, identity, etc. The server extracts the identity of WLAN and an arbitrary number is generated in order support encoding. A random key is then computed by the route of the WLAN that assist the server in authentication process. Finally, the IMSI is encrypted by the WLAN using public key. It also uses message authentication code. Li et al. [15] have presented a robust protocol in order to meet the authentication in WLAN with faster response time. The technique presented by author has realized the distribution of authentication key using roundtrip control messages. Better than conventional handshaking based authentication, the presented technique was found to reduce delay while authenticating node in contrast to EAP based scheme of authentication. Hence, we find that usage of EAP-based scheme is frequently used. Another study presented by Fan et al. [16] have EAP-based authentication which majorly aims to fulfill the security demands of the WLAN with better assurity of minimal computational complexity and higher degree of forward secrecy. The study outcome was compared with other existing studies using EAP-based schemes to find competitive computational time for carrying out authentication. Study carried out by Bouabidi et al. [17] have presented a scheme that addresses security and speed problems related to authentication mechanism in WLAN network. The technique makes the authentication server to release a token that ensures the minimization of communication between two nodes by reducing the quantity of the tickets sent. The outcome of the study was assessed using handover latency, blocking probability, packet loss rate, etc. Lopez et al. [18] have developed a technique to ensure faster authentication by using Kerberos protocol in heterogeneous wireless network. The technique doesn't need any alteration or change in the existing wireless technology in order to implement it. The authors have implemented it on a real-time experimental test bed using open source application to implement Kerberos protocol. The outcome of the study was assessed with respect to existing EAP based authentication to find that presented technique offers better resiliency and faster vertical handoff operation over wireless networks.

Study towards authentication mechanism of CDMA network was presented by Ramadan et al. [19]. The authors have presented a unique key agreement protocol for strengthening the mutual authentication system. The study implements a simple key agreement protocol and used bilinear maps as a part of signature computation and generation of session keys. Study on similar direction was carried out by Venkaatsubramanian et al. [20]; however, the focus was more on security against physical attacks. According to the techniques, a request beacon is forwarded for joining the network with an aid of symmetric key. This

beacon is encrypted by message authentication code and then it is forwarded to neighbor nodes. The technique allows dual encryption level in order to protect integrity and confidentiality in physical and data link layer. Deng et al. [21] have presented a scheme that is meant for faster and secured handoff mechanism on WLAN (802.11i). The study intends to minimize delay during handoff authentication. Chi et al. [22] have presented an approach of authentication between mesh networks to minimize the cost of handoff. Implemented over analytical and simulation modelling, the study outcome was tested for minimal handoff delay. Qachri et al. [23] have developed a security scheme in 4G network to perform vertical handoff. The authors have presented a scheme where they have used signaling factor in order to alter the meta-protocol. The presented technique has validated the model using a standard cryptographic verifier. Yan et al. [24] have presented a technique of secure handoff mechanism in order to minimize the channel probing delay using the channel condition. Ganan et al. [25] have discussed another secure hand off mechanism in vehicular adhoc networks. The authors have carried out a simulation based study considering PHY and MAC parameters in wireless standard of 802.11p. The study outcome was found to be better than existing system as compared with existing handoff schemes with respect to throughput, packet delivery ratio, and handoff disruption time. Hence, it can be seen that there are sufficient level of work being carried out with respect to secure handoff mechanism with faster authentication. The next section discusses about the problems being identified from the review.

3. PROBLEM IDENTIFICATION

This section discusses about the problems that have been identified after reviewing the existing research work. The problems are briefed as follows:

