




# Probabilistic Verification Scenarios with Reduced Authentication Delay for Handoff Clients in Mesh Networks

Geetanjali Rathee<sup>1</sup>  · Naveen Jaglan<sup>2</sup> · Hemraj Saini<sup>1</sup> · Samir Dev Gupta<sup>2</sup> · Binod Kumar Kanaujia<sup>3</sup>

Published online: 12 December 2018  
© Springer Science+Business Media, LLC, part of Springer Nature 2018

## Abstract

In this paper, we have proposed a secure handoff procedure by generating and assessing the tickets for each mesh client which are divided among various zones of mesh routers depending on their transmission range. Further, a trusted third party authentication server is proposed that is responsible for generating and assigning the tickets of each mesh client which are stored distributively at mesh routers. However, during the mobility whenever the range of current serving mesh router decreases, the mesh client needs to connect to a foreign mesh router by authenticating itself in order to continue its network services. The foreign mesh router validates the authenticity of its handoff mesh client by verifying its ticket. The proposed mechanism reduces the potential issue of storage overhead and security threats at mesh clients as all the tickets are stored distributively in the database of each mesh router. The proposed technique is validated with a commercial simulator NS2 over certain network parameters and different probabilistic scenarios of authentication.

**Keywords** Handoff · Wireless mesh network · Security threats · Probabilistic authentication techniques · Authentication delay

---

✉ Geetanjali Rathee  
geetanjali.rathee123@gmail.com

Naveen Jaglan  
naveenjaglan1@gmail.com

Hemraj Saini  
hemraj1977@yahoo.co.in

Samir Dev Gupta  
samirdev.gupta@jiit.ac.in

Binod Kumar Kanaujia  
bkkanaujia@ieee.org

<sup>1</sup> Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnaghat 173234, India

<sup>2</sup> Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Wagnaghat 173234, India

<sup>3</sup> School of Computational and Integrative Sciences, Jawaharlal Nehru University (J.N.U.), New Delhi, India

## 1 Introduction

*Handoff* is considered to be an imperative procedure in order to support the mobility in the communication process. Generally, it is defined as connecting with a foreign mesh router (FMR) or new mesh router (MR) by exiting the current serving router's range due to signal reduction during the mobility [1, 2]. Wireless mesh network (WMN), an auspicious communication prototype is atypical kind of multi-hop wireless technology consisting of 2 sorts of nodes that are MRs and mesh clients (MCs) [3–5]. MRs offers the internet connectivity and act as the spine of the whole network while MCs accesses the services via MRs. Whenever a MC mobile outside the current MR range, the signal-to-noise ratio (SNR) falls due to signal reduction, therefore, the significant reduction of SNR creates the MC to search a FMR having good signal strength for enhanced services that triggers the handoff process in the network [6].

Since the nodes of WMN are mobile, limited and unstable by security with new performance concerns, a significant reduction in handoff may cause an abundant performance issues that affects the performance with the storage/communication delay and network threats [7–10]. During the handoff, it is prerequisite that mobile clients verify their authentication not only with a short impediment, but also with the defense of the mobile clients as well as the handoff process. Numbers of scientists/researchers have designed various handoff procedures by suggesting certain security mechanisms such as ticket based process, cryptographic mechanism and trusted third party mechanism [11–13]. However, the major drawback with these approaches is storage and communication overhead and key management issues. Even though, few researchers have resumed the overhead drawbacks using trusted third party approach, however, the security attacks at MCs and MRs still remain a major threat in mesh environments. Therefore, there is a need to advance the network metrics in order to ensure a resilient and secure approach during handoff [14, 15].

Although there exist various authentication procedure during handoff where third party is responsible to store and verify the mobile clients handoff. However, the proposed technique may not significantly reduce the authentication delay as all the tickets are stored at third party and MC needs to communicate with third party through various mesh routers. This manuscript aim is to propose a secure handoff mechanism that further reduces the authentication delay of previous proposed mechanism. The technical contribution of the paper is described as follows.

- An authentication server that generates and assigns the ticket to verify the mobile client's authenticity.
- Handoff procedure which explains the actual handoff mechanism in the network.
- Further authentication delay and verification process that is analyzed in different probabilistic scenarios over small (up to 25 number of nodes) and large (up to 250 number of nodes) network sizes using NS2 simulator.

The remaining structure of the paper is organized as follows. Section 2 discusses the related work. The network structure of the whole manuscript with proposed handoff mechanism is detailed in Sect. 3. Further, Sect. 4 discusses the performance evaluation of existing and proposed mechanism by showing the probabilistic scenarios of both the approaches and finally Sect. 5 concludes the paper.

## 2 Related Work

Multi-hop [16], proactive [17] and ticket-based [18] are generally three different sorts of handoff procedures that are used to authenticate the handoff clients in mesh networks. In multi-hop approaches, handoff client desires to re-authenticate itself to authentication server (AS) that is at multi-hop distance away from it while proactive authentication mechanism reduces the multi-hop distance by pre-distributing the credentials and pair-wise master keys (PMK) of log-in authentication process before moving the client to another domain. Further, ticket based handoff protocol decreases the handoff delay and storage, communication and key management overheads by distributing the tickets as successful log-in authentication.

EAP-TLS [19] and PANA [20] are the two multi-hop authentication protocols where handoff client authenticates itself to the AS by passing the source messages through multiple routers. Let us assume a scenario where there is a reduction in the SNR ratio and the handoff client needs to leave its current MR and search for new router to access its services. In order to continue its services, handoff client needs to re-authenticate itself with another router by sending a request message containing its MAC address and the base service set identifier (BSSID) of the old MR. Upon getting the request data, the new router forwards the request message to third party in order to confirm old MR. If BSSID is legal then AS will forward acceptance message to the new MR holding the security message for handoff transmission between new and old MR. Park et al. [21] have projected a proactive mechanism where after successful verification of mobile client, AS forwards a PMK to its allied MR with its client's identity. However, the major drawback of this approach is that the pre-distribution of certificates and keys acquires spare traffic overhead while in ticket verification process, client's authenticity is deliberated by verifying and generating the tickets by the AS that overcome the issues of security threats at MRs and MCs. In order to reduce security threats and handoff latency, a number of schemes have been proposed by different researchers/scientists. Further discussions explained some more effective handoff procedures related to our work. Huang et al. [22] have proposed a profligate handoff that is executed by sending a context transfer activation request (CTAR) to the new servicing MR. Before the handoff, mobile client forwards a CTAR as a token to its current MR and switches to new router's range. After getting the request from handoff client, previous MR forwards the activation token to the new router. Upon attainment in the range of new router, MC sends its activation request token to it. The new router calculates the activation token using the metrics supplied by previous router and if the token forwarded by previous MR matches with the client's token, handoff verification completes effectively. The major advantage of this technique is that handoff procedure completes with less communication steps between MC and MR, however, the technique may be prone to other performance issues such as each time handoff client needs to forward the activation request to its previous MR and the previous MR sends the request to new MR that cause significant handoff delay. Further, storage overhead exists at each MC as it has to store the CTAR into its routing table.

