Trust and Privacy Based Authentication Method for Vertical Handoff Decision in Heterogeneous Network

M. Dhipa, B. Kalaavathi, A. Chandrasekar

Abstract: ***Next generation wireless networks involve diverse wireless access technologies to support multimedia services to the roaming users with different Quality of Service constraints at anytime and anywhere. The increased number of users and service providers in the integrated network architecture requires authentication mechanism between communication entities to ensure secured handover. The existing security standards of each network are not able to provide most favorable security requirements of the heterogeneous networks because of independent and incompatibility of various wireless networks. Therefore, Trust and Privacy based Multi-attribute Vertical Handoff (TPMVHO) decision algorithm along with Hybrid Genetic Cuckoo Search algorithm to optimize the attributes weight is proposed to select an optimal network for secure handoff mechanism. Simulation results show the reduction in handoff rate, blocking rate and enhanced throughput against Improved Particle swarm optimization based Multi-attribute Vertical Handoff (IPMVHO).***

I. INTRODUCTION

Next Generation Wireless Networks (NGWNs) depend on heterogeneous infrastructure involving various wireless access technologies [1]. It allows users to be connected seamlessly to different Radio Access Technologies which complement each other to satisfy the end user's demands that expect Quality of Services (QoS). Since no individual wireless network can satisfy users' need under all circumstances. The Heterogeneous Wireless Networks (HWNs) are set up all over the world to support such demanding need of users in multimedia applications with always-best connected network.

The heterogeneous wireless environment permits numerous operators and service providers to make use of each other framework to cater the users' demands at the highest level. Therefore, it is essential to give flawless handover whilst shifting in such environment. Due to the open network environment, HWN has become prone to various security threats. Therefore, security is a principal requirement in the handover process to preserve the privacy of the users.

This imposes the designing a robust vertical handoff decision mechanism to offer secure and seamless handover that permits the users to travel freely among the available wireless networks without worrying about security and privacy issues (for instance their identities and locations). The implementation of security mechanism in the handover procedure introduces a delay which degrades the QoS provisioning to the users [2].

In order to resolve this, context-aware based weight assignment TPMVHO, a trust and privacy based authentication technique is introduced to carry out the vertical handoff process in secured manner. The proposed methodology employs Intuitionistic Fuzzy Technique for Order of Preference by Similarity to Ideal Solution Multi-Attribute Decision Making (IF-TOPSIS MADM) algorithm along with Hybrid Genetic-Cuckoo Search (HGCS) optimization algorithm to select the optimal network for handover process. It utilizes pairing-free anonymous mobile node handover authentication method which involves lower computation and communication cost for secure transmission and preserve user privacy.

II. RELATED WORK

A brief review of several handover authentication protocols have been proposed using different techniques is presented in this section.

The authors in [3] proposed a pairing-free identity-based authenticated key agreement protocol based on the computational Diffie-Hellman problem over Elliptic Curve Cryptography (ECC) group. It reduced the time required for message exchange, energy consumption and protocol delay which favours for real-time application. An improved pairing-free Identity-based Authenticated Key Agreement protocol based on ECC was proposed in [4] to get rid of session-specific temporary information attack and key off-set attack. It minimized the message exchanges and computational overheads. The author in [5] introduced Handover Keying, a localized re-authentication scheme to reduce the latency due to several authentication exchanges between the mobile terminal and its home network. The ticket-based and pseudonym-based cryptographic techniques was utilized in [6] to offer secure vertical handoff process with privacy preserving capability between integrated WiFi-WiMAX networks. It reduced the handover authentication delay by minimizing message exchange time and resist against several malicious attacks. The authors in [7] introduced a novel Privacy-Aware Handover Authentication utilizing Schnorr like ID-based signature method without pairing for speedy and secure handover authentication method. The user privacy was attained with lesser computation and communication cost. The authors in [8] developed a novel handover authentication protocol by using the merits of pseudo identity mechanism and ECC to

Revised Manuscript Received on 22 September, 2019.

