Wireless Pers Commun (2017) 94:2645–2664
DOI 10.1007/s11277-016-3877-5

User Path Prediction Based Key Caching and Authentication Mechanism for Broadband Wireless Networks

Rajakumar Arul[1] · Gunasekaran Raja[1] · Kottilingam Kottursamy[1] · Pavithra Sathiyanarayanan[1] · Swaminathan Venkatraman[1]

Published online: 10 November 2016

Abstract Broadband wireless networks namely wireless interoperability for microwave access and long term evolution utilizes the EAP and EPS mechanisms for authentication. However, these mechanisms incur considerable delay during handoffs. This delay during handoffs results in service disruption which becomes a severe bottleneck. To overcome this delay, our article proposes (UPP-KC) a key caching mechanism based on user path prediction. If the user follows the predicted path, he/she bypasses the normal authentication mechanism and obtains the necessary authentication keys directly. Through analytical and simulation modeling, we have proved that our mechanism effectively decreases the handoff delay, thereby achieving fast authentication without compromising on the security standards.

Keywords LTE · WiMAX · Handoff · Authentication · EAP and pattern mining

✉ Rajakumar Arul
rajakumararul@gmail.com

Gunasekaran Raja
gunamit@annauniv.edu

Kottilingam Kottursamy
k.kottilingam@gmail.com

Pavithra Sathiyanarayanan
pavikkdi@gmail.com

Swaminathan Venkatraman
santuv92@gmail.com

[1] Department of Computer Technology, Anna University, Chennai, Tamil Nadu, India

1 Introduction

Wireless broadband networks have emerged as a promising wireless technology due to their high data rate [1], wide coverage, low cost and built in support for mobility [2, 3]. In spite of all the advantages, there are numerous security issues which may result in deployment challenges. A significant security aspect is an authentication. WiMAX and LTE-A offer a flexible means for authenticating Subscriber Stations and users to protect against unauthorized use [4]. Prime authentication mechanism directly adopted by the IEEE 802.16e is the extensible authentication protocol (EAP) based authentication. Authentication server (AS) and authentication, authorization, and accounting (AAA) server are the two primary entities responsible for the EAP-based authentication of a user. It also helps the users to choose the appropriate mechanisms to get authenticated in a particular location [4–6].

At the same time, LTE-A network witnesses different access authentication procedures such as EPS-AKA during handover to the E-UTRAN, the EAP-AKA or the EAP-AKA' during handover to trusted non-3GPP access networks and IKEv2 with EAP-AKA or EAP-AKA' during handover to untrusted non-3GPP access networks, being followed in diverse mobility scenarios. [7].

A standards-developing body called the 3GPP has developed a 4G mobile technology named as Long Term Evolution, otherwise known as 4G LTE [8]. This technology is more advanced than the existing mobile technology because the users can have special features like VoIP, high-quality video conferencing, video messaging in their mobile phones. However, mention has not yet been made about the handover preparations in the 4G LTE systems standards. IEEE 802.16 otherwise known as WiMAX is also capable of providing high-speed internet access in the wide area. Hence, it is firmly believed that the integration of WiMAX and LTE networks can provide a complete wireless scheme for delivering high-speed Internet access to businesses, homes, and hot mobile nodes by combining their special features. [9].

2 Related Works

As most applications are being driven highly by mobile users, there is a need to study the mobility issue as part of the system [3]. When a Mobile Station (MS) handovers from one Base Station (BS) to another, the MS has to undergo complete EAP authentication with the AS. It involves a series of steps which can be summarized as a 3-way handshake with BS and finally exchanging the traffic encryption key (TEK) [10]. However, EAP mechanism takes excessive time due to its public key cryptographic operations [11]. Also, the round trip time (RTT) associated with every handoff is time consuming. Any failure in this process may lead to session termination due to latency or lack of resources. In order to reduce the latency that occurs during the handover, mobile WiMAX supports recycling techniques on the authentication key materials, allowing users to reuse key materials from the previous authentication. However, it creates critical security issues such as a lack of valid entity authentication [2, 12].

The handover process of WiMAX involves scanning [13–16] and it is one of the required phases to locate the target BS [17]. However, the redundant or unnecessary scanning of neighbor BSs effectuates delay and results in an MAC overhead which consequently is likely to affect real-time applications. To reduce scanning delay, Lu et al. [18]

propose a scanning scheme which estimates the approximate location of the MS so that the number of scanned neighbor BSs can be controlled.

Ben-Mubarak et al. [17] propose a fuzzy logic based self-adaptive handover algorithm to provide efficient handover decisions. Based on the MS velocity and RSSI value, handover parameters such as handover threshold and handover margin are all rendered self-adaptive. Their simulation results show that the algorithm can reduce the number of ping-pong handovers and handover delay.

Various solutions that are aimed at improving latency resulted in security compromise [9, 19]. Shing et al. proposed a key caching mechanism to speed up the handover for mobile WiMAX. By this mechanism, when an MS leaves the old ASN-GW, the MS key records are cached in the old ASN-GW. The MS uses the cached MSK, if it returns to the ASN-GW before the lifetime expires [20]. Apart from its regular routines, ASN-GW is again loaded with storage components to store the used credentials. On the other hand, the old ASN-GW consumes extra storage to maintain the MS key records when the MS leaves the old ASN-GW, which is a major overhead. Re-authentication is a compressed form of full EAP-based authentication in handover by reusing the authentication parameters exchanged between the AS and the MS in the last authentication. The EAP re-authentication protocol (ERP) allows MS and the AS to use the extended master session key (EMSK) from the previous EAP authentication for Master Session Key (MSK) derivation. Thus, instead of carrying out a full EAP authentication, the MS and the AS will only need a single round trip to exchange the ERP messages. It reduces the overhead considerably [21, 22]. Discarding the other issues, our work is aimed at improving the efficiency of authentication thereby achieving seamless handover in mobile WiMAX which can be directly adapted to LTE and LTE-A Networks also since they share the same MAC Layer. This paper is organized as follows: The primary authentication mechanism using EAP is described in Sect. 3. The proposed work UPP-KC is discussed in Sect. 4. The formal verification using probabilistic distributions and the performance analysis of our proposal are presented in Sects. 5 and 6 respectively. Finally, in Sect. 7, we conclude the paper along with the direction for future work.