- **Problems in EAP-based solution**: It has been observed that majority of the schemes for handoff in WLAN has used EAP-based solution. The biggest problem about this technique is that it has higher number of message exchanges between the user and the server, which is considerably a time consuming process. Apart from it, there is also a higher dependence of more number of EAP messages between user and server making it further slow. This will also call for joining the server in the network resulting in further propagation and authentication delay.
- **Overlooking flaws in WLAN security**: It is already known that WEP (Wireless Equivalent Privacy) is the frequently used security protocol in WLAN authentication system and is already shrouded by various security issues. Normally, the research work towards secure vertical handoff mechanism has not considered the inherent problems associated with WLAN e.g. open authentication, shared key-based authentication, mutual authentication, etc. Apart from this, another significant problem is ignoring the fact that existing security technique doesn't address the problem of access control using mutual authentication between the user and the router in WLAN.
- **Less Work in Data Privacy**: A typical security algorithm is hard to find in existing research work focusing on vertical handoff between WLAN and CDMA networks. There are few of the existing studies that do address this problem. The existing techniques focus on implementing complex cryptography on horizontal handoff scheme, which doesn't solve the purpose when it comes to heterogeneous wireless network. Hence, existing studies doesn't emphasize on data privacy considering the problem of vertical hand off schemes.
- **Approaches are less Computational complex**: It should be known that majority of the wireless nodes operating on any kinds of wireless network are consistently draining its resources in order to get connected. Hence, there is no single literature to discuss the suitability of the existing algorithm in optimizing the resource utilities. Handoff mechanism in order to be faster will require an algorithm to work almost instantaneous, which is not the case in existing literatures.

Hence, it has been seen that although there are many studies designed towards addressing the security problems in vertical handoff between WLAN and CDMA networks. Both WLAN and CDMA network has different process of getting authenticated, where the existing cryptographic algorithm doesn't emphasize on exploring new parameters or entities that can possibly reduce the authentication delay. Hence, the problem statement can be – "It is a challenging task to retain a better balance between superior security and faster authentication in the vertical handoff considering WLAN and CDMA".

4. PROPOSED SYSTEM

The prime purpose of the proposed system is to present a novel authentication mechanism for supporting faster mechanism of vertical handoff and thereby minimize authentication delay. The study has adopted an empirical approach that introduces a new schema or technique of vertical handoff mechanism. However, the main focus of the design was to incorporate security using feature-based encryption as it is essential to implement security features in the vertical handoff mechanism. The proposed architecture of this design phase is shown in Fig.1.

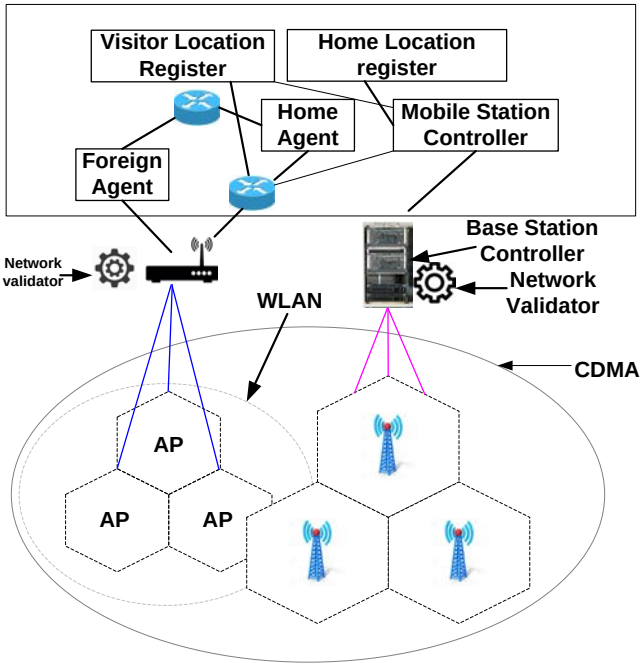

Figure 1 Proposed Architecture of Fast Authentication Mechanism

The design of the proposed security system is meant for vertical handoff between WLAN and CDMA system. The study considers a special entity called as network validator who is responsible for validating the legitimacy of any node or network or services during the roaming mode. Different from conventional security measures, the proposed system uses *feature*-based encryption, where *feature* represents certain parameters of a node whose values keeps constantly on changing within a certain limit. To make the authentication schema computationally efficient, a simple tree-based theory was adopted just to formulate the security policies. The prime intention is to ensure the faster handoff mechanism without much delay when a node travels in foreign network. The technique uses public key, a security policy, and message as an input that results in performing encryption. The novelty of proposed system is that an encrypted code consists of authorization to the receiver node to perform decryption if they have access to same security policy. Compared to existing system using complex cryptography, proposed FAVH offer simple and very lightweight key management in order to ensure a good balance between robust key management and faster authentication. The next section discusses about the research methodology that has been adopted.

