Security of Handoff Latency by Prescanning with help of Neighbourgraph

Debabrata Sarddar
Department of Electronics and Telecommunication Engg, Jadavpur University, Kolkata – 700032

Shubhajeet Chatterjee
Department of Electronics and Communication Engg, Institute of Engg. & Managment college, saltlake, Kolkata-700091.

Pulak Mazumder
Department of Electronics and Telecommunication Engg, Regent Education & Research Foundation, Barracpore

Arnab Raha
Department of Electronics and Telecommunication Engg, Jadavpur University, Kolkata – 700032

Karmajyoti Panigrahi
Department of EIE, Techno India College of Technology College, Newtown.

Utpal Biswas
Department of Computer Science and Engg, University of Kalyani, Nadia, West Bengal, Pin- 741235.

Mrinal Kanti Naskar
Department of Electronics and Telecommunication Engg, Jadavpur University, Kolkata – 700032

ABSTRACT
Due to rapid growth in IEEE 802.11 based Wireless Local Area Networks (WLAN), handoff has become a burning issue. A mobile station (MS) requires handoff when it travels out of the coverage area of its current access point (AP) and tries to associate with another AP. But handoff delays provide a serious barrier for such services to be made available to mobile platforms. Throughout the last few years there has been plenty of research aimed towards reducing the handoff delay incurred in the various levels of wireless communication. In this paper, based on Neighbor Graph Cache (NGC), we introduce a pre-scanning mechanism in which an STA starts scanning before it needs actual handoff. The simulation results show that the proposed method reduces the handoff latency effectively.

Keywords
IEEE 802.11, Handoff latency, GPS (Global Positioning System), Base Station (BS), Mobile Station (MS), Neighbor APs.

1. INTRODUCTION
Handoff has become an essential criterion in mobile communication system especially in urban areas, owing to the limited coverage area of Access Points (AP). Whenever a MS move from current AP to a new AP it requires handoff. For successful implementation of seamless Voice over IP communications, the handoff latency should not exceed 50ms. But measurements indicate MAC layer handoff latencies in the range of 400ms which is completely unacceptable and thus must be reduced for wireless networking to fulfil its potential.

With the advent of real time applications, the latency and packet loss caused by mobility became an important issue in Mobile Networks. The most relevant topic of discussion is to reduce the IEEE 802.11 link-layer handoff latency. IEEE 802.11 MAC specification [1] defines two operation modes: ad hoc and infrastructure mode. In the ad hoc mode, two or more stations (STAs) recognize each other through beacons and hence establish a peer-to-peer relationship. In infrastructure mode, an AP provides network connectivity to its associated STAs to form a Basic Service Set (BSS). Multiple APs form an Extended Service Set (ESS) that constructs the same wireless networks.

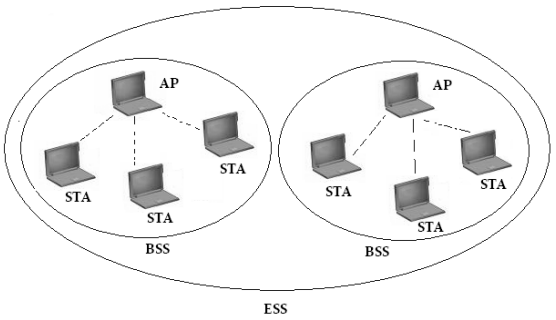

Figure 1.

1.1. Channel distribution
IEEE802.11b and IEEE802.11g operates in the 2.4GHz ISM band and use 11 of the maximum 14 channels available and are hence compatible due to use of same frequency channels. The

channels (numbered 1to14) are spaced by 5MHz with a bandwidth of 22MHz, 11MHz above and below the centre of the channel. In addition there is a guard band of 1MHz at the base to accommodate out-of-band emissions below 2.4GHz. Thus a transmitter set at channel one transmits signal from 2.401GHz to 2.423GHz and so on to give the standard channel frequency distribution as shown in [Figure.2].

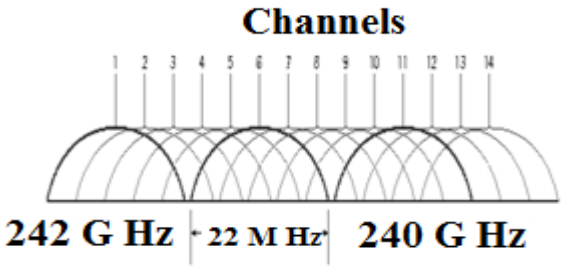

Figure.2 Channel Distribution

It should be noted that due to overlapping of frequencies there can be significant interference between adjacent APs. Thus, in a well configured network, most of the APs will operate on the non-overlapping channels numbered 1, 6 and 11.