In order to overcome the above limitations, the authors have proposed other security techniques discussed in [23, 24], in which after completing the initial full authentication process, handoffs will be provided by deriving a PMK between individual MCs and AS, a separate PMK is consequent between each AS and MC. Before the handoff, neighboring routers interacts with AS in order to get nth PMK. Although the approach leads to significant reduced handoff delay, however, an independent PMK is needed between MC-AS that

is difficult to maintain. Further, MR needs to interrelate with AS for getting the keys that increases the communication instance in the network. A *Group-based Handoff* [25, 26] technique was proposed by Fu et al. in order to maintain a fast handoff; a group key is used among all the Base Stations (BSs). Accounting, authentication and authorization (AAA) server assigns a multi-BS group key (MGK) to all the BSs and a single MGK is used among all BSs to decrease the storage and key management overhead and effective occurrence of handoff procedure. PMK is shared between serving BS and user. The current BS computes a ticket for the handoff using MGK after recognizing the handoff client and the ticket containing a PMK that authenticates the handoff procedure. During handoff, mobile client forwards the ticket issued by current BS to the new BS and the new BS decrypts it using PMK and MGK and confirms the handoff if PMK is legitimate. The major drawback with this approach is that only a single group key is used among all the BSs so that if one of the BS is attacked, the whole network prone to threat to forge the ticket used among all the MCs.

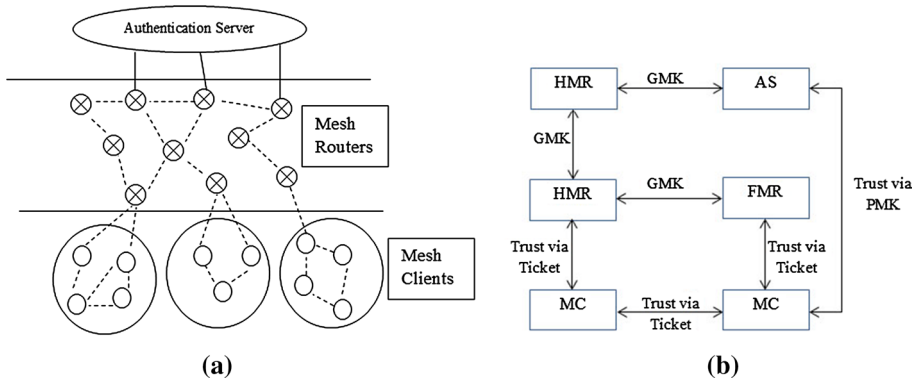
Further, the approach proposed by Xu et al. [27] that is taken as the base paper of our paper is Ticket-based Handoff approach. The author proposed a ticket based mechanism by describing the procedure into different steps (1) ticket issuing step that is used to produce the tickets for handoff mechanism and (2) re-authentication step that is done in the actual handoff verification. In ticket issuing phase, each MC and MR stores the tickets and keys of their domains into their databases where during handoff, whenever a MC enters into FMR to access the services, MRs converse with each other to identify the domain and to get the keys and ticket of the handoff client to verify its legitimacy. The major limitation with this approach is that the interaction between MRs indulges a number of security attacks i.e. message forging and DoS attacks and may lead to communication overhead and significant delay issues. Further, the storage of tickets and keys at MC does engage several resource constraints such as energy consumption, memory and storage overhead problems. Moreover, the intruders can easily attack on MCs and communicating MRs in order to modify or forge the data and affect the network performance by adding the delay process.

As per best-of-the-authors knowledge no other existing technique provides guarantee to reduced authentication delay [28] and resilient nature against the security attacks. Although various handoff procedures have been proposed; however, it may not be able to reduce the authentication process [29–32]. Therefore, the main focus of the proposed protocol is to reduce authentication delay and ensure a secure communication process under various security attacks over probabilistic scenarios of authentication verification process.

## 3 Proposed Solution

### 3.1 Proposed Network Model

The architecture of the proposed mechanism is depicted in Fig. 1a consisting of number of MRs, MCs and an AS. MCs are the one that are distributed among various domains and access the network services via MRs while an AS is a trusted third party authority that is responsible to generate the tickets for each MC and distribute it to the individual MRs in a distributed manner. MRs are the one that act as the backbone of the entire network and store the tickets distributed by AS into their databases for e.g. if there are 100 MRs and 1000 MCs then the AS will generate 1000 tickets and distribute 100 tickets to each individual MR so that even if the intruder attacks one of the MR with in a domain or MC then a



**Fig. 1** The proposed technique, **a** network architecture, **b** trust model

limited amount of information is going to be compromised. The taxonomy used throughout the proposed mechanism is depicted in Table 1.

A secure and an efficient handoff mechanism is built upon the concept of tickets, keys and AS that generates and issues the tickets; and are trusted by various entities in mesh environments.

Figure 1b represents a trust relationship model among communicating entities having certain number of devices.

1. *Trust between HMR and AS* The trust among AS and HMR is recognized via group based master key generated by the AS.
2. *Mesh Router* Any two mesh routers either FMR or HMR trust each other using GMK in a network.
3. *Mesh Router and Mesh Client* The mutual trust between routers i.e. HMR or FMR and client is recognized via AS ticket.
4. *Mesh Client* The mutual trust depends upon PMK assigned by AS and is recognized by distributing the messages between the MCs.

The complete execution of the proposed mechanism is illustrated by dividing it into three different steps such as local verification step, ticket generating-distributing step and handoff verification step. In local verification step, MC proves the validity to its HMR by distributing some local messages while in second step, AS calculates the

**Table 1** Taxonomy of the proposed approach

Abbreviations	Meaning
MC	Mesh client
MR	Mesh router
AS	Authentication server
HMR	Home mesh router
FMR	Foreign mesh router
GMK	Group based master key
MK	Master key

tickets using group based master key mutual between AS-MRs. AS assigns the same tickets to routers that are at single hop distance among each other. The advantage of subjecting same tickets is that it lessens computational overhead at AS and keys/storage overhead at MCs and MRs. The tickets stored in MR's will be used by MC and MR for the future use. Further, the handoff verification phase will be successful in step three if the metrics of the tickets propel by FMR matches with the one sent by the mobile client. If new router communicates with previous router, there is no need for full handoff. A half handoff or localized process is triggered between mobile MR and MC that lessens latency and handoff cost. There is an assumption that routers and MCs are loosely coordinated and server does the following operations prior to WMN deployment.