M. Dhipa, Research Scholar (Part-Time), Anna University, Chennai, Tamil Nadu, India.
(Email ID: dhipachandrasekar@gmail.com)
Dr. B. Kalaavathi, Professor/CSE, KSR Institute for Engineering and Technology, Tiruchengode, Tamil Nadu, India.
(Email ID: kalabhuvanesh@gmail.com)
Dr. A. Chandrasekar, Professor/CSE, Malla Reddy Institute of Technology and Science, Secunderabad, Telangana, India.
(Email ID: chandru.as76@gmail.com).

offer trust and privacy preserving services in Mobile Cloud Computing.

The authors in [9] introduced distributed security architecture for authenticating mobile terminals through hop by hop authentication and neighbor authentication in the network using Elliptic Curve Diffie-Hellman (ECDH) protocol. In this, whenever a new mobile terminal connects with the network; the base station will inform it to the existing stations. In [10], a new Anonymous Authentication for Vertical Handoff (AAVHO) was introduced to guard the user's identity and reduced certificate management overhead. Also, the protection against man-in-the-middle and replay attacks was provided. A new trusted handover authentication protocol was introduced in [11] by considering the merits of pseudo identity method and ECC algorithm to attain user anonymity and untraceability along with trust authentication in handover process efficiently. It had the capability to resist the diverse security attacks and attained universality and robust security.

The authors in [12] introduced a secure cost effective handover decision and authentication scheme comprising three phases: handover decision, handover grouping and handover authentication. In this, the validation process was performed on the available mobile terminals and carried out the authentication for valid nodes only. A novel enhanced Anonymous Handover Authentication (AHA) protocol with batch verification was developed in [13] to address high communication costs due to bilinear pairing or hash-to-point operations of preceding AHA protocols. This methodology offered greater security with less computation cost and increased communication cost.

In [14], an Anonymous Mobile Node Handover Authentication (AMNHA) protocol, a new pairing-free handover authentication method was devised to overcome impersonation attack by providing mutual authentication for both the parties of communications. The user anonymity and untraceability was provided by authentication server through the generation of unlinked pseudo-IDs for every mobile terminal. The authors in [15] suggested a novel handover authentication method based on ECC to resist key compromise attack and attained forward secrecy, escrow-free and strong anonymity for mobile terminals. The batch verification was used by target access point to confirm the rightness of many received messages at the same time to minimize the computation and communication overhead. In [16], a timing advance based secure context-aware handover method was proposed based on the user mobility prediction and timing advance. It helped in integrating strong authentication during handover process with reduced call drops and packet losses. The authors in [17] suggested an anonymous batch handover authentication protocol using group signature technique to pre-distribute handover keys. The session key was generated for mutual authentication between mesh clients and mesh routers. Mesh clients' real identity information, locations and motion trajectory were defended well by group signature, ECC and message authentication code efficiently.

III. PROPOSED CONTEXT-AWARE BASED WEIGHT ASSIGNMENT TPMVHO METHODOLOGY

In this work, IF-TOPSIS MADM is used to choose an optimal network for vertical handoff among the available wireless network in the presence of uncertainty. It makes strong decision in highly complex domain by considering large number of attributes together. Each attribute is assigned with weight value to signify its relative importance in decision making problem. The assignment of weight values plays a significant role in decision making since the change in weights influence the final ranking order of the alternatives. In this work, HGCS algorithm is employed to find the optimized weights since the classical methods get trapped at a suboptimal solution. It enhances the level of optimization and speed of convergence as feasible for practical optimization problems.