1.2. Handoff

When a MS moves out of reach of its current AP it must be reconnected to a new AP to continue its operation. The search for a new AP and subsequent registration under it constitute the handoff process which takes enough time (called handoff latency) to interfere with proper functioning of many applications.

Three strategies have been proposed to detect the need for hand off[2]:

1)mobile-controlled-handoff (MCHO):The mobile station(MS) continuously monitors the signals of the surrounding base stations(BS)and initiates the hand off process when some handoff criteria are met.

2)network-controlled-handoff (NCHO):The surrounding BSs measure the signal from the MS and the network initiates the handoff process when some handoff criteria are met.

3)mobile-assisted-handoff (MAHO):The network asks the MS to measure the signal from the surrounding BSs. The network make the handoff decision based on reports from the MS.

Handoff can be of many types:

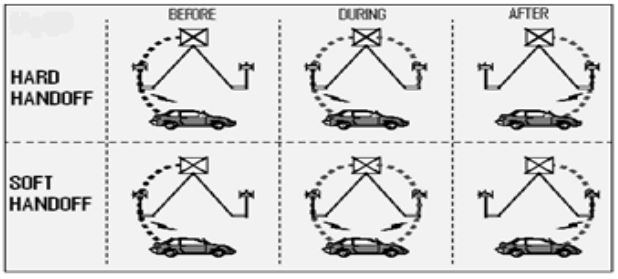

Figure 3.

Hard & soft handoff: Originally hard handoff was used where a station must break connection with the old AP before joining the new AP thus resulting in large handoff delays. However, in soft handoff the old connection is maintained until a new one is established thus significantly reducing packet loss as shown in figure 3.

In NGWS(next generation wireless system),two types of handoff scenarios arise: horizontal handoff, vertical handoff[3][4].

- *Horizontal Handoff:* When the handoff occurs between two BSs of the same system it is termed as horizontal handoff. It can be further classified into two:
  - *Link layer handoff* : Horizontal handoff between two BSs that are under the same foreign agent(FA).
  - *Intra system handoff* : Horizontal handoff between two BSs that belong to two different FAs and both FAs belong to the same gateway foreign agent (GFA) and hence to the same system.
- *Vertical Handoff* : When the handoff occurs between two BSs that belong to two different GFAs and hence to two different systems it is termed as vertical handoff .

The handoff procedure consists of three logical phases where all communication between the mobile station undergoing handoff and the APs concerned is controlled by the use of IEEE802.11 management frames as shown below in [fig4].

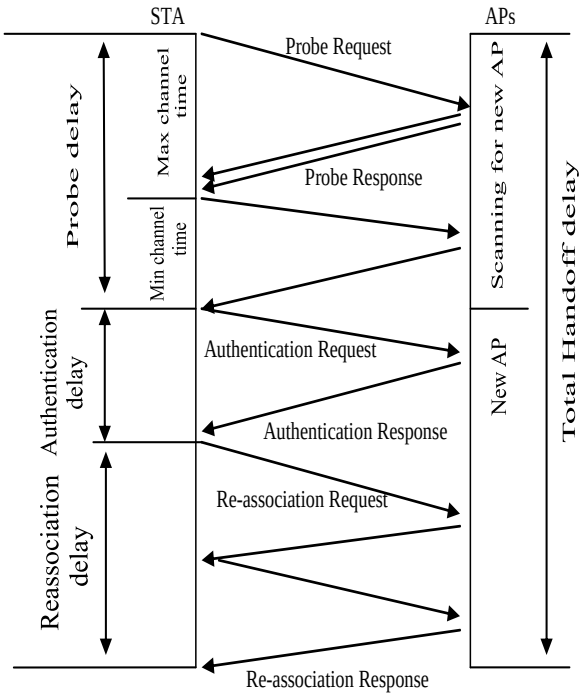

Figure 4. Handoff Process

Scanning: When a mobile station is moving away from its current AP, it initiates the handoff process when the received signal strength and the signal-to-noise-ratio have decreased significantly. The STA now begins MAC layer scanning to find new APs. It can either opt for a passive scan (where it listens for

beacon frames periodically sent out by APs) or chose a faster active scanning mechanism wherein it regularly sends out probe request frames and waits for responses for T_{MIN} (min Channel Time) and continues scanning until T_{MAX} (max Channel Time) if at least one response has been heard within T_{MIN}. Thus, $n*T_{MIN} \leq$ time to scan n channels $\leq n*T_{MAX}$. The information gathered is then processed so that the STA can decide which AP to join next. The total time required until this point constitutes 90% of the handoff delay.