- AS and MRs preserve trusted relationship and set up secure connections, and
- Full authentication is done by running EAP-TLS.

### 3.1.1 Local Verification Step

After the deployment of network architecture whenever a client needs to access the services with its HMR then it can happen via distributing some messages. Initially, each MC and MR verifies to the AS with their keys and access the signature of the server for mutual authentication process as discussed below. The pictorial representation of local verification step is depicted in Fig. 2a.

1. During the initial message, MC forwards the  $ID_{MC}, ID_{HMR}, Sig_{server}$  as a message to its HMR.
2. After accessing the message from the MC, router verifies the authenticity of that client by confirming its  $sig_{server}$  and sends the message as  $ID_{MC}, ID_{HMR}, Sig_{server}$  to the client.
3. Correspondingly, if client needs to validate the MR then it may verify it by identifying the router's message.

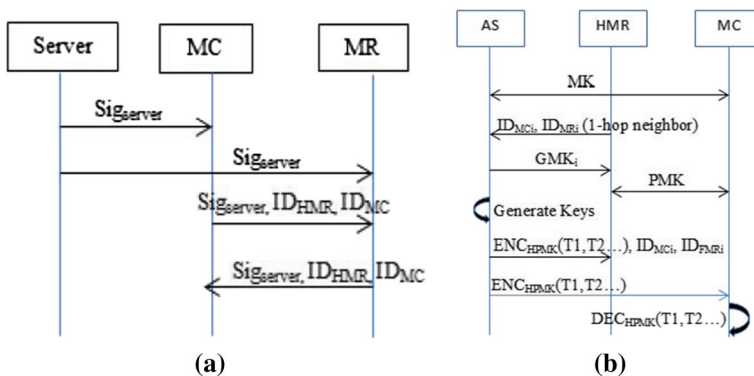


Fig. 2 The pictorial representation of **a** local authentication phase, **b** ticket generation-assigning phase

```

If ( $message_{MC} == message_{MR}$ )
    Client is trust and able to access the services
Else
    The client is not a trusted
    
```

### 3.1.2 Ticket Generating-Distributing Step

This step purpose is to generate the keys between AS-HMR, AS-MC and HMR-MC. The AS creates and assigns the tickets based on the keys produced among AS-MC. The current serving router is called as HMR and the targeted handoff router is defined as FMR. The following steps and Fig. 2b details this step.

1. A master key (MK) is produced among AS-MC to set up a secure channel with each other. Further, PMK among HMR-MC and AS-HMR is generated via MK.
2. Due to the functionality of router, each router is known of its single hop neighbor router which forwards the identity (ID) of each client and its single hop neighbor routers to AS that generates a GMK using routers' ID. Routers that are at single hop away among each other will contribute to the same master key as depicted in Table 2. Finally secure communication among HMR-MC is recognized by sharing PMK derived from MC's master key.
3. By deciding a nonce  $n$ , an expiration time  $t$  and the identities of MRs and clients, AS produces the corresponding handoff ticket  $T_i$  for the handoff verification and then assign the tickets  $T_i$  to corresponding MR <sub>$i$</sub>  for their future concern

$$TAK_i = H_{GMK_i}(ID_{HMR}, ID_{FMR}, ID_{MC}, n, t, sig_{server})$$

$$T_i = (TAK_i, ID_{HMR}, ID_{FMR}, ID_{MC}, n, t).$$

After generating the tickets Authentication Server aim is to distribute it to the individual MRs in a distributed manner in order to avoid the authentication delay during handoff. MRs are the one that act as the backbone of the entire network and store the tickets distributed by AS into their databases for e.g. if there are 100 MRs and 1000 MCs then the AS will generate 1000 tickets and distribute 100 tickets to each individual MR so that even if the intruder attacks one of the MR with in a domain or MC then a limited amount of information is going to be compromised.

**Table 2** AS routing table

MRs identity	Generated keys	Tickets
1	GMK <sub>1</sub>	Ticket <sub>1</sub>
2	GMK <sub>1</sub>	Tticket <sub>1</sub>
3	GMK <sub>1</sub>	Ticket <sub>1</sub>
4	GMK <sub>1</sub>	Ticket <sub>1</sub>
5	GMK <sub>1</sub>	Ticket <sub>1</sub>
6	GMK <sub>2</sub>	Ticket <sub>2</sub>
7	GMK <sub>2</sub>	Ticket <sub>2</sub>

### 3.1.3 Handoff Verification Step

The main objective of our manuscript is to reduce the authentication delay. Therefore, in this step, AS after generating the clients tickets will distribute randomly to their corresponding MR's domain. This mechanism reduces the authentication verification process as handoff client request their tickets to their HMR and reduces risk of intruders as tickets are not stored at MC database and each router store some tickets so that even if it is hacked by an intruder, then it may not affect the entire network performance. The handoff verification step takes place when there is reduction in the SNR among HMR to mobile MC due to increase of interaction distance. The below steps discuss the interaction steps encountered during handoff verification step.

- Initially handoff client searches for an  $FMR_i$  depending upon its good SNR ratio. The  $FMR_i$  is chosen by taking the distance among MC-MR. A threshold of SNR is decided that is computed as signal strength shown in Eq. 1. Routers having significant signal strength will be chosen as  $FMR_i$

$$signal\ strength = \frac{Distance}{SNR}. \quad (1)$$

During the simulation environment, the distance among MRs is known as the signal strength depends on SNR value and the routers. From the known distance, it is easy to compute the signal strength. The node that is mobile can initiate the handoff and gets better signal strength.

- After generating the tickets, AS will randomly distribute the tickets to the corresponding domains' mesh routers. Upon request, AS will send the ticket of handoff MC to HMR and FMR where the handoff client is reaching. The advantage of this mechanism is that once the FMR authenticates a handoff MC, it will store the its corresponding ticket into its database so that next time when the same MC reaches to same FMR range, the transfer of ticket between HMR-FMR reduces.
- Now, during the mobility, handoff client will request for ticket  $T_i$  from its HMR. As FMR already stores it tickets sent by AS, FMR verifies the ticket  $T_i$  of that MC after matching with its stored ticket.