In the proposed algorithm, the network selection process is distributed to the available visitor networks to reduce the processing delay. Mobile terminal (MT) transmits the handover request to available visitor networks with estimated weight values based on application requirements. The Network Quality Values (NQVs) are computed in the visitor networks as given in equation (1) and send to mobile terminal. On receiving NQVs, mobile terminal arranges them in a list and picks the network with the highest value as the target network to execute the handoff process after the authentication process.

$$NQV_i = \frac{S^-}{S^+ + S^-} \qquad (1)$$

where, NQV_i indicates the quality of i^{th} visitor network. S^+ and S^- denote distance measures from Intuitionistic Fuzzy Positive Ideal Solution and Intuitionistic Fuzzy Negative Ideal Solution respectively.

In this work, pairing-free anonymous mobile node handover authentication method is employed for secure communication and preserving privacy of the users. It contains two stages: pre-deployment stage and handover authentication phase.

Pre-deployment Phase:

The intention of this stage is to initialize the system and create an initial setup for the upcoming handover and authentication process. Table 1 shows the notations used in this algorithm.

System Initialization:

It is presumed that the Authentication Server (AS) will carry out the system initialization process before the deployment of interworking networks. The AS performs the subsequent operations:

Step 1: Selects a k-bit prime q appropriately and finds tuple $\{F_q, E/F_q, C, D\}$

Step 2: Selects random numbers $s; r \varepsilon Z_q^*$ as the master key, and calculate the system public keys $PK_1 = sP, PK_2 = rP$

Step 3: Selects four secure hash functions H_1, H_2, H_3 and H_4

Step 4: Distributes $\{F_q, E/F_q, C, D, PK_1, PK_2, H_1, H_2, H_3, H_4\}$ as parameters of systems and maintains the master key secret

Table 1: Notations used in the Algorithm

Notations	Explanation
q	a k-bit prime
F_q	a prime finite field
E/F_q	an elliptic curve E over F_q
C	a cyclic additive group, $C = \{(x, y): x, y \epsilon E/F_q\} \cup \{\theta\}$
D	Generator for the group C
ID_x	Identity of entity x
ts	a time stamp
$H_1()$	a secure hash function $H_1: \{0,1\}^* \times C \rightarrow Z_q^*$
$H_2()$	a secure hash function $H_2: \{0,1\}^* \times \{0,1\}^* \times C \rightarrow \{0,1\}^k$
$H_3()$	a secure hash function $H_3: \{0,1\}^k \times C \rightarrow \{0,1\}^k$
$H_4()$	a secure hash function $H_4: \{0,1\}^k \times \{0,1\}^k \times \{0,1\}^k \rightarrow \{0,1\}^k$
PK	Public key
S_x	entity x's private key

Vertical Handover Authentication Phase:

A vertical handover process is performed by MT when the current serving network fails to support the user demands. In the meantime, MT initiates the key pre-distribution process before the VHO process.

a. Key Pre-distribution:

In this phase, every PoA sends its identifier ID_{PoA} to the AS. The AS calculates S_{PoA}, private key and return long term secret key tuple (ID_{PoA}, S_{PoA}) to the PoA. Likewise, MT conveys the request message with its identity ID_{MT} to AS. Then, AS verifies the validity of MT. If the requested MT is valid, AS selects a group of unlikeable pseudo-IDs $PID = pid_1, pid_2, \ldots..$ AS evaluates an equivalent private key S_{pid_i}, for every pseudo-ID and returns all tuples (pid_i, S_{pid_i}) to MT. By performing this, the MT can modify its pseudo-ID frequently to attain identity and location privacy during handover authentication stage. The private key S_{PoA} and S_{pid_i} are calculated as : $S_{PoA} = r + H_1(ID_{PoA} \| PK_2)$s and $S_{pid_i} = r + H_1(pid_i \| PK_2)s$.