5. Research Methodology

The prime basis of the proposed research work is based on the fact that every wireless network will execute some sort of security algorithm in order to perform node authentication. Such authentication needs to be performed when one mobile node moves from its home network and enter into foreign network. The process of invoking security protocols in homogeneous handoff mechanism are less complicated; however, it is not the same in vertical handoff mechanism due to differences in routing process and adherence to different IEEE standard. The proposed system is however considering two different types of network groups i.e. WLAN and CDMA, where the problem is to generate Faster Authentication Vertical Handoff (FAVH) scheme. This section will present the mechanism adopted to develop FAVH.

Fig.2 highlights the pictorial representation of FAVH that aims to perform uninterrupted vertical handoff mechanism between WLAN and CDMA network without any dependence of neighbor key predistribution. The novelty as well as contribution of the proposed system is that it uses a specific term called as feature which is deployed for performing faster handoff authentication. The methodology adopted for designing feature-based encryption is based mainly on cryptographic usage on public keys. The novelty of the approach is that-in conventional cryptography the frequently used schemes in vertical handoff are i) a public key from the receiver is utilized for ciphering the message and ii) altering the public key utilized in the form of random strings viz. name of user, email ID, etc (used in Identity-based schemes). However, FAVH scheme uses a kind of hybridizing between these two techniques where such node identities are not used directly but it extracts certain features of them that keep on changing dynamically e.g. speed, transmission range, position etc. The technique allows encryption of message only using subset of such features or be defining security policies over a set of features. The scheme considers that a base station in CDMA network (or trusted authority) issues a key to the user in order to perform decryption of the message. The proposed scheme associates the private key of the user with the set of feature where the encrypted message actually represents a policy of accessing the network over a defined range of features. The successful decryption occurs only when the features are satisfied by the security policy embedded in the encrypted message. Different kinds of mathematical operation are possible to define the security policies. A simple mechanism adopted in FAVH scheme is shown in Fig.2. The pictorial representation shows only 4 numbers of features {i.e. Speed, Transmission range, Number of neighbor, and Position}. Therefore, according to the security policy imposed, the user will be permitted to perform decryption. Interesting point to be noted here is when any one of the user is performing decryption, other user will not be able to perform decryption under the same security policy. Therefore, proposed FAVH discretize the handoff authentication where the authorization is already embedded within the encrypted message. Another interesting point is the security policy may be accessible by other legitimate nodes, but only the node who has received authorization policy (through encrypted data) are only permissible to decrypt it. The technique also provide substantial amount of security as the private key is extracted from the encrypted message, which ensure better privacy factor too and faster authentication mechanism.

Hence, FAVH is a type of public key cryptography in true sense.