3 System Background

3.1 EAP Framework and Authentication

The basic authentication in WiMAX is carried out using the AAA server. EAP [23] is used for this basic authentication, and it is encapsulated in Privacy Key Management (PKMV2) [20–22, 24]. The IEEE 802.1X authentication scheme is used for the initial network entry as shown in Fig. 1. The necessary process of authentication is through ASN-GW which serves as the authenticator for MS. It forwards the authentication messages between the AAA server and the MS. ASN-GW stores information after authentication. The authenticator sends the EAP request message to MS which in turn responds with the EAP response and the user identity (AAA server address and user account). The message is then forwarded to the AAA server using the AAA server address. Then the AAA server issues an EAP request to MS which responds with a random number MS-RAND. The AAA server contacts Home Location Register (HLR) to obtain a RAND number and generate a Signed RESponse (SRES) and a cipher key K_c. The AAA then utilizes the K_c and MS-RAND to compute MSK and EAP integrity

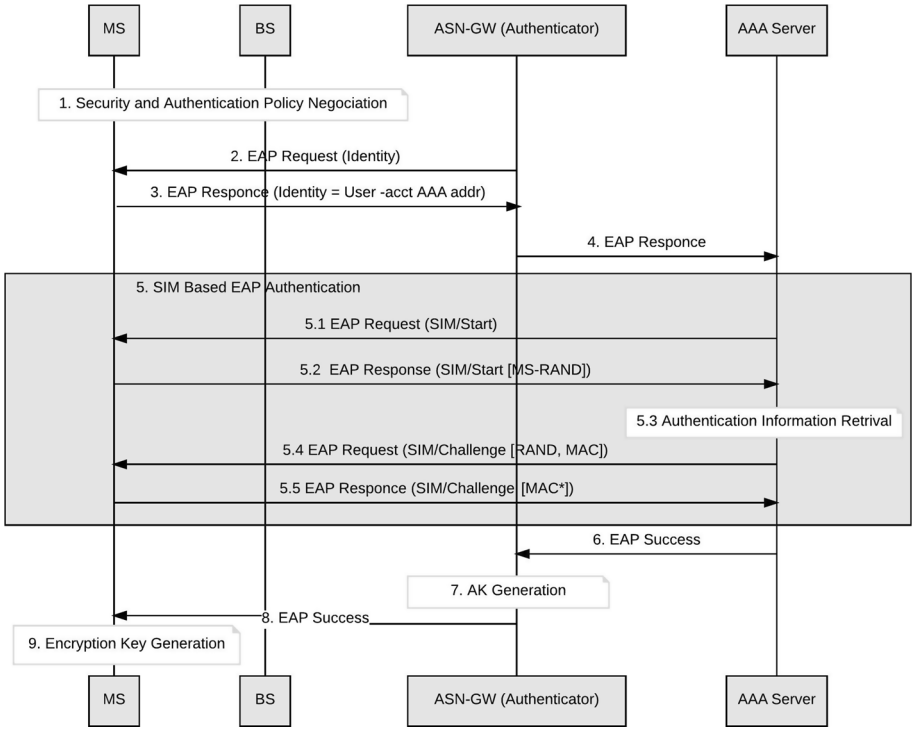


Fig. 1 Initial network entry in IEEE 802.1x

key K_{EAP}. Message Authentication Code (MAC) is derived from K_{EAP}, and the AAA sends the MAC and the RAND to MS. The MS then uses the RAND, MS-RAND, and K_i (from sim card) to generate its SRES*, K_c, MSK, K_{EAP}. Then it verifies the MAC it receives from the AAA server. It ensures that the AAA server is authenticated. The MS then responds with MAC*, SRES*, K_{EAP}. The AAA also verifies the MAC* using the SRES ensuring MS is authenticated. The MSK, MSK lifetime and the MS authorization profile are sent to ASN-GW. The ASN-GW derives AK using the BS address and MSK. The MS is informed with the successful authentication message. The BS then generates the TEK to ensure the integrity. Figure 1 describes the Network entry procedure that is involved in the general EAP based authentication scheme that is followed in the Mobile WiMAX.

Those algorithms that are required to be used to derive keys and generate keys are defined in the PKMV2. Once the successful authentication and authorization process is over, Source Key materials are generated. These source keys play the role of a parent from which all the forthcoming derivatives are derived. These keys are responsible for ensuring management message integrity to deliver the traffic encryption keys at both the ends. All the keys that are derived in PKMV2 are through Dot16KDF.

PKMV2 supports two authorization schemes: Firstly, it is used for authorization based on RSA and secondly for authentication based on EAP.

The Authorization Key (AK) will be derived by the SS and BS as a successful outcome of the Authentication and Authorization based on EAP and RSA respectively as shown in Fig. 2.

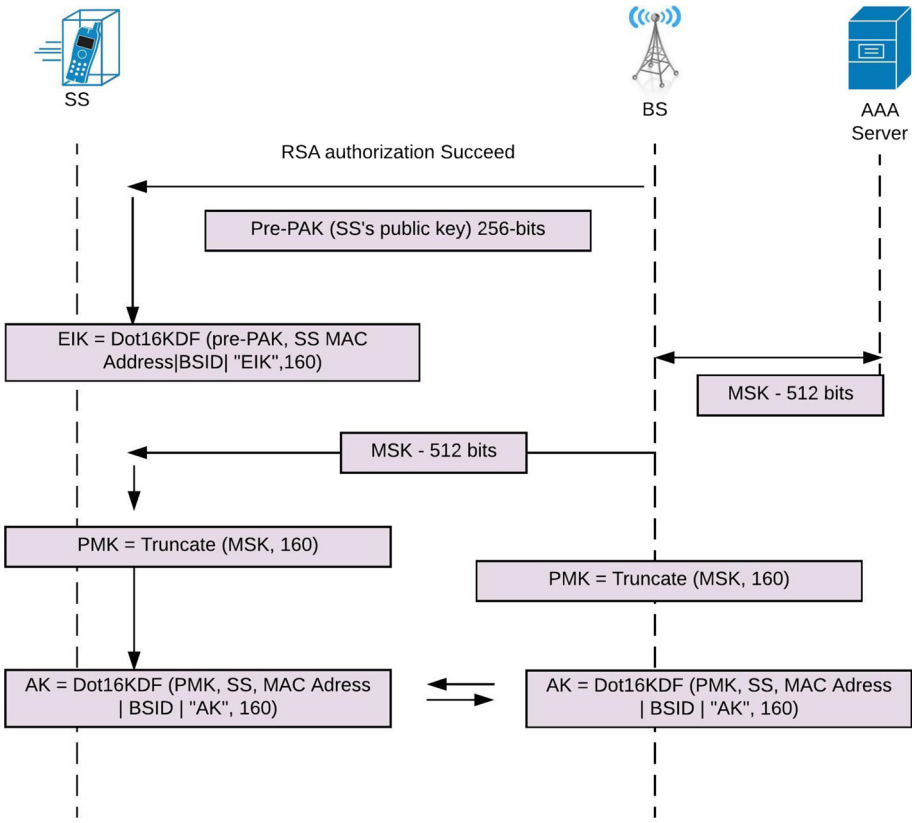


Fig. 2 Key derivation of AK from MSK

Once the Mutual Authentication is achieved, the BS generates a pre-primary authorization key (pre-PAK) and forwards it to SS by encrypting this key with the Public key of SS certificate. PAK is generated from Base Station Identifier (BSID) and the received pre-PAK with MAC address of SS [25].