Authentication: Authentication is necessary to associate the link with the new AP. Authentication must either immediately proceed to association or must immediately follow a channel scan cycle. In pre-authentication schemes, the MS authenticates with the new AP immediately after the scan cycle finishes. IEEE 802.11 defines two subtypes of authentication service: 'Open System' which is a null authentication algorithm and 'Shared Key' which is a four-way authentication mechanism. If Inter Access Point Protocol (IAPP) is used, only null authentication frames need to be exchanged in the re-authentication phase. Exchanging null authentication frames takes about 1-2 ms.

Re-Association: Re-association is a process for transferring associations from old AP to new one. Once the STA has been authenticated with the new AP, re-association can be started. Previous works has shown re-association delay to be around 1-2 ms. The range of scanning delay is given by:-

N × Tmin _ Tscan _ N × Tmax

Where N is the total number of channels according to the spectrum released by a country, Tmin is Min Channel Time,Tscan is the total measured scanning delay, and Tmax is Max Channel Time. Here we focus on reducing the scanning delay by minimizing the total number of scans performed.

In section 2 we take you through the various works that have already been done to achieve this and in section 3 we explain our proposed method. This is followed by performance evaluation of our proposed technique using simulations in section 4 after which in section 5 we propose a few areas in which further improvement can be made. Finally, we provide an extensive list of references that has helped us tremendously in our work.

2. RELATED WORKS

A number of different schemes have been proposed to reduce handoff latency in IEEE 802.11 wireless LANs. IEEE 802.11b based wireless and mobile networks [5], also called Wi-Fi commercially, are experiencing a very fast growth upsurge and are being widely deployed for providing variety of services as it is cheap, and allows anytime, anywhere access to network data.

The new age applications require a seamless handover while the small coverage of individual APs has increased the number of handoffs taking place. Thus reducing the handoff latency has become a burning issue and much work has been done to achieve this. See [6] for an overall review of popular methods suggested.

Shin et al in [7] have introduced a selective scanning algorithm with the help of channel masking technique coupled with a caching mechanism to significantly reduce the handoff delay. However, it still scans excess APs even after the new AP may have already been found and thus leaves room for further improvements.

Handoff, an inherent problem with wireless networks, particularly real time applications, has not been well addressed in IEEE 802.11, which takes a hard handoff approach [8].

In [9] the authors have introduced a novel caching process using neighbor graphs by pre-scanning neighbor APs to collect their respective channel information. The concept of neighbor graphs can be utilized in different ways and have become very popular in this field. In [10] a pre-authentication mechanism is introduced to facilitate seamless handover. [11] is a novel approach towards reducing handover latency in AP dense networks.

Besides, much progress has been made in introducing GPS aided handoffs; vide [12] to [13]. To reduce handoff latency in wireless LAN using IAPP [14], an algorithm on context transfer mechanism using 'Neighbor Graph' (NG) [15] was suggested in [16]. However, IAPP was only reactive in nature and creates an additional delay in a handoff. One approach on Physical layer (PHY) is the method using two trans-receivers, where a wireless Mobile station (MS) has two Wireless Network Interface Cards (WNICs) [17], one for keeping connection to current AP and the other for scanning channels to search for alternate APs [18].

Chung-Sheng Li et al. in [19] focused on neighbor graph caching mechanism for link layer handover. They use cache BSSIDs, SSIDs and channels of APs. They defined as,

$G' = (V', E)$

$V'=\{v_i v_i = (ap_i, \text{BSSID, SSID and channel}), v_i \in V\}$,

$e=(ap_i, ap_j)$,

$NC(ap_i) = \{ap_{ik}: ap_{ik} \in V', (ap_i, ap_{ik}) \in E\}$,

Where *G'* is the modified NGC and *V'* is the set containing APs with BSSIDs, SSIDs and channels of neighbor APs.