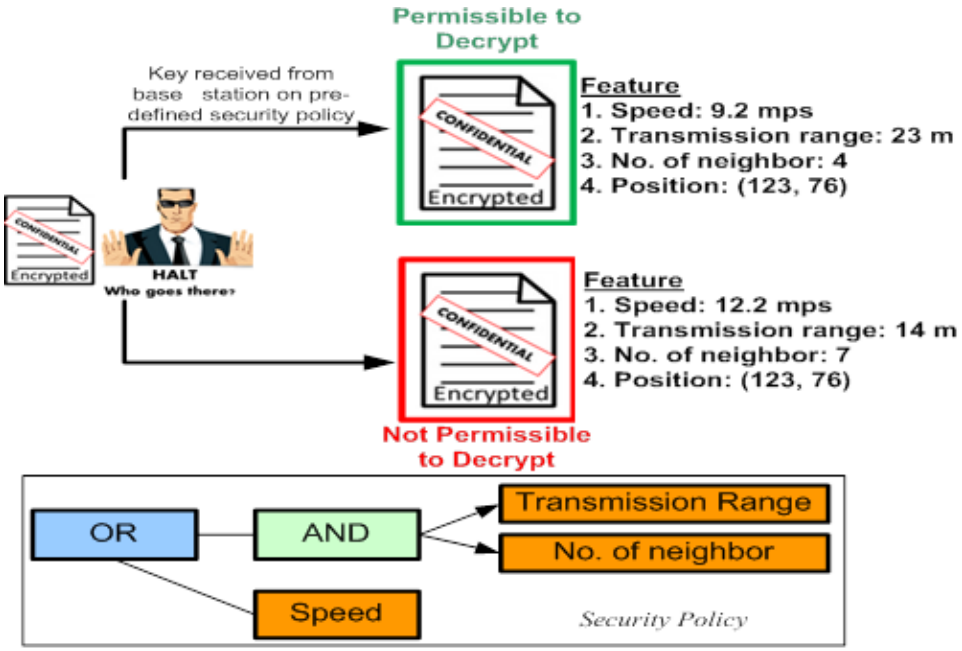

Figure 2 Proposed Scheme of Novel Authentication based faster vertical handoff

6. Algorithm Implementation

The algorithm aims for ensuring faster authentication process when a mobile users switches from WLAN to CDMA network. It should be noted that WLAN has a support of access points (or routers) and CDMA network has a support of base station. Following are the descriptive details of algorithms being implemented in this regards.

A. *Assumptions of Algorithm Design*

The study assumes that there is an entity by the name network validator Nval which is responsible for developing a scheme to gain an admission to the network using tree. Different from existing tree-based technique, this mechanism will consider leaf node represents parameters and non-leaf nodes to represents cut-off (or threshold) for admission towards networks. Hence, Nval will generate encryption scheme which could be permitted to be decrypted by device Ms only. For better applicability of the study, the device is assumed to have any secure authentication mechanism to be found executed in its home network. If the preliminary authentication is found successful that the system considers full authorization for the validator in home network to forward its identification details to the device in order to perform vertical hand off. The study also assumes possession of public key Kpu and private key Kpr with total rights of performing encryption being retained by network validator only. However, before to that, we also assume that each base station has already authenticated the network validator.

B. *Algorithm for Key Generation*

This algorithm is mainly responsible to maintain a better balance between vertical hand-off with higher security and faster process of authentication. Once the network validator Nval is found to be authenticated by the base station then a private key Kpr, a public key Kpu, and precedence of the network group will be allocated to each legitimate network group. An interesting point here is that the base station will release catalogued information of the legitimate network enrollment. The catalogued information of the legitimate network group is encrypted with simple encryption key. The algorithm allows the device to forward a beacon to the base station (Line-2). While forwarding the beacon, we consider it uses some secured communication link of the home network and the beacon consists of *positional information about the device, precedence value of the device, road, and landmark*. This algorithm for generation of the key is being carried out by the base station itself. The base station uses a unique technique in order to develop a public key K_{pu} and private key K_{pr}. After developing public key Kpu, it is flagged as available to all nodes while Kpr is not flagged to others. Along with this, a private key Kpr is also generated by the base station. The technique initially formulates an arbitrary value and represents a feature set along with correspondence generation of a random value against each feature to finally use Euler's

theorem for generating public key (Line-3) and main key η, where *g*, *a*, and *p* are random numbers . In a short, it can be also said that the base station executes this technique that considers the inbuilt key and a feature set to generate private keys. The base station will use the key generation technique using main key η and user-defined features φ in order to generate private key K_{pr} (line-4). In the next part of the algorithm, the base station forwards the private key along with the catalogued information of the legitimate network group to the device. Authentication token is done by encryption process of prior secret key. It (BS) also forwards the K_{pu} to the network validator N_{val}. Finally, it is the task of the network validator N_{val} to perform encryption using this key in order to allow further authorization. In order to perform encryption, the network validator generates a random key K_{ran} along with other two random numbers a and b (Line-6-7).

Algorithm for key generation in home network

Input: M_s (device/mobile station), BS (base station), N_{val} (network validator), η (main key), φ (user-defined features), k_{pr} (Private key), K_{pu} (public key)

Output: key

Start

1. Init M_s, N_{val}, BS.
2. $M_s \xrightarrow{beacon} BS$
3. $K_{pu} \rightarrow euler(g, a)^p$ & $\eta \rightarrow g^p$
4. $K_{pr} \rightarrow key(\eta, \varphi)$
5. $BS \rightarrow (K_{pr}, val\_list)$
6. $N_{val} \rightarrow gen(k_{ran}, a, b)$
7. $data_{enc} = encrypt(k_{ran}, (g, g)^p)$
8. $BS \rightarrow sign(data_{enc}:K_{pr}) = key$
9. Generates key

End

The network validator N_{val} applies signature over the encrypted data $data_{enc}$ with an aid of private key in order to finally generate key that can be used for authorizing the vertical handoff in foreign network (Line-8-9). The proposed algorithm considers that if the decrypted key is found matching with the connected features then only the device will be given access to resources in foreign network. The scope of this algorithm ends here when a node leaves the home network. The further security in the foreign network is assisted by next algorithm.