In the EAP authentication mode, a 160-bit EAP integrity key (EIK) is derived from pre-PAK. This protects the first group of EAP exchange message. EAP exchanges produce a 512-bit MSK. It is known to AAA server, the Authenticator (BS) and the receiver (SS). The Pairwise Master Key PMK is generated from the MSK by truncating MSK to 160 bits at both sides. This is shown in Fig. 2.

After every successful authentication the BS or SS requests for an authorization policy. Usually, EAP performs two round authentication operations. The negotiations after the successful first round of authentication imply that the SS and BS perform two rounds of EAP. Once this 2nd round is completed, the AK is generated in BS and SS.

4 Pattern Based User Path Prediction and Authentication Mechanism (UPP-KC)

Like caching, based on retrieval and replacement policies, this is a kind of approach that depends on the user activity or behavior in mobile data management. That is to say, it is servicing the user groups by predicting their move often towards various landmarks [26]. An all-time favorite DNA structure reveals the facts about a human being. This can be considered as a classical example of pattern based data management. With the help of numerous user activity patterns, data deliverables to the users at the right spot will even get faster. Like data mining, mining of user behavior patterns helps in making various permutations and combinations to predict the user activity. The frequent access to railway subway for ticketing is one such a sequential approach. There is more number of such sequential behavior, or user activity is mined to get different approaches in the mining of sequential patterns [27–32] Here we have considered one such approach that reveals the fact of Pattern based mobile data management approach.

The proactive authentication scheme was a successful attempt at predicting the next move or location of a mobile user to provide service at the right time and place. Such a prediction [33] can be done through multiple activities of a user. Multiple activity is composed of region movement [26, 34, 35], client request and concurrences of both or interleaving of all the above. This is simply like listing all the 'n' ways to a specific location and every route to attain the destination is said to be pattern. Let us consider the example of MU1 (Mobile user 1) and MU2 (Mobile user 2) start from the same location A. MU1 starts from A and goes to a new location B for lunch and moves to another location C for shopping, then to D for shopping again and to E for a watching a movie, and eventually to a subway at F and then to the final destination G. Let MU2 move from A to B for lunch; then after lunch to a new location E to request a store service in his current location E; let him now move to the next location F to meet a stock market assistance and finally through subway let him reaches his destination D. From the above examples we have classified the service patterns into three; they are defined by the examples again.

- Both starts from the same location A and reaches B for lunch is an example of Location-service pair pattern.
- Then they go to different places C and D but requesting for the same service is an example of Service-only pattern.
- After reaching the same location F and requesting for different services is an example of Location-only pattern.

With these patterns we have designed a proactive authentication management algorithm for users to continue their service independent of their locations.

Pattern_Based_Authentication (user UID)

```
1. Log – Initial Visit logs in User Database
2. T – Threshold Value
3. Pattern = (BS1, BS2, … BSN) = Modified_Apriori(Log, T)
4. ifuser enters BSi do
5. MSK = Obtain MSK from AAA
6.      for BSi+1 to BSN in Pattern do
7. Broadcast(MSK)
8.     counter = N-i-1
9. end if
10. for j = i + 1 to N do
11. if user enters BSj do
12.            counter = counter - 1
13. else
14. counter = 0
15.            drop MSK
16. end if
17. end for
```

//Path Prediction Algorithm

```
1.Un: User itemset of size n
2.Fn : frequent itemset of size n
3.F1 = {frequent items};
4.for (n = 1; Fn !=NULL n++) do begin
5.Un+1 = Users generated from Fn;
6.for each Authentication Au in database do
  increment in Un+1;
7.Fn+1 = candidates in Un+1 with min_support
8.end
9.return Union_Un Fn;
```

With fast moving users, handovers occur more frequently and the available handover authentication mechanisms do deteriorate. To support fast moving users, we propose a key caching mechanism with User Path Prediction (UPP-KC). Mobility of fast moving users is not always random. Most of the users fall in a general pattern, which can be extracted and used for authentication. The user mobility is logged in the user database of the AAA server. Fast moving users following a general pattern will have frequent visits to some BSs. Every visit of the user will be logged and pattern mining algorithms can be used on these logs to determine the frequent pattern. Once the pattern is determined and every user is associated with his frequent pattern [36–38], the authentication keys can be multicast to the BSs in that pattern and the MSK is cached in the pattern to facilitate fast authentication during handoffs as shown in Fig. 3. The authentication mechanisms based on UPP-KC during the initial network entry and during handoffs are described below

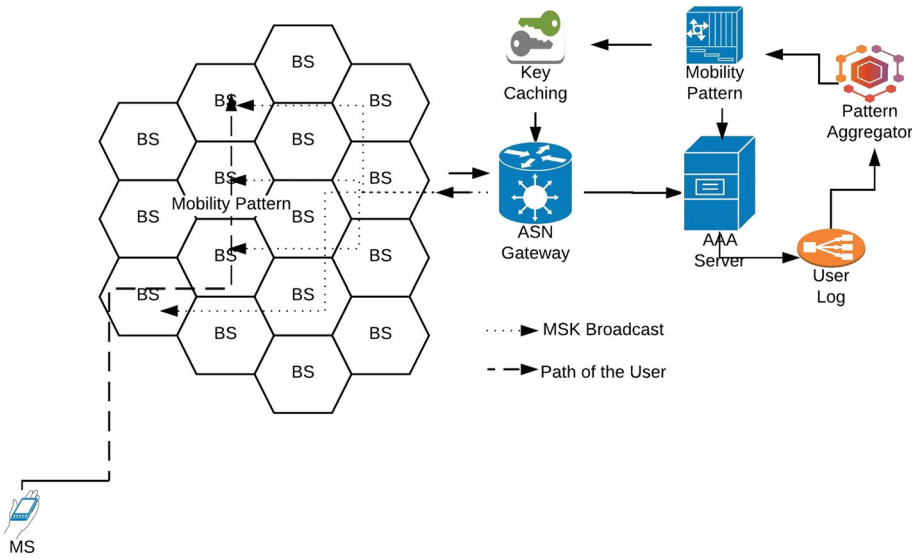


Fig. 3 Authentication for frequent user path prediction

Case 1: Initial Network entry

Step 1. As with normal authentication mechanisms, all the steps of IEEE 802.1X authentication take place during the initial network entry and the MSK is derived for the user (MS).

Step 2. Once the MS enters the network after its initial authentication, the frequent pattern of the MS is determined from the User Database log of the AAA server.

Step 3. The MSK established during the initial network entry is given to the BSs in the frequent pattern of the MS.

Case 2: Handover authentication

Step 1. The identity of the MS is examined by processing the certificate using certificate authority (CA).