E is the set of edges. *NC* is the neighbor APs of an AP. By this process they significantly reduce the handoff delay. It saves time as NGC consists of APs, channels and additional information of BSSIDs and SSIDs.

In our work also we look at another such position dependant solution with a view to minimize overhead signalling problems. This is necessary since extensive pre-scanning is unacceptable in high traffic AP dense networks.

In [6], a new handover management technique has been proposed using neighbour graph.

In [7] the authors have introduced a novel caching process using neighbor graphs by pre-scanning neighbor APs to collect their respective channel information. The concept of neighbor graphs can be utilized in different ways and have become very popular in this field. In [8] a pre-authentication mechanism is introduced to facilitate seamless handover. [9] is a novel approach towards reducing handover latency in AP dense networks.

Besides, much progress has been made in introducing GPS aided handoffs; vide [10], [11], [12], [13], [14]. In our work also we look at another such position dependant solution with a view to minimize overhead signalling problems. This is necessary since extensive pre-scanning is unacceptable in high traffic AP dense networks.

3. PROPOSED WORK

We propose a pre-scanning method to reduce the scanning time as this delay contributes 90% of the total handoff delay. We use selective channel scanning as 1,6 and 11^{th} channel as they are non overlapping and in a well configured wireless network all or most of the APs will operate on these three channels. So, even in case of higher traffic load condition we have a great chance to

find free channel for best handoff. In the following, we describe the algorithm for pre-scanning mechanism. In our proposed method scanning process starts before handoff. We use selective scanning with the help of Neighbor Graph Cache [8] to find the best APs in the old AP's neighborhood region when the STA moves out of its old AP. Figure 5 and 6 describes the handoff process from device and NG server's point of view. We propose an algorithm in the following

i. After call setup the STA starts scanning.
ii. The cache is updated with scanned results.
iii. Above two process repeat n times up to actual handoff needed.
iv. When handoff needed, NG server fetches the information from cache.
v. The result is saved in device.
vi. If STA finds best scanned AP's information, handoff occurs; otherwise it waits for next scan result.

Let the STA needs handoff after *T* from the starting of a call and NGC takes *Ts* for scanning. Total no. of times cache is updated with neighbor graph information before handoff is,

$n=T/Ts$ …… (1)

So the scanning delay depends upon *n.* The scanning delay will be minimum if the probability of *n* being an integer is greater. In this case delay will be the fraction part of *n.* For best case scanning delay is nearly equal to zero (when *n* is integer). For any condition the delay will be less than *Ts* as the fraction part of *n* or the remainder of the division is less than *Ts.* Here delay is only due to authentication and reassociation delay and delay due to processing delay of devices. Pre-authentication process can also be adopted to reduce the handoff delay. Thus in this process the handoff delay is reduced drastically.