C. Algorithm for Authentication in Foreign Network.

This algorithm is mainly responsible for ensuring better authentication when the mobile node enters a foreign network. In this algorithm, the device initially forwards the validation request to the new network validator Nval of the new networking group (i.e. foreign network) (Line-1). The network validator then forwards the generated key (from prior algorithm) to the device in order to initiate authentication mutually among the two different networks (i.e. WLAN and CDMA) (Line-2). The algorithm uses simple encryption key in order to encrypt the public key (Line-3) that belongs to the network validator. The device then refers its catalogued information of the legitimate network group for all the new networking groups and correspondingly performs authentication. It applies some simple protocol for performing the authentication within the new domain to ensure faster hand-off mechanism of authentication. It simply checks if the encryption values of both the networks are same or different (Line-4). If both the encryption values are found to be same then only the authentication of the signature can be considered to be successful.

Algorithm for authentication in foreign network

Input: M_s (mobile station), BS (base station), N_{val} (network validator), η (main key), φ (user-defined features), k_{pr} (Private key), K_{pu} (public key)

Output: Signature validation

Start

1. $M_s \xrightarrow{Val\_REQ} new(N_{val})$
2. $New(N_{val}) \xrightarrow{key} M_s$
3. enc→encryption(k_{pub}(new(N_{val}))
4. If ($encryption_{home} \neq encryption_{foreign}$)
5. Abort validation
6. Else
7. Validated signature

End

Therefore, the above mentioned algorithms are executed within the device that takes the input of the encrypted code (generated from Line-3) as well as generated key from 1st algorithm. One of the interesting points about the algorithm is that its features keep changing based on the mobility of the node, which is beyond the reach of any intruder to guess. Finally, the device authorizes the users to use the services and everything happens within a fraction of time. The algorithm also forwards one acknowledgement to the network validator by concatenating random key and time stamp using any existing cryptographic encryption function.

7. RESULT DISCUSSION

This section of the paper discusses about the outcome accomplished from the proposed study implementation. The complete implementation has been carried out over Matlab. As the study is focused on secured and fast vertical handoff scheme, so handoff delay would be the better performance parameter to assess the effectiveness of outcome. However, for better analysis, we split the

conventional handoff delay parameter into more three parameters e.g. key generation time, encryption time, and decryption time. The study also considers comparing the outcomes with that of frequently used EAP authentication technique in WLAN. In duration of this assessment it was also checked for its backward and forward secrecy, algorithm processing time, computational complexity etc. All the performance parameters are checked with respect to increasing number of mobile station. Each mobile station represents number of nodes which is a primary source of query generation process. More queries by the user will results in increasing number of request for joining the network which will call for implementation of proposed authentication protocol. Fig.3 shows the trend of average key generation time, which is originally the successful computational of first algorithm discussed in previous section.