Step 2. Once the identity of the MS is confirmed, the MSK obtained by the BS is used directly.

```
Algorithm For Authentication @ AAA Server
    //Authentication in the 1st BS in the Predicted Path
        Initiate Authentication
        1. Start Auth_Req to BS
        2. if (Pattern !found)
        3. then Initiate Normal Authentication
        4. Else
        5. for i=1 to Max(Patttern)
        6. do Cache MSK as Cached_MSK
        7. If (Visiting Bs !in Pattern)
        8. then Fetch New_MSK
        9. Else use Cached_MSK
        Complete Authentication at BS

    //Authentication of the MS in the Predicted Path
        Initiate Authentication
        1.   Start Auth_Req to BS
        2.   If (Cached_MSK == Present)
        3.   Use Cached_MSK to derive derivatives at the BS
        4.   Used already derived Keys by MS in the Previous BS
        5.   Else
        6.   Initiate Normal Authentication
        Complete Authentication
```

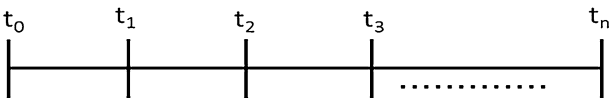
A detailed description of the message exchanges that occur in UPP-KC based handoff authentication is described in Fig. 4.

5 Mathematical analysis

5.1 Systematic analysis of existing algorithm with UPP-KC algorithm

Although this proposed algorithm effectively avoids the execution of IEEE 802.1X authentication, it consumes extra storage to keep track of the user's pattern along with the key which includes 512 or 1024 bits totally. This can be justified with the fact that the actual time taken by the user to follow normal IEEE 802.1X authentication mechanism is extremely large.

5.2 Movement Time Line of MS



Let, t_0—Initial network entry authentication occurs, t_1—MS moves to a random ASN or new ASN, t_2—MS moves via the predicted pattern, t_n—End point of mobility

Hence,

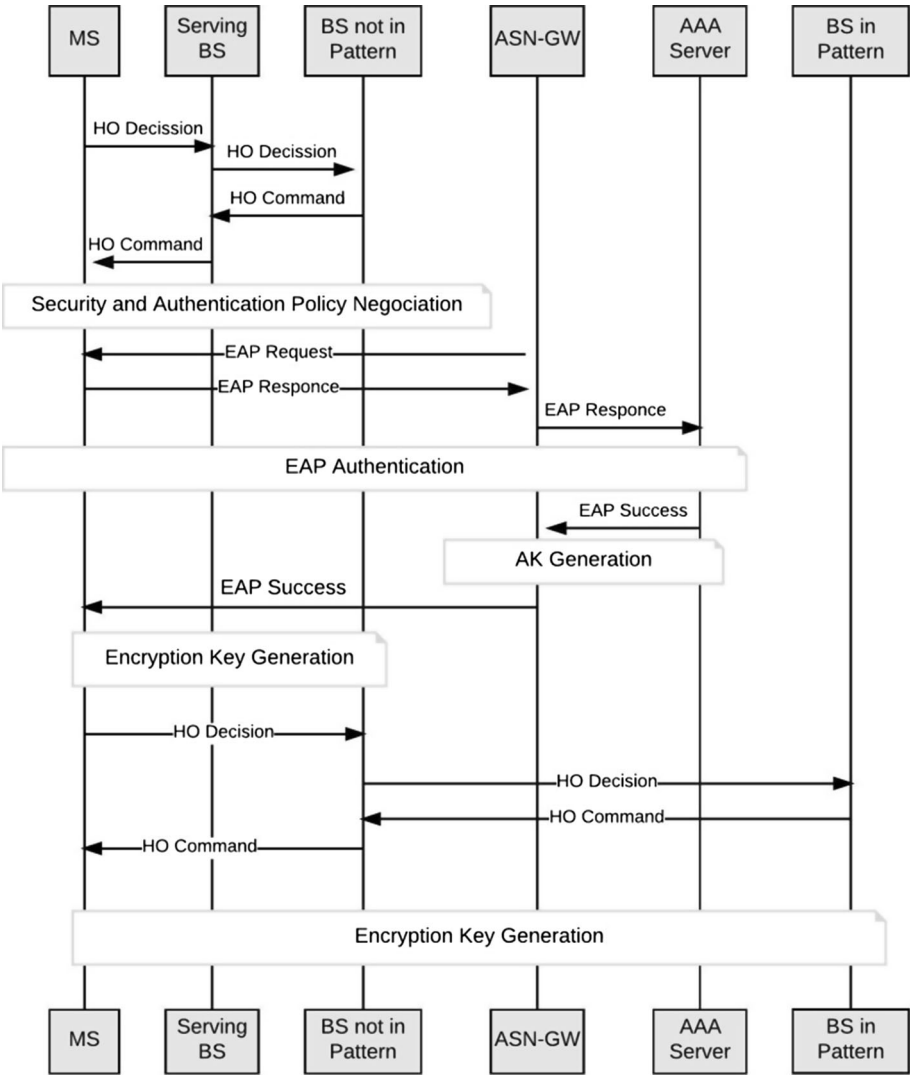


Fig. 4 UPP-KC based handover authentication

$$T_k = t_n - t_1 \tag{1}$$

If MS does not take the path via pattern, the key remains unused.

If the MS follows predicted pattern, the time taken would be,

$$T_k^* = T_k - S, \quad \text{where } S = t_2 - t_1 \tag{2}$$

T_k—Entire life time, which may vary exponentially, T_k^*—Reuse period As with any stochastic process, the comparison of IEEE 802.1X mechanism with UPP-KC mechanism can be accomplished by analyzing the time factor.

Three output measures are evaluated in our study:

1. α: the probability that the MS returns to the old ASN-GW
2. E [T_k| ($t_2 - t_1$) ≥ T_k]: The MS doesn't take the predicted path
3. E [T_k^*| ($t_2 - t_1$) ≥ T_k]: MS uses the path along the pattern

We derive the above output measures for exponentially distributed S with fixed T and then generalize the derivation for generally distributed S with exponentially distributed T.

5.2.1 Derivation for Exponentially Distributed S and Fixed T

The departure of the MS from the old ASN-GW is a random observer to the MSK lifetime. For the fixed MSK lifetime T, from the residual life theorem, T_k has a uniform distribution over $0 \le T_k \le T$. Then, α is derived as

$$\alpha = P[T \le T_k]$$

$$= \int_{T_k=0}^{T} \left(\frac{1}{T}\right) \left(\int_{S=0}^{T_k} \lambda e^{-\lambda S} dS \right) dT_k$$

$$\alpha = \frac{e^{-\lambda T} + \lambda T - 1}{\lambda T}$$

$$E[T_k | S \ge T_k] = \frac{E[T_k \text{ and } S \ge T_k]}{P[S \ge T_k]}$$

$$E[T_k \text{ and } S \ge T_k] = \int_{S=0}^{T} \lambda e^{-\lambda S} \left(\int_{T_k=0}^{S} T_k \left(\frac{1}{T} dT_k\right) \right) + \int_{S=T}^{\infty} \lambda e^{-\lambda S} \left(\int_{T_k=0}^{T} T_k \left(\frac{1}{T} dS\right) \right)$$