After receiving the private key S_{PoA} and S_{pid_i}, the PoA and MT can certify the key by inspecting: $S_{PoA}D = PK_2 + H_1(ID_{PoA} \| PK_2)PK_1$ and $S_{pid_i}D = PK_2 + H_1(pid_i \| PK_2)PK_1$.

b. Handover Authentication Stage:

In this stage, mutual authentication between MT and new PoA is achieved. The shared Pairwise Transient Key (PTK) among them can be created directly during handover authentication. The following messages are exchanged in this stage:

Handoff from $MT \rightarrow AP/BS$: $M_i, R_{MT}, H_3(PTK_1 \| R_{PoA})$

The MT chooses a new pseudo-ID pid_i and the equivalent private key S_{pid_i}. Later, MT selects a random value $a \in Z_q^*$, that acts like a nonce, and evaluates $R_{MT} = a * D$. Moreover, let $M_i = pid_i \| ID_{PoA} \| ts$, in which ts is included by MT to cancel out replay attacks and $\|$ specifies message concatenation operation. Afterwards, the MT evaluates $b = H_4(M_i)$ and $R_{PoA} = b * D$, and evaluates public key PK_{PoA} and the shared secrets K_1. The MT calculates the session key PTK_1 using public key and shared secrets as below:

$$PK_{PoA} = PK_2 + H_1(ID_{PoA} \| PK_2)PK_1 \quad (2)$$

$$K_1 = S_{pid_i} R_{PoA} + aPK_{AP} \quad (3)$$

$$PTK_1 = H_2(pid_i \| ID_{PoA} \| K_1) \quad (4)$$

On completion of these procedures, the MT carries out a hash function on PTK_1 and R_{PoA} as the authentication value $H_3(PTK_1 \| R_{PoA})$. The MT returns M_i, R_{MT} and $H_3(PTK_1 \| R_{PoA})$ to PoA at the last part of the execution.

Handoff from PoA→ MT: $H_3(PTK_2 \| R_{MT})$

After getting the message, the PoA verifies ts, time stamp from M_i to protect from replay attack. In case this time stamp ts expires, this message will be rejected. Or else, it evaluates $b = H_4(M_i)$ and $R_{PoA} = b * D$. The PoA validates $H_3(PTK_1 \| R_{PoA})$ using MT's public key, shared secrets and session key as follows:

$$PK_{MT} = PK_2 + H_1(pid_i \| PK_2)PK_1 \quad (5)$$

$$K_2 = S_{PoA} R_{MT} + bPK_{MT} \quad (6)$$

$$PTK_2 = H_2(pid_i \| ID_{PoA} \| K_2) \quad (7)$$

The PoA carries out hash function on PTK_2 and R_{PoA} to create a verification value $H_3(PTK_2 \| R_{PoA})$. If this generated value is equal to received value $H_3(PTK_1 \| R_{PoA})$ and continues to the next step. Now, the MT is successfully authenticated. Likewise, AP/BS sends $H_3(PTK_2 \| R_{PoA})$ to MT for authentication purpose. After receiving this message, the MT verifies $H_3(PTK_2 \| T_{MT})$. If this confirmation value is correct, the PoA is fruitfully authenticated by MT. At the last of execution process, session key $PTK_1(PTK_2)$ is set up between MT and PoA to complete the mutual handover authentication process.

Attack Resistance:

It has the capability to oppose several types of attacks in wireless environment. For eavesdropping, even the attackers capture the data transmission in recently established links; the attacker cannot obtain the content of packets. It is because that PTK is used to encrypt and protect the content of packets. In this algorithm, since the key agreement is devised using Computational Diffie-Hellman, both MT and AP transmit the packets by verifying Diffie-Hellman public components and create session keys through long-term secret keys. This attains mutual authentication between the entities and thus it resists the man-in-the-middle attack. This algorithm also resist replay attack by using different time stamp ts. In this, only the legal users can obtain the long-term secret keys from the AS and thus, the spoofing and impersonation attacks are prevented.

The workflow of the proposed algorithm is presented in Figure 1.