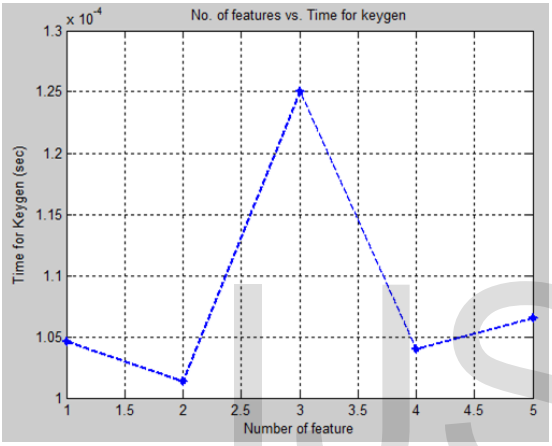

Figure 3 Analysis of Key Generation Time (s) in FAVH

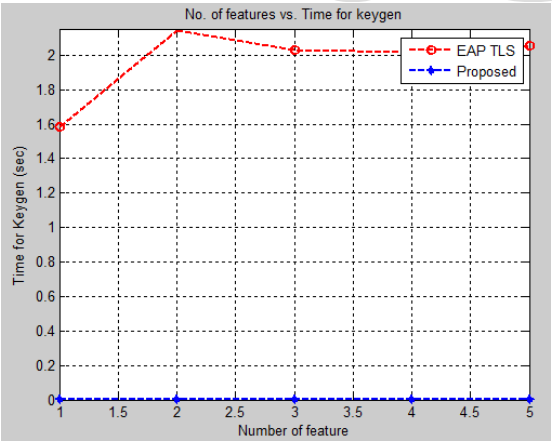

Figure 4 Comparison of Analysis of Key Generation Time (s) between FAVH and EAP-TLS

The outcome shows that proposed FAVH can generate the keys very fast as compared to conventional EAP-TLS techniques (Fig.4). The prime reason behind this outcome is that EAP-TLS doesn't address much of scalability issue. So with increase of nodes (i.e. MS) there is also an increase of mutual authentication between server and user resulting in increasing key generation time. However, proposed FAVH acts differently here. It performs its authentication using two things i.e. i) security policy and ii) encrypted code with authorization along with usage of encryption function.

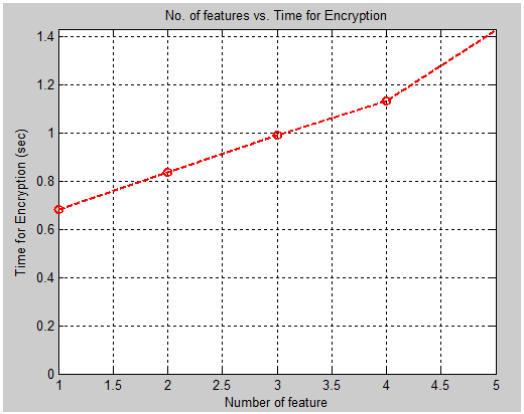

Figure 5 Analysis of Encryption Time (s) in FAVH

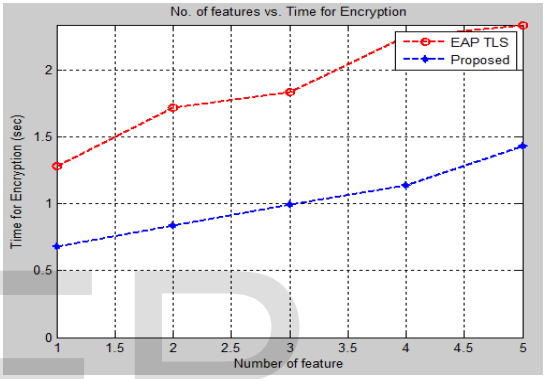

Figure 6 Comparison of Analysis of Encryption Time (s) between FAVH and EAP-TLS

As the mobile device gets its spontaneous updates there is a less probability of more delay for security protocol structure to reach the device. On the other hand, the complete encryption and decryption is governed by the network validator which resides in base station controller. Hence, node-to-node interaction time is reduced. Further usage of encryption key results in almost instantaneous generation of key. Hence, it is unlikely that FAVH is going to get affected by increase of number of nodes provided the total number of nodes also complies with the service capacity of a base station. This fact can also be reflected by the encryption time analysis in Fig.5, where it can be seen that there is a slight increase in encryption time from 0.65 to 1.4 seconds. The prime reason for this slight increase in time is because after the security policy is received by the node (as shown in Line-5 of first algorithm), the network validator has to generate a random number, which will be also used in data encryption (as shown in Line-6-7 of first algorithm) followed by digital signature (as shown in Line-8 of first algorithm). Hence, this operation give slide delay window of 1.4 seconds, which is still much better than conventional EAP-TLS approach (Fig.6).