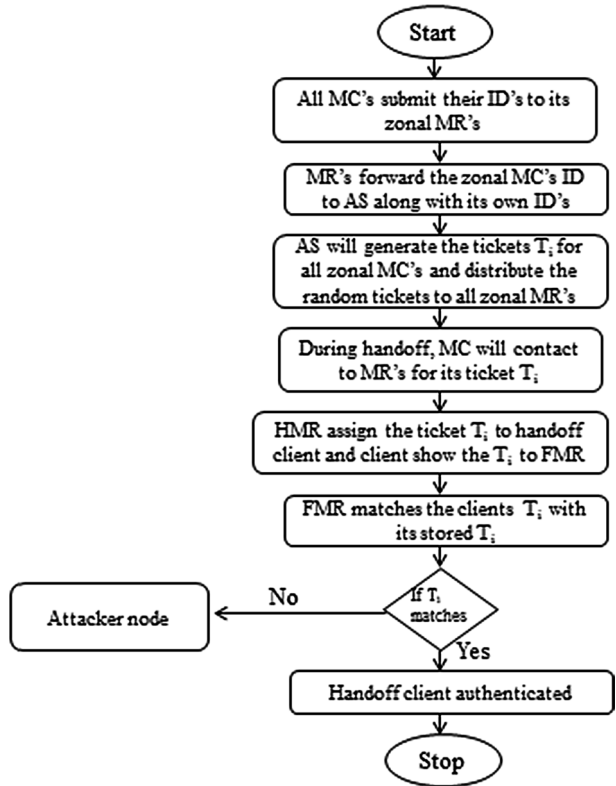
```

If (handoff  $MC_{Ticket} == FMR_{Ticket}$ ) then
    The client is verified
Else
    The client is not verified
  
```

The flowchart of proposed handoff mechanism is depicted in Fig. 3 where the AS will generate the tickets of each MC corresponding to their domains' MRs and distribute the tickets to the individual MRs. During the handoff process, MC will connect to their domain MRs accessing their tickets in order to overcome the authentication delay and security threats.



**Fig. 3** Flowchart of the proposed secure handoff mechanism



### 4 Performance Evaluation

For the purpose of simulating the existing and proposed approach, the simulation is done over NS2 simulator. The environmental setup for simulation is presented in Table 3 where 500 m × 500 m network area is constructed having small and large network sizes consisting of 25 and 250 number of nodes respectively. The clients are mobile in nature means they can leave their HMR and connect to other HMRs range at any time and the mobility speed of mesh clients is setup as 0–5 m/s with the transmission range of 25 m/s. Further the communication ranges of MAP routers are 120 m/s and MAC layer

**Table 3** The networking parameters of the existing and proposed technique

Network parameter	Value
Network area	500 m × 500 m
Number of nodes	25,250
MAC	802.11
Simulation time	60 s
Mobility speed	0–5 m/s
Clients	5200
Mesh clients transmission range	0–25 m/s

protocol used is 802.11. The simulation time for the experiment is setup as 60 s. The architecture of WMN proposed in the manuscript have AS that is responsible for producing the tickets to mesh routers and clients, two internet gateway routers IGW that provide the connection among mesh routers and internet and MRs that offers the services to clients to actually utilize the services. As shown in Fig. 1a, MRs is distributed into different zones that provide the services to their zonal or domain's mesh clients as HMR. The domains are produced according to transmission range of mesh clients with their HMR. The clients having good SNR from their HMR are measured as one domain.

This manuscript aim is to optimize the verification delay and analyze the results with different probabilistic scenarios i.e. no authentication, false authentication and correct authentication.

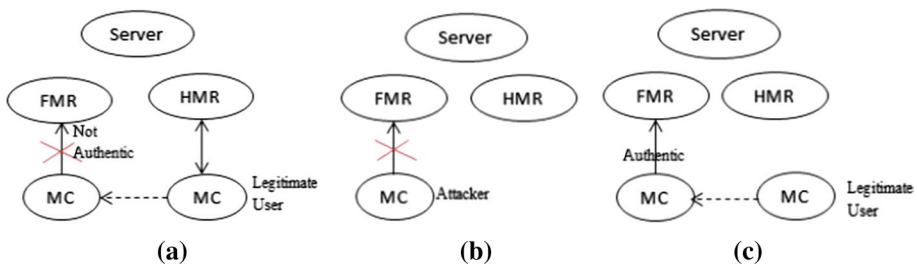
*Authentication Delay* is described as how much time the mechanism requires re-authenticating the handoff client. Here, a network of 200 mobile clients is constructed having the mobility rate of 0–5 m/s. Further, both the approaches are analyzed under different probabilistic scenarios such as *No authentication* where a malicious user or an attacker is proficient to authenticate itself with the FMR and the FMR identifies that it is an attack. *False authentication* is a situation where the mobile client is justifiable; however, the FMR is unable to authenticate it. Both the approaches existing and proposed are experimented under this scenario that is how many times a mobile client is able to verify itself with the FMR. Further, *Correct authentication* is when a legitimate mobile client verifies itself with the FMR and is able to validate it.

Both the techniques [existing (considered as the basic) and proposed] are analyzed under three different scenarios (as depicted in Fig. 4a–c) over small and large network sizes and analyzed how many times a mobile client comes under no authentication, false authentication and correct authentication.

The numerical values of evaluated parameters such as average authentication delay, maximum authentication delay, false authentication, no authentication and correct authentication over small and large network sizes are detailed in Tables 4 and 5. Further, Figs. 5, 6, 7, 8, 9, 10, 11, and 12 depicts the evaluated graphs corresponding to the listed tables. The detailed explanation of each graph is discussed in the below text.