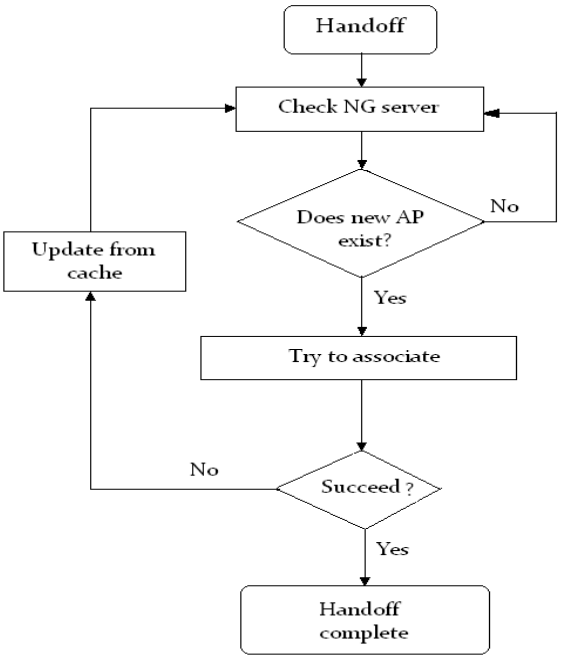

Fig 5. Flow chart of Handoff mechanism

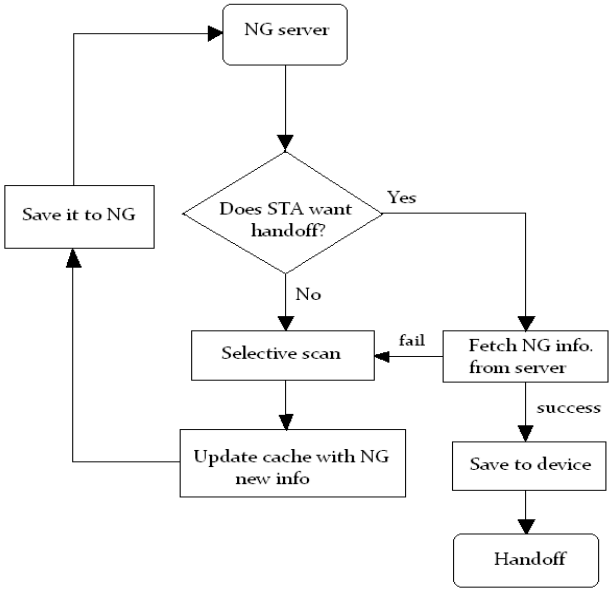

Fig.6 Flow chart from server's view pont

4. SIMULATION RESULTS

To evaluate the proposed algorithm we simulate three mechanisms: fast passive scan, fast active scan and neighbor graph cache (NGC) mechanism. We used previously measured scan times for our simulation: fast passive scan time as 150ms, fast active scan time as 32.36ms and NGC scan time as 0.299ms. Figure 7 and 8 show that the effective delays are lesser than the previous values. Here we took T from equation 1 from 1sec to 10sec and Ts as their respective values. The curves are all periodic in nature. The values of delays are repetitive. So for any higher values of T the delay is periodic like these graphs. Figure 9 shows some discrete values of three delays. The simulation results indicate that the average delays for fast passive, fast active and NGC scan are 55ms, 14.904ms and 0.194ms respectively. Therefore, we expect that our proposed algorithm can be a useful method for scanning as it effectively reduces delay time.

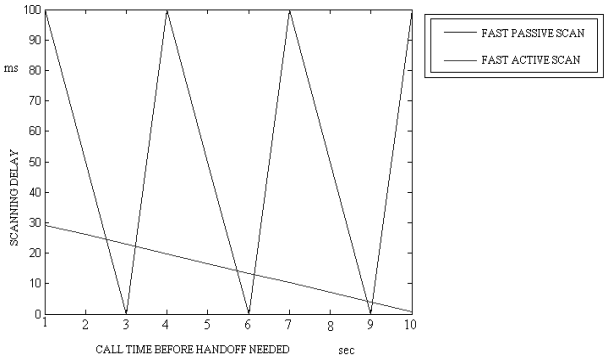

Figure7. Scanning delay for fast passive and fast passive scan.

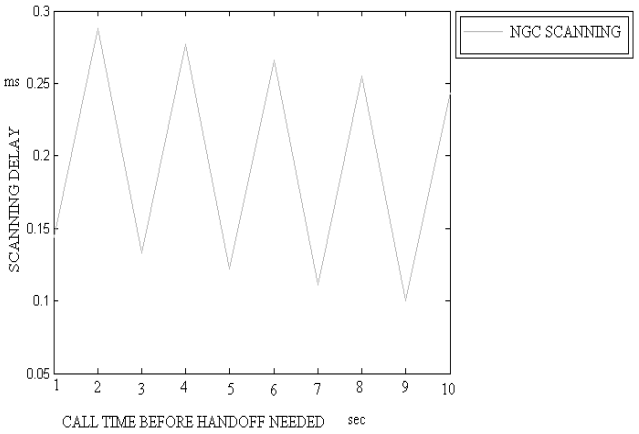

Figure8. Scanning delay for NGC.

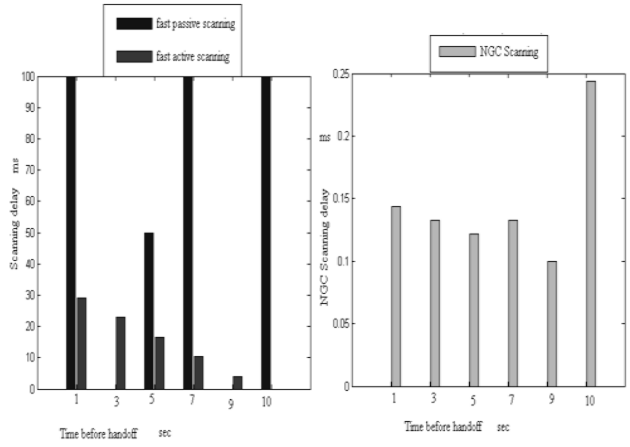

Figure9. Scanning delays

5. CONCLUSION

In this paper we described a neighbor graph based pre-scanning method that supports IEEE 802.11 based WLAN. We proposed a pre-scanning mechanism to reduce the handoff delay caused by device's mobility. Our simulation result indicates that our approach considerably reduces scanning delay. As scanning delay contributes 90% of the total handoff delay, this method reduces the handoff delay drastically. However, our proposed method leaves some drawbacks which we can leave for the future works.