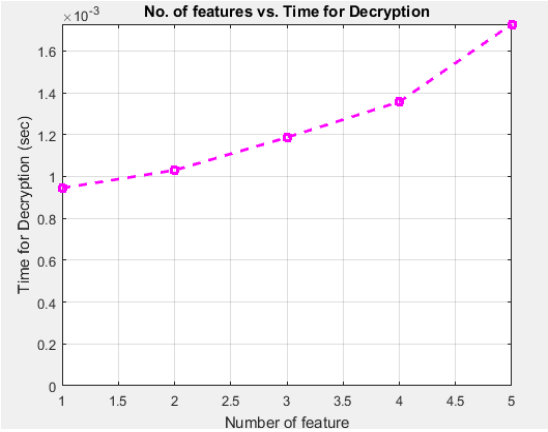

Figure 7 Analysis of Decryption Time (s) in FAVH

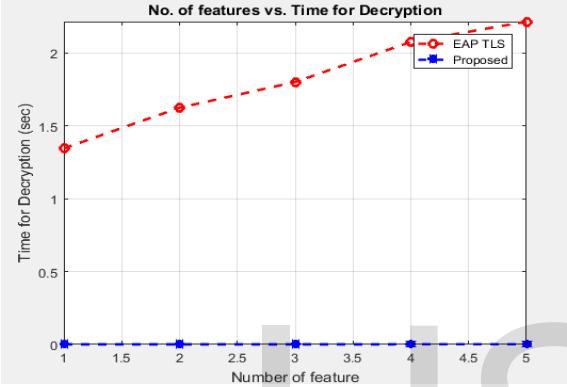

Figure 8 Comparison of Analysis of Decryption Time (s) between FAVH and EAP-TLS

Fig.7 shows the analysis of the decryption time. A closer look into the trend will show that there is a very minor increase in the decryption time in the range of 0.95-1.65 seconds, which is faster than encryption time. Moreover, the trend doesn't have gradient ascent pattern. This fact easily means that the proposed algorithm exhibits the properties of non-repudiation towards the communication, which is one of the essential properties of security protocols along with privacy and integrity. The complete algorithm takes roughly around 2.745seconds to execute over core i3 processor with 4 GB RAM. Change of operating environment will only impact 5-8% of the overall performances of the algorithm. The size of the key is maintained 128 bit, but the framework is highly flexible to check for other key sizes too. Apart from memory occupied by the key, the algorithm works in dynamic way which means it doesn't generate any memory for any form of other storage while performing encryption. These mechanisms are not only secured but also have higher supportability of low-powered embedded devices too. Hence, usage of the algorithm is highly recommended for laptops, smartphones, PDA, etc on any configuration of WLAN and CDMA networks.

8. Conclusion

This paper has discussed about the secured and fast authentication mechanism for vertical handoff between WLAN and CDMA network. Different from the existing mechanism of complex approach of authentication, the complete focus of the algorithm design was to use lesser degree of complex cryptography and more usage of sustainability logic. Implementation of the proposed technique allows the sender node to perform encryption of the data to any network group of their choice. Secondly, only the intended networking group will be able to perform decryption of the routed message. At present, any form of security algorithms are mainly meant for resisting one kind of attacks only. This problem is addressed in proposed system by enabling a node to deploy their own security policies against different forms of destination nodes. It will mean that now a single node can formulate attack resistance strategy by deploying more dynamic security protocols which can address and overcome the flaws of inbuilt security systems in WLAN (e.g. WEP, WPA, TKIP, etc). The study outcome is found to posse's better performance over handoff latency as compared to existing approach.

References

[1] S. Glisic, Advanced Wireless Networks: Technology and Business Models, John Wiley & Sons, 2016

[2] M. Ismail, W. Zhuang, Cooperative Networking in a Heterogeneous Wireless Medium, Springer Science & Business Media, 2013

[3] Lagkas, Thomas D, Wireless Network Traffic and Quality of Service Support: Trends and Standards: Trends and Standards, IGI Global, 2010

[4] A. Kumar, B. Xie, Handbook of Mobile Systems Applications and Services, CRC Press, 2016

[5] M. F. Finneran, Voice Over WLANS: The Complete Guide , Newnes, Technology & Engineering - 400 pages, 2011

[6] C. Makaya, Samuel Pierre, Emerging Wireless Networks: Concepts, Techniques and Applications, CRC Press, 2012

[7] M. Khasawneh, I. Kajman, R. Alkhudaidy, A. Althubyani, "A Survey on Wi-Fi Protocols: WPA and WPA2", *Springer- Recent Trends in Computer Networks and Distributed Systems Security*, Volume 420 of the series Communications in Computer and Information Science pp 496-511, 2014