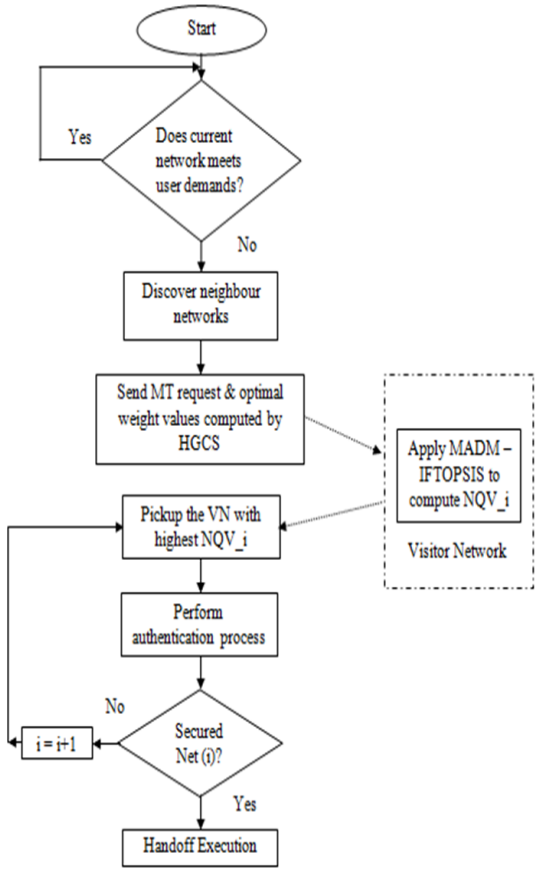


Figure 1 Context-aware based Weight Assignment TPMVHO Algorithm

IV.PERFORMANCE EVALUATION& RESULTS

The experimentation is conducted using MATLAB. It is assumed that the multi-mode capable MTs are moving arbitrarily in an overlying area of the heterogeneous wireless networks comprise WLAN, UMTS and WiMAX.

Two traffic classes, namely, Voice (real-time) and Data (non real-time) are considered. To improve the service quality provided to the users, the criteria like available bandwidth (Mbps), delay (ms), BER and Packet Loss are taken into account. Table 1 shows the most generalized attribute values of each network which are taken from various sources of literature.

Table 1: Attributes of Various Networks

Networks	Available Bandwidth (Mbps)	Delay (ms)	BER	Packet loss
WLAN 1	1~54	20~150	10^{-3}~10^{-9}	20~80
WLAN 2	1~54	20~150	10^{-3}~10^{-9}	20~80
WiMAX	1~60	30~100	10^{-3}~10^{-9}	20~80
UMTS	0.1~2	25~200	10^{-3}~10^{-9}	20~80

The simulation setup used in this work is shown in Table 2.

Table 2: Simulation Parameters

Parameter	Values
Simulator	MATLAB
Simulation Area (sq. m)	1000*1000
Simulation Time	1000 seconds
Mobile Terminals	500
Number of WLAN	2
Number of WiMAX	1
Number of UMTS	1
RSS Threshold (WLAN)	-115 dBm
RSS Threshold (WiMAX)	-110 dBm
RSS Threshold (UMTS)	-95 dBm
Range (WLAN)	100 m
Range (WiMAX)	1000 m
Range (UMTS)	3000 m
Channel Bandwidth (WLAN)	20 MHz
Channel Bandwidth (WiMAX)	10 MHz
Channel Bandwidth (UMTS)	5 MHz
Traffic Type	Voice/Data
Mobility Model	Random Way Point
Routing Protocol	QoD routing protocol

For voice applications, the attribute delay is considered as more important than BER and packet loss. The bandwidth is relatively important for this application. BER is highly prioritized to delay for data transmissions with negligible error rate. Here, the packet loss and bandwidth are relatively important for this application.

The network selection based on MT velocity and application demand is mapped in Table 3.