For example, though we have been able to reduce handoff latencies we do not consider whether the handoff was at all necessary, i.e. ping-pong effects can significantly increase the number of false handoffs taking place. The ping pong condition arises when a MS moves back and forth between two BSs very frequently. Handoff cannot take place in this condition due to this frequent movement of MS. To avoid such problem, one traditional way is that the MS is allowed to continue maintaining a radio link with the old AP until the signal strength from new AP exceeds that of the old AP. But in our proposed method MS is bound to perform handoff in handoff region i.e. it has to reject its radio link with the old AP and has to connect with the new AP within that old cell. Thus MS cannot continue its radio link with the old AP any more. So in our proposed mechanism no such cure is possible for ping pong effect.

Also, our approach may result in handoff failure in a very small number of cases when the MS moves along the borders of the sectors i.e. GPS cannot decide in which sector the MS is.

It is worth mentioning here that although the proposed work has been presented considering honeycomb structures yet our algorithm would work in a similar manner for other cell structures and neighbor AP locations. Minor changes would be introduced depending on the network topology. Limitations can be effectively eliminated by using different techniques.

The mobility measurement of the STA that is involved in handoff is the most useful one. Indeed this would require significant changes to the actual scheme as we are using Neighbor graph instead of GPS to get positional data. The ping pong effect may be minimized by using received signal strength method along with our proposed algorithm. We intend to take up these matters in future studies. The real challenge as of now is to interpret the coverage areas of APs geometrically and incorporate that knowledge locally to optimize handoff performances.

6. REFERENCES

[1] Hye -Soo Kim, Sang Hee Park, Chun-Su Park, Jae Won Kim and Sung-Jea Ko. "Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph", July 2004.

[2] Hongqiang Zhai, Xiang Chen, and Yuguang Fang. "How well can the IEEE 802.11 wireless lan support quality of service?" IEEE Transactions on Wireless Communications, 4(6):3084-3094, December 2005.

[3] Yi-Bing Lin Imrich Chalmatc, "Wireless and Mobile Network Architectures," pp. 17.

[4] AKYILDIZ, I. F., XIE, J., and MOHANTY, S., "A survey on mobility management in next generation all-IP based wireless systems," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 16-28, 2004.

[5] STEMM, M. and KATZ, R. H., "Vertical handoffs in wireless overlay networks," ACM/*Springer Journal of Mobile Networks and Applications*(MONET), vol. 3, no. 4, pp. 335-350, 1998.

[6] Jaeyoung Choi *Student Member, IEEE*, Taekyoung Kwon & Yanghee Choi, *Senior Member IEEE*, Sangheon Pack *Member, , IEEE*,Fast Handoff Support in IEEE 802.11 Wireless Networks.

[7] Arunesh Mishra, Minho Shin & William Arbaugh, An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. [Anshuman Singh Rawat & Henning Schulzrinne Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs.

[8] Sangho Shin, Andrea G. Forte, Context Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network.

[9] S. Park and Y. Choi Pre-authenticated fast handoff in a public wireless LAN based on IEEE802.1x mode IFIP TC6 Personal Wireless Communications. Singapore, October 2002.

[10] Jin Teng, Changqing Xu, Weijia Jia, Dong Xuan, D-scan: Enabling Fast and Smooth Handoffs in AP-dense802.11 Wireless Networks.

[11] Chien-Chao Tseng, K-H Chi, M-D Hsieh & H-H Chang, Location-based Fast Handoff for 802.11 Networks. IEEE COMMUNICATIONS LETTERS, VOL9, NO 4 April 2005.

[12] S.Kyriazakos, D. Drakoulis, G.Karetsos, Optimization of the Handover Algorithm based on the Position of the Mobile Terminals. Proceedings of Symposium on Communications and Vehicular Technology, October 2000.