### 4.1 Results Discussion

Figure 5 depicts the average and maximum authentication delay of existing and proposed approaches in small network sizes over different mobile clients. It can be clearly



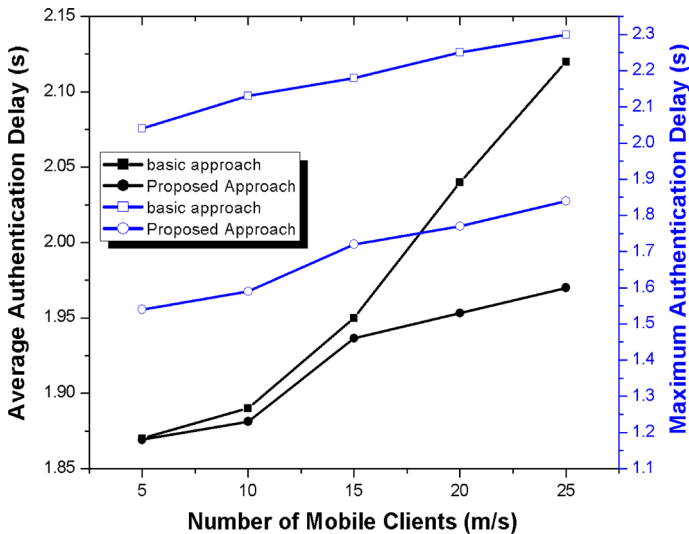
**Fig. 4** Authentication probabilistic scenarios, **a** false authentication, **b** no authentication, **c** correct authentication

**Table 4** Simulation result values for small network sizes

Number of mobile clients	Average authentication delay		Maximum authentication delay		No authentication		False authentication		Correct authentication	
	Basic	Proposed	Basic	Proposed	Basic	Proposed	Basic	Proposed	Basic	Proposed
<i>Small network size (number of mobile clients)</i>										
5	1.87	1.18	2.04	1.54	2.12	1.87	7.54	6.11	2.32	3.23
10	1.89	1.23	2.13	1.59	2.33	1.92	7.55	6.12	2.11	3.11
15	1.95	1.46	2.18	1.72	2.48	1.98	7.67	6.23	2.03	3.09
20	2.04	1.53	2.25	1.77	2.56	2.13	7.77	6.24	1.97	2.97
25	2.12	1.60	2.30	1.84	2.64	2.24	7.81	6.32	1.88	2.88

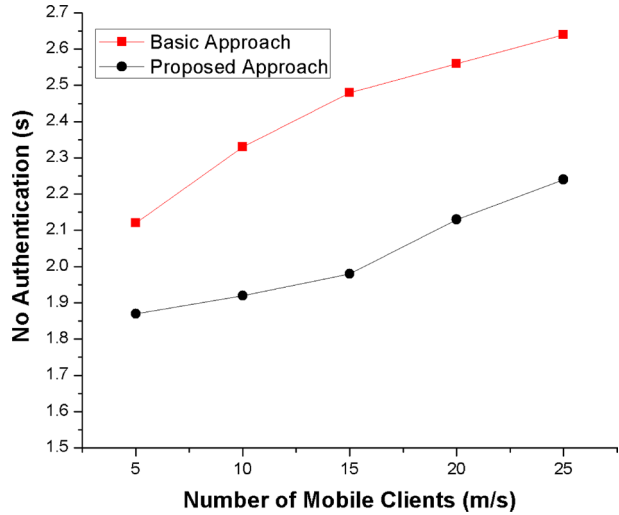
**Table 5** Simulation result values for large network sizes

Number of mobile clients	Average authentication delay		Maximum authentication delay		No authentication		False authentication		Correct authentication	
	Basic	Proposed	Basic	Proposed	Basic	Proposed	Basic	Proposed	Basic	Proposed
<i>Large network size (number of mobile clients)</i>										
50	0.51	0.32	0.58	0.34	0.89	0.58	5.97	4.33	3.84	5.34
100	0.75	0.43	0.86	0.63	1.25	0.94	6.46	4.65	3.55	4.68
150	1.03	0.82	1.24	0.99	1.78	1.30	6.90	5.11	2.94	4.11
200	1.45	0.97	1.76	1.35	2.14	1.75	7.24	5.78	2.32	3.58
250	1.98	1.24	2.21	1.68	2.67	2.18	7.88	6.21	1.87	2.74

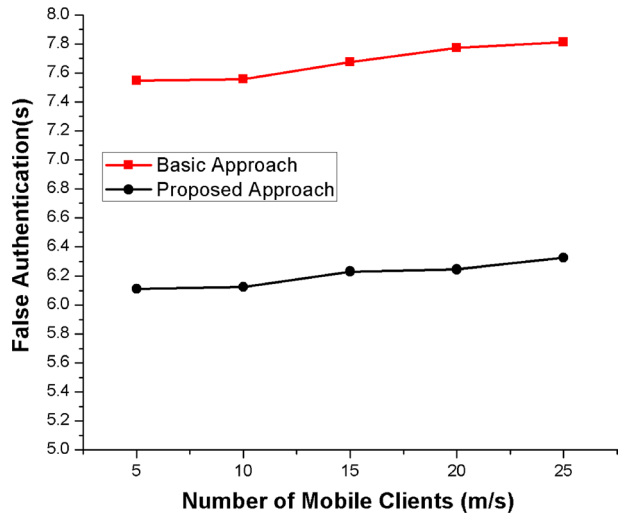


**Fig. 5** The effects of number of mobile clients over average and maximum authentication delay

**Fig. 6** The effects of number of mobile clients over no authentication delay

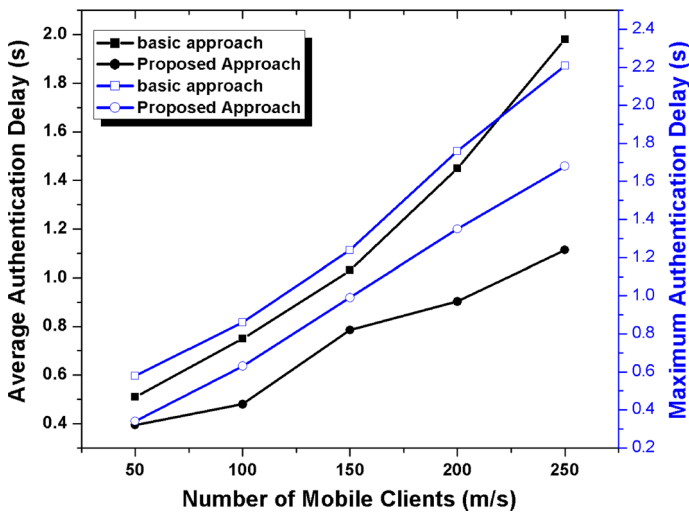
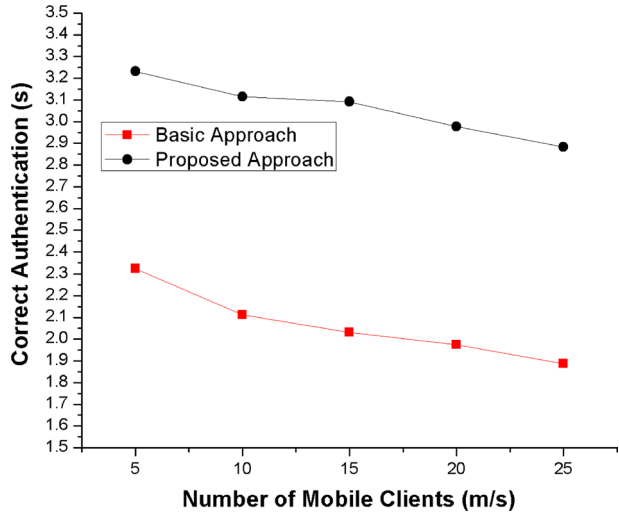