[8] Y. Zou, J. Zhu, X. Wang, L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", *Proceedings Of The IEEE—arXiv*, 2016

[9] Hemavathi, S. Akhila, "An Insight towards Trends and Effectiveness of Vertical Handoff Mechanism", *IEEE Communications on Applied Electronics*, Vol.4, No.5, February 2016

[10] A. Pandey, P. K. Pant, R. C. Tripathi, "A System and Method for Authentication in Wireless Local AreaNetworks (WLANs)", *Springer Journal, Proceedings of National Academic Science*, 2013

[11] S. S. Patkar, D. D. Ambawade, "Secure 3GPP-WLAN Authentication Protocol Based on EAP-AKA", *IEEE International Advance Computing Conference*, pp.1011-1016, 2015

[12] W. Zhu, L-F Kwok, "A Secure and Flexible WLAN Authentication Scheme for Organizations", *International Conference on Information Science and Security*, pp.1-4, 2015

[13] K. M. Ali, T. J. Owens, "Access Mechanisms in Wi-Fi networks State of Art, Flaws and Proposed Solutions", *International Conference on Telecommunications*, pp.280-287, 2010

[14] R. Bassoli, H. Marques, J. Rodriguez, C. Gruet and R. Tafazolli, "Enhanced authentication for WLAN–EPS interworking systems", *IEEE- Electronics Letters*, Vol. 51, No. 19, pp.1544–1546, 2015

[15] X. Li, F. Bao, S. Li, and J. Ma, "FLAP: An Efficient WLAN Initial Access Authentication Protocol", IEEE Transactions On Parallel And Distributed Systems, vol. 25, no. 2, February 2014

[16] C.I Fan, Y.H. Lin, and R. H. Hsu, "Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs", *IEEE Transactions On Parallel And Distributed Systems*, Vol. 24, No. 4, April 2013

[17] I. El Bouabidi, F. Zarai, M. S. Obaidat and L. Kamoun, "Fast and Secure Handover into Visited WLAN Networks", *Springer- Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering*, 2013

[18] R. M. Lopez, F. P. Garcia, Y. Ohba, F. B. Hidalgo, A.F. Gomez, "A Kerberized Architecture for Fast Re-authenticationin Heterogeneous Wireless Networks", Springer- Mobile Netw Application, vol.15, pp.392–412, 2010

[19] M. Ramadan, F.Li, C.X. Xu, K. Oteng, H. Ibrahim, "Authentication and Key Agreement Scheme for CDMA Cellular System", *IEEE International Conference on Communication Software and Networks*, pp.118-124, 2015

[20] Venkatasubramanian S. and Jothi V., "Integrated Authentication and Security Check With CDMA Modulation Technique in Physical Layer of Wireless Body Area Network", *International Conference on Computational Intelligence and Computing Research*, 2012

[21] Y. Deng, G. Wang, J. Cao, X. Xiao, "Practical secure and fast handoff framework for pervasive Wi-Fi access", *IEEE- Trust and Identity Management in Mobile and Internet Computing and Communications, IET Information Security*, 2012

[22] K-H Chi, Y-C Shih, H-H Liu, J-T Wang, "Fast Handoff in Secure IEEE 802.11s Mesh Networks", *IEEE Transactions On Vehicular Technology*, Vol. 60, No. 1, January 2011

[23] N. Qachri1, O. Markowitch, and J-M Dricot, "A Formally Verified Protocol for Secure Vertical Handovers in 4G Heterogeneous Networks", *International Journal of Security and Its Applications*, Vol.7, No.6, pp.309-326, 2013

[24] Y. Yan, Y. Qian, R. Q. Hu, "A Novel Channel Probing/Scanning Scheme for Secure Fast Handoff in IEEE 802.11-based Wireless Networks", *Computer & Electronics Engineering Faculty Publications.* Paper 97, 2011

[25] C. H. Ganan, S. Rene, J. M. Tapia, "Secure Handoffs for V2I Communications in 802.11 Networks", *Proceedings of the 10th ACM symposium on Performance evaluation of wireless ad hoc, sensor, & ubiquitous networks*, pp.49-56, 2013