$$= \frac{1 - e^{-\lambda T}}{\lambda^2 T} - \frac{e^{-\lambda T}}{\lambda}$$

$$E[T_k | S \ge T_k] = \frac{E[T_k \text{and} S \ge T_k]}{P[S \ge T_k]}$$

$$= \frac{1 - e^{-\lambda T}}{\lambda^2 T} - \frac{e^{-\lambda T}}{\lambda} \left(\frac{1}{1 - \alpha}\right)$$

$$= \frac{1}{\lambda} - \frac{T e^{-\lambda T}}{1 - e^{-\lambda T}}$$

similarly,

$$E[T_k^* | S \le T_k] = \frac{E\left[T_k^* \text{and} S \le T_k\right]}{P[S \le T_k]}$$

where,

$$E\left[T_k^* \text{ and } s \le T_k\right] = \int_{T_k=0}^{T} \left(\frac{1}{T}\right)\left[\int_{S=0}^{T_k} (T_k - S)\lambda e^{-\lambda T_k} dS\right] dT_k$$

$$= \frac{T}{2} - \frac{1}{\lambda} + \frac{1 - e^{-\lambda T}}{\lambda^2 T}$$

from the above equations,

$$E\left[T_k^* \text{ and } s \le T_k\right] = \left(\frac{T}{2} - \frac{1}{\lambda} + \frac{1 - e^{-\lambda T}}{\lambda^2 T}\right)\left(\frac{1}{\alpha}\right)$$

$$= \left(\frac{T}{2} - \frac{1}{\lambda} + \frac{1 - e^{-\lambda T}}{\lambda^2 T}\right)\left(\frac{\lambda T}{e^{-\lambda T} + \lambda T - 1}\right)$$

$$= \left(\frac{\lambda T^2}{2(\lambda T + e^{-\lambda T} - 1)}\right) - \left(\frac{1}{\lambda}\right) \tag{3}$$

5.2.2 Derivation for Generally Distributed S and Exponential T

T_k is exponentially distributed with mean $E[T] = 1/\mu$. Let S have an arbitrary distribution with density function f(S) and Laplace transform $f_*(S)$. Then, α is derived as

$$\alpha = \int_{T_k=0}^{\infty} \mu e^{-\mu T_k} \left(\int_{S=0}^{T_k} f(s) dS\right) dT_k = f^*(\mu)$$

$$E[T_k \text{ and } s \ge T_k] = \int_{S=0}^{\infty} f(s) \left(\int_{T_k=0}^{S} T_k \mu e^{-\mu T_k} dT_k\right) ds$$

$$= \frac{1}{\mu} + \left(\frac{df^*(s)}{ds}\right) - \frac{f^*(\mu)}{\mu}$$

$$E[T_k | s \ge T_k] = \frac{\mathrm{E}\ [\mathrm{T_k} \text{ and } \mathrm{s}\ \ge \mathrm{T_k}]}{\mathrm{P}[\mathrm{T_k} | \mathrm{s}\ \ge \mathrm{T_k}]}$$

$$= \left\{\frac{1}{\mu} + \left(\frac{df^*(s)}{ds}\right) - \frac{f^*(\mu)}{\mu}\right\}\left\{\frac{1}{1 - f^*(\mu)}\right\}$$

$$E\left[T_k^* \text{ and } s \le T_k\right] = \int_{T_k=0}^{\infty} \mu e^{-\mu T_k} \left(\int_{s=0}^{T_k} (T_k - s) f(s) ds\right) dT_k = \frac{f^*(\mu)}{\mu}$$

$$E\left[T_k^* | s \ge T_k\right] = \frac{E\left[T_k^* \text{ and } s \ge T_k\right]}{P[s \le T_k]} \tag{4}$$

6 Performance Measure

Table 1 depicts the strength of our proposed UPP-KC with respect to the authentication mechanisms that are proposed for the same issue. The authentication mechanism based on User Path Prediction reduces the authentication latency by 32% for the given input compared with the existing IEEE 802.1X mechanism. Therefore on a medium scale, the UPP-KC algorithm is proved to be better than the existing one considering fast authentication. When the availability of the cached MSK is considered, Whenever the user deviates from the redundant path, the deviation is recorded and it is considered for determining the pattern, next time. The performance measure is found by taking the ratio of slope values of the vectors and the parameters from the analytic proof discussed in the previous section. Based on the Eqs. 3 and 4, a graph is constructed for both the mechanisms and a comparison is made as shown in the Figs. 5 and 6. The graph is constructed by marking the expectation values (E[t]) along the horizontal axis and the total mobility time (t) values along the vertical axis. Values of UPP-KC mechanism for bestcase, average case, and worst case are compared with the IEEE 802.1X mechanism and plotted in a planar graph. It

Table 1 Comparison of Key Caching based UPP-KC with other Mechanisms

Mechanisms attributes	Re-authentication	Pre-authentication	UPP-KC
Key derivation	For every visit	For all stations	Only one time on the predicted path
Key reuse	No	No	Yes
Storage complexity	No	Not required	Easy and highly volatile
Mobility of user	Medium	Very low	High mobile
Scalability	No	No	Highly scalable
Best suited for	Frequent users	General	Highly frequent travellers

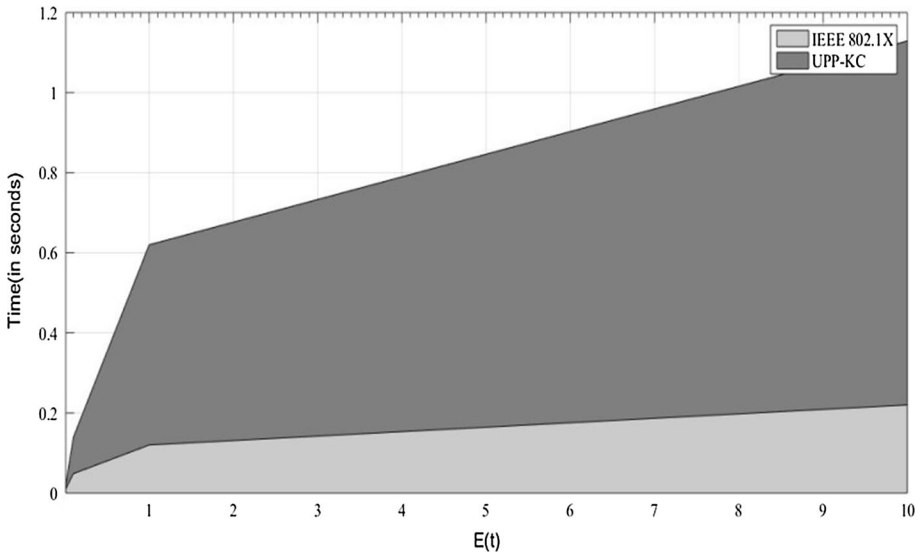


Fig. 5 Comparison of IEEE 802.1X with UPP-KC. (UPP-KC—Exponential and IEEE 802.1X—Fixed)