**Fig. 7** The effects of number of mobile clients over false authentication



seen in the graph that the average and maximum authentication delay of proposed approach is less as compared to the basic approach. Initially, during the network establishment where clients enters inside the network and starts the transmission process, the time required to initially authenticate the MCs in another domain is always more than the clients that visits the same network again. The measured authentication values (average or maximum) of proposed approach are depicted in Fig. 5 where AS distributes the tickets to corresponding MRs domain in order to verify the MCs authenticity. Whenever a MC again moves to same domain FMRs range, the authentication delay of that MC will be less as the previous history of that client is already stored in its database. While in case of basic approach, FMR needs to communicate with the HMR for every client and does not save any record in its database. So that if same client moves to same FMRs range, the entire authentication process repeats again.

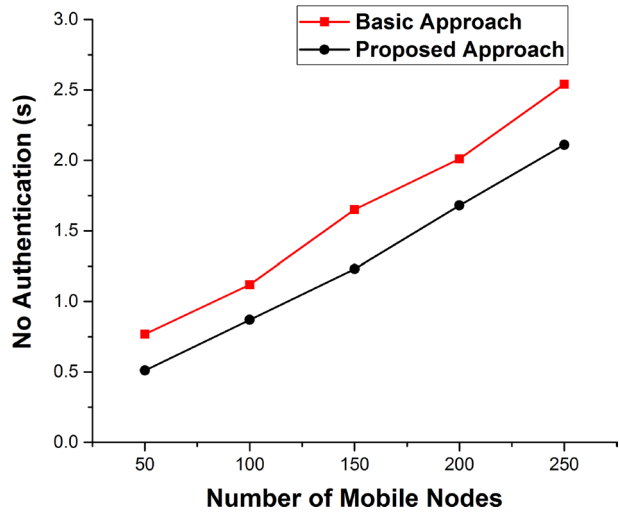
**Fig. 8** The effects of number of mobile clients over correct authentication



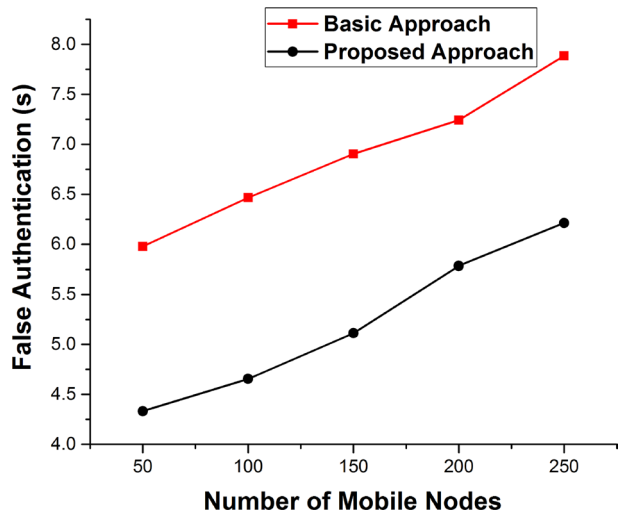
**Fig. 9** The effects of number of mobile clients over average and maximum authentication delay

Further, Figs. 6, 7 and 8 presents no, false and correct authentication graphs which shows that the proposed approach performs better as compare to existing approach. The reason is that, in proposed approach, the AS generates the tickets and randomly distributes only to their corresponding HMRs. During the mobility, whenever the handoff MC requests for their tickets to the corresponding HMRs, if intruders compromised one or more MC, then it may not affect the network performance as the authenticity is checked by the MRs. Furthermore, if intruders compromise some of the MRs then only few tickets which are stored in that particular MR domain are leaked which may further does not able to affect the entire network performance. The remaining MRs that are not compromised by the intruders may successfully identify the legitimate MCs. While in case

**Fig. 10** The effects of number of mobile clients over no authentication



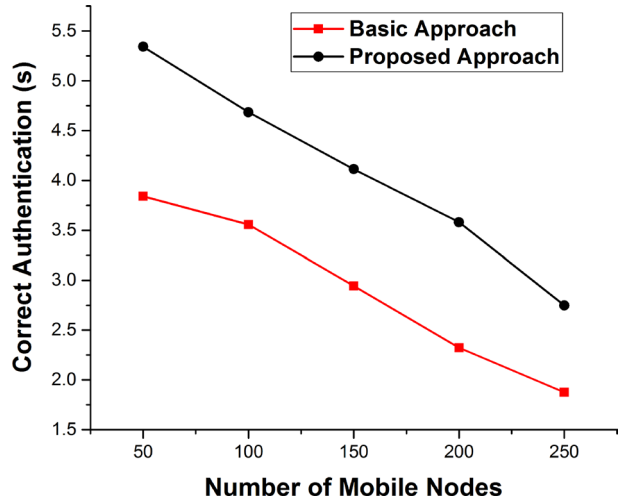
**Fig. 11** The effects of number of mobile clients over false authentication



of existing approach, all the tickets are stored at MR as well as at MC database where intruders may easily compromise MCs and can prove their authenticity in the network by forging the legitimate MC identity.

Further, the same parameters are measured against existing network sizes where network is already established while the MC are increasing inside the network. Whenever, the number of MC move from one domain to another, the authentication delay and verification procedure would be very less as compare to the existing phenomenon because each FMR maintain a history of their previous visited handoff MC into their databases and tickets are randomly distributed to their domains MRs. Figures 9, 10, 11 and 12 presents the authentication delay and verification procedure over large network sizes such as 100, 150, 200, 250. The major advantage of proposed phenomenon is that reduced authentication delay (as the tickets are stored at MR's database) and improved security

**Fig. 12** The effects of number of mobile clients over correct authentication



(even if one of the MR or entire domain is encountered by an attacker, the remaining network becomes unaffected) is provided due to distributed assignment of tickets by the AS. However, in case of existing approach, the MRs does not maintain a database, every time FMRs needs to re-authenticate the same handoff MC if it visits the same FMR again. Further, all the tickets and keys are stored at MR as well as MCs database where intruders may directly attack one or more of MR or MC and easily forge the users' security.