Table 3: Network Selection based on Application

Velocity (km/hr)	Network	Application	
		Voice	Data
LOW (<10)	WLAN	√	√
	WiMAX	√	√
	UMTS	√	√
Medium (10~80)	WLAN	X	X
	WiMAX	√	√
	UMTS	√	√
High (>80)	WLAN	X	X
	WiMAX	X	X
	UMTS	√	√

The WLAN is the most preferable network during lower mobility situations. Also it provides required bandwidth for applications. In case of non availability of WLAN, WiMAX is selected since its bandwidth is higher than UMTS. WLAN is not preferred during medium and high mobility of MTs due to its limited coverage area. Hence, the parameters from WiMAX and UMTS only are gathered to select the network. This minimizes the handover process time.

The proposed TPMVHO algorithm performance is compared with IPMVHO algorithm which does not involve security mechanism in terms of handoff events, blocking rate and throughput.

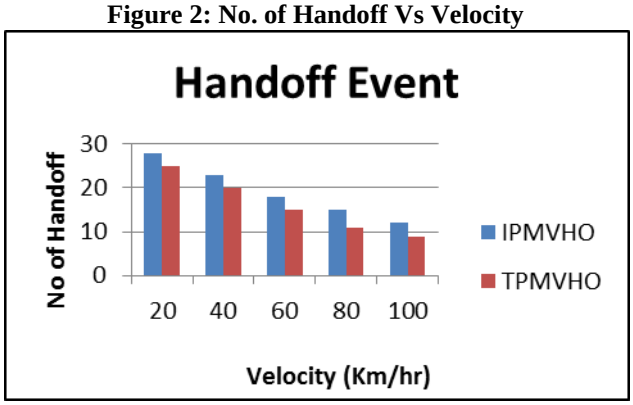
V. HANDOFF EVENTS

The handoff events are calculated for various velocities varying from 0 to 100 km/hr with an interval of 20 km/hr. From Table 4 and figure 2, it is observed that the proposed TPMVHO algorithm reduces the handoff events by 20% against IPMVHO. This is due to the inclusion of security and authentication mechanism in the vertical handoff decision algorithm. Thus, it ensures that the vertical handoff takes place in a secured way.

Table 4: No. of Handoff Vs Velocity

Velocity (Km/hr)	Handoff Events	
	IPMVHO	TPMVHO
20	28	25
40	23	20
60	18	15
80	15	11
100	12	09

Figure 2: No. of Handoff Vs Velocity



VI. BLOCKING RATE

Table 5 and Figure 3 show the reduction in blocking rate of 11.34% using TPMVHO algorithm while comparing with IPMVHO by experimenting with varying number of users. The blocking rate is found to be reduced due to the inclusion of handover authentication mechanism in the distributed vertical handoff algorithm. This reduction in blocking rate would ensure the enhancement of the bandwidth utilization, thereby providing an effective service to the users.

Table 5: Blocking Rate Vs No. of users

Number of User	Blocking Rate (%)	
	IPMVHO	TPMVHO
100	35.44	32.56
200	39.76	35.67
300	43.53	39.75
400	49.67	42.44
500	53.22	48.63

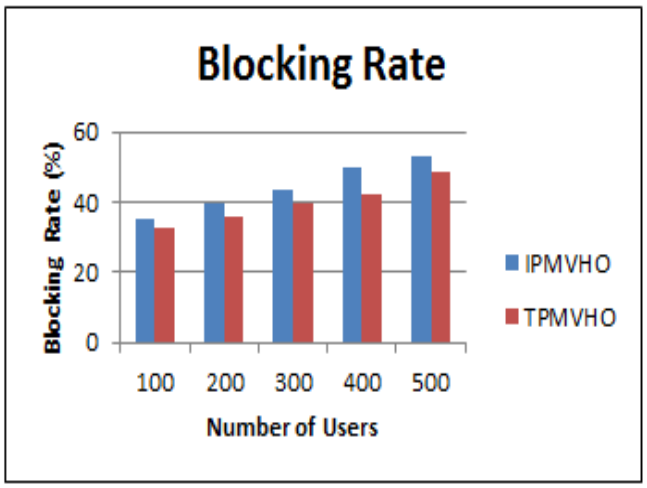


Figure 3: Blocking Rate Vs Number of Users

VII. THROUGHPUT

The TPMVHO, secured algorithm ensures the connection with the wireless network. The handoff blocking rate is observed to be low when compared to IPMVHO, unsecured algorithm. This, in turn enhances the throughput by 6.85% as shown in Table 6 and Figure 4.