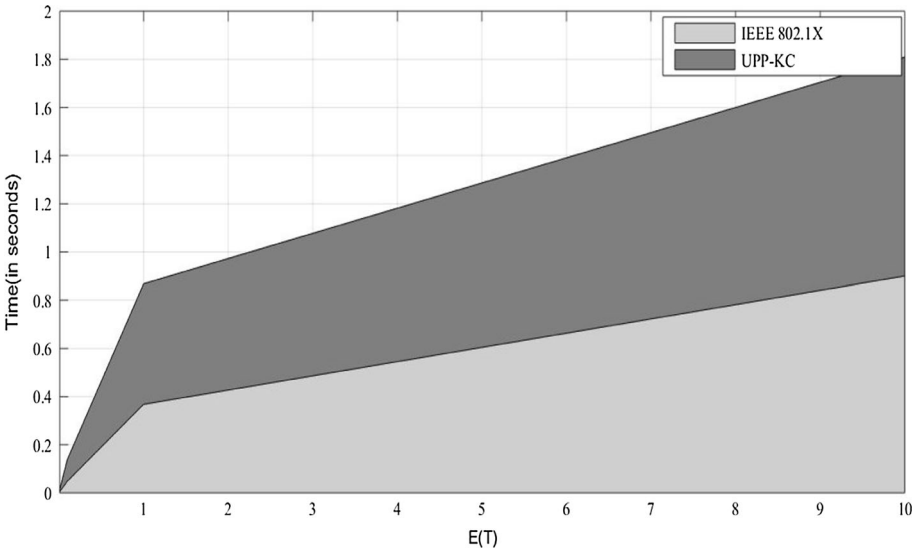


Fig. 6 Comparison of IEEE 802.1X with UPP-KC. (UPP-KC—Fixed and IEEE 802.1X –Exponential)

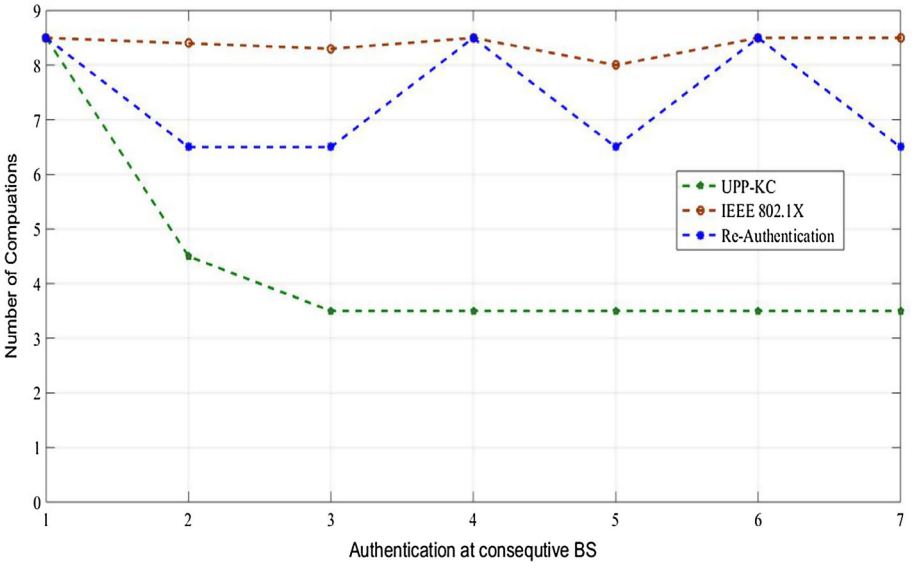


Fig. 7 Authentication of MS in the predicted path

has been found that under best and average case scenarios, the UPP-KC mechanism is exponentially efficient with the reduction in latency, whereas in worst case scenario, it coincides with the existing work depicting the fact that if the user does not have frequent path, or if the user is not frequently mobile, UPP-KC mechanism is not efficient and hence follows the standard procedure. For simulating the proposed model, the Network Simulator ns-2 is used. ns-2 as such does not support WiMAX technology. Therefore, the WiMAX

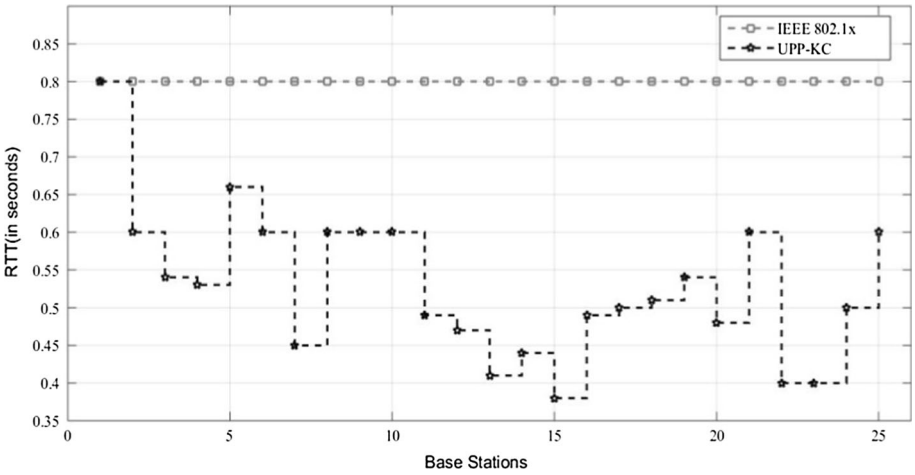


Fig. 8 Simulation based analysis of UPP-KC with IEEE 802.1X

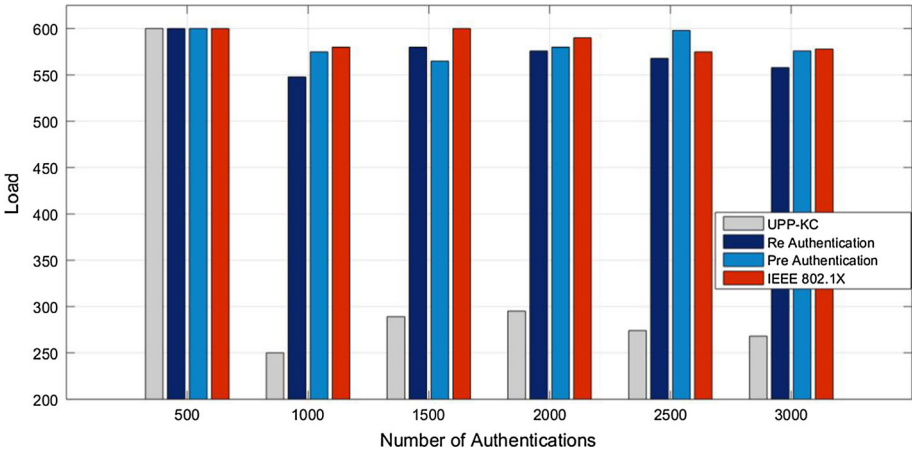


Fig. 9 Load Comparison of Authentication Protocals at MME

patch with WiMAX 802.16 PHY and MAC functions for ns-2, provided by National Institute of Standards and Technology (NIST) is used.The performance evaluation based on the trace files of ns-2 is shown in Fig. 7. The RTT for authentication message exchanges between the UPP-KC authentication and normal IEEE 802.1x are plotted in Fig. 8. Load imposed on the MME and HSS is analysed for various authentication schemes in Fig. 9.