## 5 Conclusion and Future Work

In this paper, we have proposed a secure handoff procedure by generating and assigning the tickets for each mesh client that are divided among various zones of mesh routers depending on their communication range. Further, a trusted third party authentication server is proposed that distributes the tickets to the corresponding mesh routers domains. The proposed approach has significantly resolved the issues of communication and storage overhead of MRs and MCs and security threats during the mobility of the clients in another domain. The existing and proposed approaches are simulation over NS2 to validate the network performance results against maximum and no authentication delay. Further, both the approaches are validated against different probabilistic scenarios such as no authentication, false authentication and correct authentication process. During the network establishment or handoff process, each mesh must be granted with the unique identification key by the authentication server in order to recognize the hand-off clients for the verification process that will be measured in future communication.

## References

- Zhu, L., Yu, F. R., Tang, T., & Ning, B. (2017). Handoff performance improvements in an integrated train-ground communication system based on wireless network virtualization. *IEEE Transactions on Intelligent Transportation Systems*, 18(5), 1165–1178.
- Zhou, Z., Zhang, H., & Sun, Z. (2017). An improved privacy-aware handoff authentication protocol for VANETs. *Wireless Personal Communications*, 97(3), 3601–3618.
- Khan, S., & Pathan, A. S. K. (2013). *Wireless networks and security issues, challenges and research trends*. London: Springer.
- Dykema, K. A., Bouws, B. K., Doman, T. J., Leete, III, L. F. Schenck, W. C., & Guthrie, W. E. (2013). *Wireless mesh network*. U.S. Patent 8,274,928.
- Wang, Z., Luo, Z. X., Zhang, J. L., & Saucan, E. (2016). ARAP++: An extension of the local/global approach to mesh parameterization. *Frontiers of Information Technology and Electronic Engineering*, 17(6), 501–515.
- Srivatsa, A. M., & Xie, J. (19 May 2008). A performance study of mobile handoff delay in IEEE 802.11-based wireless mesh networks. In *Proceedings of 1st international conference on communications* (pp. 2485–2489). Beijing: IEEE.
- Khabiri, M., & Ghaffari, A. (2018). Energy-aware clustering-based routing in wireless sensor networks using cuckoo optimization algorithm. *Wireless Personal Communications*, 98(3), 2473–2495.
- Babu, M. R., & Usha, G. (2016). A novel honey pot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET. *Wireless Personal Communications*, 90(2), 831–845.
- Poongodi, T., & Karthikeyan, M. (2016). Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. *Wireless Personal Communications*, 90(2), 1039–1050.
- Purohit, K. C., Dimri, S. C., & Jasola, S. (2017). Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad hoc network (VANET). *Wireless Personal Communications*, 97(4), 5099–5114.
- Anita, X., Bhagyaveni, M. A., & Manickam, J. M. L. (2015). Collaborative lightweight trust management scheme for wireless sensor networks. *Wireless Personal Communications*, 80(1), 117–140.
- Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications*, 87(3), 1037–1055.
- Rathee, G., Saini, H., & Singh, G. (2018). Aspects of trusted routing communication in smart networks. *Wireless Personal Communications*, 98(2), 2367–2387.
- Luo, M., & Wan, Y. (2018). An enhanced certificate less signcryption in the standard model. *Wireless Personal Communications*, 98(3), 2693–2709.
- Bala, S., Sharma, G., & Verma, A. K. (2016). PF-ID-2PAKA: Pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks. *Wireless Personal Communications*, 87(3), 995–1012.
- Cato, N. (2016). On next generation network security. *IEEE Network*, 31(2), 1–2.
- Mansfield-Devine, S. (2017). File-less attacks: Compromising targets without malware. *Network Security*, 17(4), 7–11.
- Xie, J., Hu, Y. P., Gao, J. T., & Gao, W. (2016). Efficient identity-based signature over NTRU lattice. *Frontiers of Information Technology and Electronic Engineering*, 17(2), 135–142.
- Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2015). An efficient two-factor user authentication scheme with unlink ability for wireless sensor networks. *Journal of Peer-to-Peer Networking and Applications*, 8(6), 1070–1081.
- Shrivastava, G., Sharma, K., & Rai, S. (2010). The detection and defense of DoS and DDoS attack: A technical overview. *Proceedings of ICC*, 27, 274–282.
- Abbas, F., & Oh, H. (2014). A step towards user privacy while using location-based services. *Journal of Information Processing Signals*, 10(4), 618–627.
- Zhang, H., Cheng, P., Shi, L., & Chen, J. (2016). Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 24(3), 843–852.
- Tseng, Y. M. (2009). USIM-based EAP-TLS authentication protocol for wireless local area networks. *Computer Standards & Interfaces*, 31(1), 128–136.
- Jayaraman, P., Lopez, R., Ohba, Y., Parthasarathy, M., & Yegin, A. (2008). *Protocol for carrying authentication for network access (PANA)*. Framework no. RFC 5193.
- Park, C., Hur, J., Kim, C., Shin, Y. J., & Yoon, H. (2006). Pre-authentication for fast handoff in wireless mesh networks with mobile APs. In *Proceedings of international workshop on information security applications* (pp. 349–363). Berlin: Springer.



26. Huang, C. M., & Li, J. W. (2009). A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture. *Wireless Communications and Mobile Computing*, 9(10), 1387–1401.
27. Ruj, S., Nayak, A., & Stojmenovic, I. (2013). Pairwise and triple key distribution in wireless sensor networks with applications. *IEEE Transactions on Computers*, 62(11), 2224–2237.
28. Dalal, R., Singh, Y., & Khari, M. (2012). A review on key management schemes in MANET. *International Journal of Distributed and Parallel Systems*, 3(4), 165–172.
29. 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.
30. Fu, A., Zhang, Y., Zhu, Z., Jing, Q., & Feng, J. (2012). An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network. *Computers and Security*, 31(6), 741–749.
31. Xu, L., He, Y., Chen, X., & Huang, X. (2014). Ticket-based handoff authentication for wireless mesh networks. *Computer Networks*, 73, 185–194.
32. Li, J., Chen, X., Li, M., Li, J., Lee, P. P., & Lou, W. (2014). Secure de-duplication with efficient and reliable convergent key management. *IEEE Transactions on Parallel and Distributed Systems*, 25(6), 1615–1625.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Geetanjali Rathee** received B.Tech. Degree in Computer Science and Engineering from MDU Rohtak, Haryana in the year 2011. She has completed her M.Tech. in Computer Science and Engineering from Jaypee University, Wagnaghat, Solan in the year 2014. She obtained her Ph.D. in Computer Science and Engineering from Jaypee University, Wagnaghat, Solan in the year 2017. Currently, she is working as an Assistant Professor in Computer Science and Engineering Department in Jaypee University, Wagnaghat, Solan. Her research interest include resiliency in wireless mesh network, routing protocols, network protocols and security in next generation communication systems, security aspects in cognitive radio network.