[13] In-Su Yoon, Sang-Hwa Chung, and Tae-Hoon Kim, A fast handover method for IEEE802.11 wireless networks using combined GPS and SNR

[14] J. Pesola & S. Pokanen , Location-aided Handover in Heterogeneous Wireless Networks. in Proceedings of Mobile Location Workshop, May2003.

[15] Jan Eric Hakegard, Multi-Cell WLAN Coverage and Capacity.

[16] Ping-Jung Huang, Yu-Chee Tseng. "A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks".

[17] M.Ohta, "Smooth Handover over IEEE 802.11 Wireless LAN, "Internet Draft : draft-ohta- smooth- handover-wlan-00.txt, Jun. 2002.

[18] Yogesh Ashok Powar and Varsha Apte, "Improving the IEEE 802.11 MAC Layer Handoff Latency to Support Multimedia Traffic".

[19] Chung-Sheng Li et.al. 'A Neighbor Caching mechanism for Handoff in IEEE 802.11 Wireless Networks.' Springer 20 March 2008,DOI 10.1007/s11227-008-0175-3.

Debabrata Sarddar is currently pursuing his PhD at Jadavpur University. He completed his M.Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.Tech in Computer Science & Engineering from Regional Engineering College, Durgapur in 2001. His research interest includes wireless and mobile system.

Shubhajeet Chatterjee is presently pursuing B.Tech Degree in Electronics and Communication Engg. at Institute of Engg. & Managment College, under West Bengal University Technology. His research interest includes wireless sensor networks and wireless communication systems.

Arnab Raha is presently pursuing B.E. (3rd Year) in Electronics and Telecommunication Engg. at Jadavpur University. His research interest includes wireless sensor networks, advanced embedded systems and wireless communication systems.

Karmajyoti Panigrahi is presently pursuing B.Tech Degree in EIE at Techno India College of Technology College, under West Bengal University of Technology. His research interest includes wireless sensor networks and wireless communication systems

Pulak Mazumder received his M.Tech in Electronics & Telecommunication Engineering from WBUT, Kolkata in 2010,and his B.Tech(AMIETE) in Electronics & Telecommunication Engineering from IETE, New Delhi in 2006. At present, he is an Asst. Professor in the Department of Electronics and Tele- Communication Engineering, Regent Education & Research Foundation, Barracpore. He was earlier a lecturer in ECE dept. at Durgapur Institute of Advanced Technology, Durgapur and Calcutta Institue of Engineering and Mangement, Tollygung, Kolkata. He served Industry more than eight years as IT Network Infrastructure Management. His research interest includes wireless and mobile communication systems.

Utpal Biswas received his B.E, M.E and PhD degrees in Computer Science and Engineering from Jadavpur University, India in 1993, 2001 and 2008 respectively. He served as a faculty member in NIT, Durgapur, India in the department of Computer Science and Engineering from 1994 to 2001. Currently, he is working as an associate professor in the department of Computer Science and Engineering, University of Kalyani, West Bengal, India. He is a co-author of about 35 research articles in different journals, book chapters and conferences. His research interests include optical communication, ad-hoc and mobile communication, semantic web services, E- governance etc.

Mrinal Kanti Naskar received his B.Tech. (Hons) and M.Tech degrees from E&ECE Department, IIT Kharagpur, India in 1987 and 1989 respectively and Ph.D. from Jadavpur University, India in 2006.. He served as a faculty member in NIT, Jamshedpur and NIT, Durgapur during 1991-1996 and 1996-1999 respectively. Currently, he is a professor in the Department of Electronics and Tele-Communication Engineering, Jadavpur University, Kolkata, India where he is in charge of the Advanced Digital and Embedded Systems Lab. His research interests include ad-hoc networks, optical networks, wireless sensor networks, wireless and mobile networks and embedded systems. He is an author/co-author of the several published/accepted articles in WDM optical networking field that include "Adaptive Dynamic Wavelength Routing for WDM Optical Networks" [WOCN,2006], "A Heuristic Solution to SADM minimization for Static Traffic Grooming in WDM uni-directional Ring Networks" [Photonic Network Communication, 2006], "Genetic Evolutionary Approach for Static Traffic Grooming to SONET over WDM Optical Networks" [Computer Communication, Elsevier, 2007], and "Genetic Evolutionary Algorithm for Optimal Allocation of Wavelength Converters in WDM Optical Networks" [Photonic Network Communications,2008].