Table 2 describes the spectrum utilization parameter for the heterogeneous network and the comparison of the existing protocols with our proposed caching UPP-KC.

Table 2 Spectrum utilization by our proposed key caching based UPP-KC

Time	No. of requests	No. of keys	Key generation with UPP-KC	Spectrum utilization per request					
				2G existing (Bits/s/Hz)	2G with proposed UPP-KC (Bits/s/Hz)	3G existing (Bits/s/Hz)	3G with proposed UPP-KC (Bits/s/Hz)	4G existing (Bits/s/Hz)	4G with proposed UPP-KC (Bits/s/Hz)
T1	19,877	19,877	13,598	13.23	9.05	0.313	0.21443	0.0238	0.0163
T2	19,562	19,562	14,691	13.02	9.77	0.308	0.2316	0.0234	0.0176
T3	20,053	20,053	15,021	13.34	9.99	0.316	0.2368	0.0240	0.0180
T4	17,655	17,655	13,021	11.75	8.66	0.278	0.2053	0.0211	0.0156
T5	19,862	19,862	14,521	13.22	9.66	0.313	0.2289	0.0238	0.0174
T6	16,532	16,532	12,354	11.00	8.22	0.260	0.1948	0.0198	0.0148
T7	18,968	18,968	15,674	12.62	10.43	0.299	0.2471	0.0227	0.0188
T8	17,635	17,635	12,589	11.73	8.37	0.278	0.1985	0.0211	0.0151
T9	18,350	18,350	14,985	12.21	9.97	0.289	0.2363	0.0220	0.0179

7 Conclusion and Future Work

This paper has proposed UPP-KC, a caching mechanism where the keys are cached only along a predicted path. The most frequent pattern in the user's path is determined using appropriate pattern predicting algorithm to minimize the computational complexity. The resources for authentication can be reserved along this pattern so as to reduce the wastage of resources and making authentication faster along the pattern as the resources are already reserved. The future work is aimed at analysing and extracting all the services that a user avails in a particular BS. This will allow us to provide only those services that the user frequently avails in a BS [39, 40], thereby further optimizing the allocation of resources without compromising on security or handoff time.

Using shared master keys as the base for key derivation might be a possible weakness. In the event of the master keys (pre-PAK and MSK) being not kept secret and the authentication processes being not made fool proof, a malicious user could listen to connection or even hijack it. However, this weakness is implementation dependant, because it is the manufacturer who decides the selection of the preferred authentication method (EAP).

Acknowledgements Rajakumar Arul gratefully acknowledges support from Anna University for Anna Centenary Research Fellowship. Gunasekaran Raja gratefully acknowledges support from DST - SERB Fast Track for Young Scientists in Engineering Sciences F.No. SR/FTP/ETA-110/2011. Gunasekaran Raja, Rajakumar Arul, Kottilingam Kottursamy, Pavithra Sathiyanarayanan, Swaminathan Venkatraman gratefully acknowledges support from NGNLabs, Department of Computer Technology, Anna University, Chennai.

References

1. Golubeva, T. V., Zaitsev, E. O., & Konshin, S. V. (2016). Research of WiMAX standard to organize the data transmission channels in the integrated control system of earth-moving machines. In *17th international conference of young specialists on micro/nanotechnologies and electron devices (EDM)*, pp. 91–95, August 2016.
2. Air Interface for Broadband Wireless Access Systems. *IEEE standard for local and metropolitan area networks,* IEEE Std 802.16 m™-2011.
3. Pack, S., & Choi, Y. (2004). Fast handoff scheme based on mobility prediction in public wireless LAN systems. *IEEE Proceedings—Communication, 151*(5), 489–495.
4. Lee, T.-F. (2013). User authentication scheme with anonymity, unlinkability and untrackability for global mobility networks. *Security Communiation Networks Wiley, 6*(11), 1404–1413.
5. Fu, A., Zhang, Y., Zhu, Z., & Liu, X. (2010). A fast handover authentication mechanism based on ticket for IEEE 802.16m. *IEEE Communications Letters, 14*(12), 1134–1136.
6. Choi, J., & Jung, S. (2010). A handover authentication using credentials based on chameleon hashing. *IEEE Communications Letters, 14*(1), 54–56.
7. Cao, J., Ma, M. Li, H. Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. *IEEE Communications Surveys & Tutorials*, *16*(1), First Quarter 2014.
8. ITU-T, X.1642. (2016). *Telecommunication standardization sector of ITU*, pp. 1–30, March 2016.
9. Edward, E. P. (2016). A novel seamless handover scheme for WiMAX/LTE heterogeneous networks. *Arabian Journal for Science and Engineering, 41*(3), 1129–1143.
10. Nguyen, T. N., & Ma, M. (2012). Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. *IEEE Transactions on Wireless Communications, 11*(6), 2179–2181.
11. Hao, F. (2010). On robust key agreement based on public key authentication. In *Financial cryptography and data security, lecture notes on computer science* (Vol. 6052, pp. 383–390). Springer.
12. Enhancements to Support Machine-to-Machine Applications. *IEEE standard for air interface for broadband wireless access systems*. IEEE Std 802.16p™—Oct. 2012.