Table 6 Throughput Vs Simulation Time

Simulation time (Sec)	Throughput (Mbps)	
	IPMVHO	TPMVHO
200	1.41	1.53
400	1.52	1.63
600	1.62	1.72
800	1.69	1.81
1000	1.78	1.92

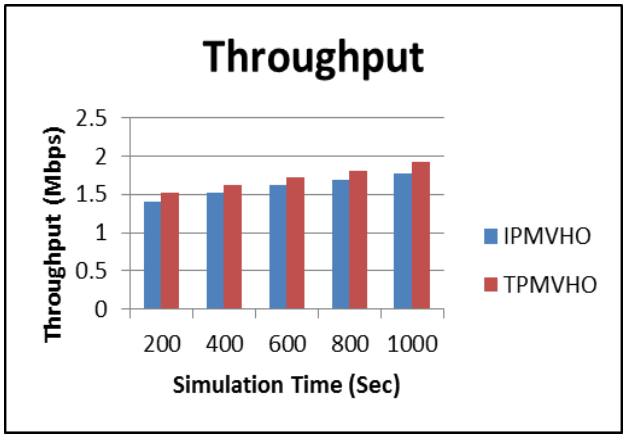


Figure 4 Throughput Vs Simulation Time

VIII. SUMMARY

The secure handoff across heterogeneous wireless access networks is a challenging issue due to the different characteristics of each network. This paper presented a novel IF-TOPSIS MADM algorithm and pairing-free anonymous mobile node handover authentication method to enhance the handover mechanism. Particularly, the novel method gives user anonymity and intractability, and attains higher competence. The experimentation outcomes prove that the proposed algorithm shows superior performance than the previous method.