**Naveen Jaglan** was born in 1989, obtained his B.Tech. and M.Tech. degree in Electronics and Communication Engineering in 2009 and 2011 respectively from Kurukshetra University, Kurukshetra, India. He obtained his Ph.D. degree on Microstrip antennas in Jaypee Institute of Information Technology Noida in 2016. He has authored/co-authored several research papers in referred International Journals and Conferences. He is also a co-author in the Handbook of Research on Advanced Trends in Microwave and Communication Engineering published by IGI Global Publishers USA. His research has included microwave communications, planar and conformal microstrip antennas including array mutual coupling, EBG, PBG, FSS, DGS, novel antennas, UWB antennas, MIMO systems, numerical methods in electromagnetics, composite right/left handed (CRLH) transmissions and High-k dielectrics. His skill includes modelling of antenna and RF circuits with Ansoft HFSS/CST Microwave Studio/ADS Momentum, measurements using Vector Network Analyzer and Anechoic Chamber.



**Hemraj Saini** is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnaghat-173234 India. He has received his Ph.D. from Utkal University, Bhubaneswar, India in 2012, M.Tech. from Punjabi University, Patiala, India and B.Tech. from NIT Hamirpur, India in 2005 and 1999, respectively. He is having more than 16 years of teaching and R&D experience. He has published around 100 research papers in journals and conferences of international repute. He has organized National and International conferences sponsored by agencies like IEEE, CSI, AICTE, CSIR, DST etc. He is the member of different professional technical and scientific associations such as IEEE (Mem. No. 92738007), ACM (Mem. No. 5156611), IAENG (Mem. No. 133186), etc. Presently he is providing his services in various modes like, reviewer for different reputed journals and conferences and also the Member of Editorial boards and Technical Program Committees.



**Samir Dev Gupta** obtained his B.E. (Electronics) from Bangalore University (University Visvesvaraya College of Engineering, Bangalore), M.Tech. (Electrical Engineering) from I.I.T. Madras, M.Sc. (Defence Studies) from Madras University, and Ph.D. from J.I.I.T. Noida. He is currently designated as Director and academic head of Jaypee University of Information Technology (JUIT) Wagnaghat, Solan, H.P., India. He has over three and a half decades of work experience in the areas of avionics, communication, radar systems and teaching at UG and PG level. His teaching career spans over 22 years and 6 months includes in addition to teaching at JIIT, Noida since December 2002, teaching at Institute of Armament Technology under Pune University, now Defence Institute of Advanced Technology (Deemed University) for PG programmes and training and development needs of Indian Air Force (I.A.F.) and Defence Research and Development Organization (D.R.D.O.), Air Force Technical College (A.F.T.C.), Bangalore where graduate engineers from IIT's, NIT's and Indian and foreign Universities undergo Aeronautical Engineering (Electronics) course for about

18 months prior joining Technical Officers' branch of the I.A.F. and Advanced Stage Trade Training Wing at Guided Weapon Training Institute, Baroda He was also a recognized postgraduate teacher in microwave communication at Pune University. His research interest is in the area of conformal microstrip patch antenna for aircraft systems. His publications in referred journals and conferences are well cited. His previous assignments includes, Deputy Director at Air Headquarters and were involved in planning, coordinating and directing maintenance, modification of aircraft and helicopter systems, modifications and induction of advance electronic systems into I.A.F., Commanding Officer of an 8 GHz LOS microwave communication unit, Senior Engineer looking after maintenance of airfield navigation aids, techno-logistic management of ground based communication equipment as Aeronautical Engineering (Electronics) Branch officer of the I.A.F., Chairman Communication Advisory Committee at I.A.T. Pune. He is qualified for first and second line servicing of Mirage-2000 aircraft. Work experience on Mirage Mission Simulator and fly by wire systems of Mirage-2000 aircraft. Led and supervised highly qualified and skilled engineering officers and technicians of I.A.F. in maintenance and operation of missile, radar and communication systems. Experienced in management of resources to achieve time bound targets and objectives viz. successfully implemented contract with international and national agencies for induction of Unmanned Aerial Vehicle, Portable Laser Designating Systems and up gradation of aircraft simulators for the I.A.F. Prior to joining JUIT Wagnaghat as Director and academic head, he was a Professor in the department of ECE at Jaypee Institute of Information Technology (JIIT), Noida. He also initiated training and placement process for JIIT, Noida. Successfully placed first and second batch students of Jaypee Education System in top-notch national and multinational organizations through campus recruitment. He has been associated at JIIT, Noida in students' welfare and discipline as Associate Dean of Students and Chairman Proctorial Board respectively.



**Binod Kumar Kanaujia** had completed his B.Tech. in Electronics Engineering from KNIT Sultanpur, India in 1994. He did his M.Tech. and Ph.D. in 1998 and 2004; respectively from Department of Electronics Engineering, Indian Institute of Technology Banaras Hindu University, Varanasi, India. He has been awarded Junior Research Fellowship by UGC Delhi in the year 2001–2002 for his outstanding work in electronics field. He has keen research interest in design and modelling of microstrip antenna, dielectric resonator antenna, left handed metamaterial microstrip antenna, shorted microstrip antenna, ultra-wideband antennas, reconfigurable and circular polarized antenna for wireless communication. He has been credited to publish more than 150 research papers with more than 800 citations with h-index of 15 in peer-reviewed journals and conferences. He had supervised 50 M. Tech. and 08 Ph.D. research scholars in the field of microwave engineering. He is a reviewer of several journals of international repute i.e. IET Microwaves, Antennas and Propagation, IEEE Antennas and Wireless Propagation Letters, Wireless Personal Communications,

Journal of Electromagnetic Wave and Application, Indian Journal of Radio and Space Physics, IETE Technical Review, International Journal of Electronics, International Journal of Engineering Science, IEEE Transactions on Antennas and Propagation, AEU-International Journal of Electronics and Communication, International Journal of Microwave and Wireless Technologies, etc. Dr. Kanaujia had successfully executed 04 research projects sponsored by several agencies of Government of India i.e. DRDO, DST, AICTE and ISRO. He is also a member of several academic and professional bodies i.e. IEEE, Institution of Engineers (India), Indian Society for Technical Education and The Institute of Electronics and Telecommunication Engineers of India.