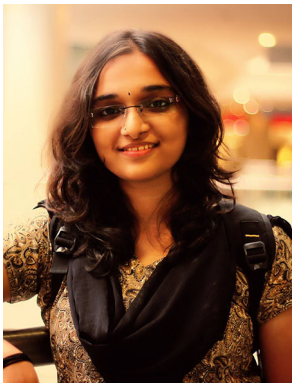
13. Son, L. H., & Thong, P. H. (2016). Soft computing methods for WiMax Network Planning on 3D Geographical Information Systems. *Journal of Computer and System Sciences, 83*(1), 159–179.
14. Zhang, Q., Das, S. K., & Rodriguez-Carrion, A. (2016). A 2-D random walk mobility model for WiMAX location update. *Computer Communications, 28*, 86–96.
15. Gautam, A. K., Bisht, A., & Kanaujia, B. K. (2016). A wideband antenna with defected ground plane for WLAN/WiMAX applications. *AEU—International Journal of Electronics and Communications, 70*(3), 354–358.
16. Kansal, L., Sharma, V., & Singh, J. (2016). Performance evaluation of FFT-WiMAX against WHT-WiMAX over Rayleigh fading channel. *Optik—International Journal for Light and Electron Optics, 127*(10), 4514–4519.
17. Ben-Mubarak, M. A., Ali, B. M., Noordin, N. K., Ismail, A., & Ng, C. K. (2013). Fuzzy logic based self-adaptive handover algorithm for mobile WiMAX. *Wireless Personal Communication, 71*(2), 421–1442.
18. Qi, L., & Ma, M. (2012). Achieving faster handovers in mobile WiMAX networks. *Wireless Personal Communications, 65*(1), 165–187.
19. Wang, D., Cheng, H., He, D., & Wang, P. (2016). On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. *IEEE Systems Journal* (99), 1–10.
20. Hsu, S.-F., & Lin, Y.-B. (2009). A key caching mechanism for reducing WiMAX authentication cost in handoff. *IEEE Transactions on Vehicular Technology, 58*(8), 4507–4513.
21. Al Shidhani, A., & Leung, V. C. M. (2011). Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers. *IEEE Transactions on Dependable and Secure Computing, 8*(5), 699–713.
22. Fu, A., Lan, S., Huang, B., Zhu, Z., & Zhang, Y. (2012). A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks. *IEEE Communications Letters, 16*(11), 1744–1747.
23. Liu, D. Q., & Coslow, M. (2008). Extensible authentication protocols for IEEE standards 802.11 and 802.16. In *International conference on mobile technology, applications, and systems mobility '08*, pp. 792–799, 2008.
24. Zhang, L., Seta, N., Miyajima, V., & Hayashi, H. (2007). Fast authentication based on heuristic movement prediction for seamless handover in wireless access environment. *IEEE Wireless Communication and Networking, WCNC,* 2891–2895.
25. Ahson, S. A., & Ilyas, M. (2007). *WiMAX: Standards and security*. Boca Raton: CRC Press.
26. Chen, T.-S., Chou, Y.-S., & Chen, T.-C. (2012). Mining user movement behaviour patterns in a mobile service environment. *IEEE Transactions on Systems, Man and Cybernetics, 42*(1), 87–101.
27. Yun, C.-H., & Chen, M.-S. (2007). Mining mobile sequential patterns in a mobile commerce environment. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviewers), 37*(2), 278–295.
28. Tseng, V. S., & Lin, K. W. (2005). Mining sequential mobile access patterns efficiently in mobile web systems. In *19th international conference on advanced information networking and applications* (Vol. 2, pp. 762–767).
29. Cao, H., Mamoulis, N., & Cheung, D. (2005). Mining frequent spatio–temporal sequential patterns. In *Fifth IEEE international conference on data mining*, ICDM, pp. 82–89, 2005.
30. Tseng, V.S., Lu, H.-C., & Huang, C.-H. (2007). Mining temporal mobile sequential patterns in location-based service environments. In *International conference on parallel and distributed systems*, pp. 1–8, December 2007.
31. Lin, N. P., Hao, W.-H., Chen, H.-J., Chueh, H.-E., & Chang, C.-I. (2007). Discover sequential patterns in incremental database. *International Journal of Computers, 1*(4), 196–201.
32. Hara, Takahiro, & Madria, Sanjay Kumar. (2009). Consistency management strategies for data replication in mobile ad hoc networks. *IEEE Transactions on Mobile Computing, 8*(7), 950–967.
33. Merah, A. F., Samarah, S., & Boukerche, A. (2012). Vehicular movement patterns: A prediction-based route discovery technique for VANETs. In *IEEE ICC conference on communications*, pp. 5291–5295, June 2012.
34. Prasad, P. S., & Agrawal, P. (2010). Movement prediction in wireless networks using mobility traces. In *7th IEEE consumer communications and networking conference (CCNC)*, pp. 1–5, January 2010.
35. Chakraborty, S., Dong, Y., Yau, D. K. Y., & Lui, J. C. S. (2005). On the effectiveness of movement prediction to reduce energy consumption in wireless communication. *IEEE Transactions on Mobile Computing, 5*(2), 157–169.
36. Wu, B., Zhang, D. Lan, Q., & Zheng, J. (2008). An efficient frequent patterns mining algorithm based on apriori algorithm and the FP-tree structure. In *Third international conference on convergence and hybrid information technology, ICCIT,* pp. 1099-–102, November 2008.

37. Chai, S., Yang, J., & Cheng, Y. (2007). The research of improved apriori algorithm for mining association rules. In *International conference on service systems and service management,* pp. 1–4, June 2007.
38. Shi, Y., & Zhou, Y. (2011). An improved apriori algorithm. In *IEEE international conference on electronics and optocelectronics*, pp. 476–478, July 2011.
39. Chou, Z.-T., & Lin, Y.-H. (2016). Energy-efficient scalable video multicasting for overlapping groups in a mobile WiMAX network. *IEEE Transactions on Vehicular Technology, 65*(8), 6403–6416.
40. Luca, R. Ciotîrnae, P., & Greu, V. (2016). Evaluation and improvement of WiMAX real throughput at application level using experimental study analysis and resulted optimization rules. In *2016 international conference on communications (COMM)*, June 2016.

Rajakumar Arul pursued his Bachelor of Engineering in Computer Science and Engineering from Anna University, Coimbatore. He received his Masters in Computer Science and Engineering at Anna University—MIT Campus. Currently, he is doing Doctorate of Philosophy under the Faculty of Information and Communication in NGN Labs, Department of Computer Technology, Anna University—MIT Campus. He is a recipient of Anna Centenary Research Fellowship. His research interest includes Security in Broadband Wireless Networks, WiMAX, LTE, Robust resource allocation schemes in Mobile Communication Networks.

Gunasekaran Raja is an Associate Professor in Department of Computer Technology at Anna University, Chennai and also the Principal Investigator of NGNLabs. He received his B.E. degree in Computer Science and Engineering from University of Madras in 2001, a M.E. in Computer Science and Engineering from Bharathiyar University in 2003, and the Ph.D. in Faculty of Information and Communication Engineering from Anna University, Chennai in 2010. He was a Post-Doctoral Fellow from University of California, Davis, USA, 2014–2015. He was a recipient of Young Engineer Award from Institution of Engineers India (IEI) in 2009 and FastTrack grant for Young Scientist from Department of Science and Technology (DST) in 2011. Current research interest includes 5G Networks, LTE-Advanced, Wireless Security, Mobile Database and Data Offloading. He is a member of IEEE, ACM, CSI and ISTE.

Kottilingam Kottursamy is a candidate for Ph.D. in Department of Computer Technology at Anna University, Chennai and a senior scholar of NGN Labs at Anna University. He received his B.E. degree in Computer Science and Engineering from Anna University in 2006, a M.E. degree in Computer Science and Engineering from Anna University in 2009. His research interest includes Data management in Next Generation Networks, Software Defined Networking, Mobile Databases and Power aware Computing.



Pavithra Sathiyanarayanan completed B.E in Computer Science and Engineering from Madras Institute of Technology in 2014. Research interest includes Broadband Wireless Networks and Wireless Security.

Swaminathan Venkatraman completed B.E in Computer Science and Engineering from Madras Institute of Technology in 2014. Research interest includes Network Security and Future Generation Networks. He is also a student member in IEEE.