REFERENCES

1. Naïm Qachri, Olivier Markowitch and Jean-Michel Dricot 2012, 'Vertical Handover Security in 4G Heterogeneous Networks: Threat Analysis and Open Challenges', Proceedings of International conference on Future Generation Information Technology, pp. 7-14.
2. Zou, Y, Zhu, J, Wang, X& Hanzo, L 2016, 'A Survey on Wireless Security: Technical Challenges, Recent Advances & Future Trends', Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765.
3. Xuefei Cao, Weidong Kou and Xiaoni Du 2010, 'A Pairing-free Identity-based Authenticated Key Agreement Protocol with Minimal Message Exchanges', Information Sciences, Elsevier, vol. 180, pp. 2895-2903.
4. SK Hafizul Islam and G. P. Biswas 2012, 'An Improved Pairing-free Identity-based Authenticated Key Agreement Protocol Based on ECC', Procedia Engineering, Elsevier, vol. 30, pp. 499-507.
5. Muhammad Waseem Khan 2013, 'Secure and Efficient Vertical Handover in Heterogeneous Wireless Networks', International Journal of Advanced Networking and Applications, vol. 5, no. 2, pp. 1908-1912.
6. Anmin Fu, Gongxuan Zhang, Yan Yu and Zhenchao Zhu 2014, 'A Privacy Preserving Vertical Handover Authentication Scheme for WiMAX-WiFi Networks', KSII Transactions on Internet and Information Systems, vol. 8, no. 9, pp. 3250-3265.
7. Guangsong Li, Qi Jiang, Fushan Wei and Chuangui Ma 2015, 'A New Privacy-aware Handover Authentication Scheme for Wireless Networks', Wireless Personal Communications, vol. 80, no. 2, pp. 581-589.
8. Xu Yang, Xinyi Huang and Joseph K. Liu 2016, 'Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing', Future Generation Computer Systems, vol 52, pp. 190-195.
9. Niranjani, D and Ganaga Durga, M 2016, 'Distributed Security Architecture for Authentication in 4G Networks', Proceedings of IEEE International Conference on Advances in Computer Applications, pp. 286-291.
10. Suman 2016, 'A Novel Authentication Algorithm for Vertical Handoff in Heterogeneous Wireless Networks', International Conference on Computing for Sustainable Global Development, pp. 3352-3357.
11. Xu Yang, Xinyi Huang and Joseph K. Liu 2016, 'Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing', Future Generation Computer Systems, vol 52, pp. 190-195.
12. Niranjani, D and Ganaga Durga, M 2017, 'Secure Cost-Effective Handover Decision and Authentication Technique for 4G Networks', International Journal of Pure and Applied Mathematics, vol. 117, no. 7, pp. 413-426.
13. Debiao He, Ding Wang, Qi Xie and Kefei Chen 2017, 'Anonymous Handover Authentication Protocol for Mobile Wireless Networks with Conditional Privacy Preservation', Science China Information Sciences, vol. 60, pp. 1-17.
14. Rui Chen, Guangqiang Shu, Peng Chen and Lijun Zhang 2017, 'Enhanced Security and Pairing-free Handover Authentication Scheme for Mobile Wireless Networks', Journal of Physics Conference Series, pp. 1-9.
15. Changji Wang, Yuan Yuan and Jiayuan Wu 2017, 'A New Privacy-preserving Handover Authentication Scheme for Wireless Networks', Sensors, pp. 1-14.
16. Vincent Omollo Nyangaresi, Silvance, O. Abeka and Anthony Rodrigues 2018, 'Secure Timing Advance Based Context-Aware Handover Protocol for Vehicular Ad-hoc Heterogeneous Networks', International Journal of Cyber-Security and Digital Forensics, vol. 7, no. 3, pp. 256-274.
17. Dongcheng Wang, Li Xu, Feng Wang and Qikui Xu 2018, 'An Anonymous Batch Handover Authentication Protocol for Big Flow Wireless Mesh Networks', EURASIP Journal on Wireless Communications and Networking, pp. 1-8.

AUTHORS

M.Dhipa completed B.E (EIE) in Easwari Engineering College, Madras University, Chennai in 2004 and M.E (Applied Electronics) in K.S.R. College of Technology, Anna University, Chennai in 2006. She is pursuing Ph.D. under Anna University, Chennai. She is having 12 years of teaching experience in various institutions. She has published about 8 papers in various International Journals. Her area of interest includes Heterogeneous Networks, Mobile Computing and IoT.

Dr. B. Kalaavathi received B.E. (Computer Science and Engineering) degree in 1993 from Bharathiyar University, M.Tech from Pondicherry University in 2000 and Ph.D from Periyar University in 2010. She is currently working as a Professor/Head in the Department of CSE in K.S.R. Institute for Engineering and Technology, Tiruchengode. She has about 24 years of experience in teaching. She is a member of CSI & ISTE INDIA. Her current areas of interest include Mobile Computing, Data Structures and Algorithms Analysis.

Dr. A.Chandrasekar received B.Sc. Degree in Computer Science from Nagamalai Navarasam Arts and Science College, Bharathiar University, Tamil Nadu, India in 1998, M.Sc. Degree in Computer Technology from K.S.R. College of Technology, Anna University, Tamil Nadu, India in 2000, M.E. in Computer Science and Engineering from K.S.R. College of Technology, Anna University, Tamil Nadu, India in 2006. He also obtained his Ph.D. Degree in Information and Communication Engineering from Anna University, Tamil Nadu, India in 2016. He is having 16 years of teaching experience in various institutions. He has published 17 papers in various International Journals. His area of interest includes Mobile Computing, Design and Analysis of Algorithms and Internet of Things