Security Enhancement for Authentication of nodes in MANET by checking the CRL status of Servers

Azeem Irshad, Wajahat Noshairwan, Muhammad Shafiq,
Shahzada Khurram, Ehtsham Irshad, Muhammad Usman

University Institute of Information Technology
Pir Mehr Ali Shah, Arid Agriculture University
Rawalpindi, Pakistan
{ irshadazeem2, wajahat.noshairwan, shafiq.pu,
schahzada, ehtshamirshad, manilasani} @gmail.com

Abstract. MANET security is becoming a challenge for researchers with the time. The lack of infrastructure gives rise to authentication problems in these networks. Most of the TTP and non-TTP based schemes seem to be impractical for being adopted in MANETs. A hybrid key-management scheme addressed these issues effectively by pre-assigned logins on offline basis and issuing certificates on its basis using 4G services. However, the scheme did not taken into account the CRL status of servers; if it is embedded the nodes need to check frequently the server's CRL status for authenticating any node and place external messages outside MANET which leads to overheads. We have tried to reduce them by introducing an online MANET Authority responsible for issuing certificates by considering the CRL status of servers, renewing them and key verification within MANET that has greatly reduced the external messages.

Keywords: Authentication, MANET Authority, CRL, TTP, 4G, Mobile Ad hoc Network

1 Introduction

Mobile Ad hoc Networks (MANETs) are infrastructure-less networks comprising mobile nodes and are vulnerable to attacks for lack of any specific boundary and random entry of nodes in the network. Authentication is the hallmark of security and failure to achieving this so far is a stumbling block in the way of securing MANET. At small scale the authentication can be managed by the nodes through handshaking [6], but at larger scale it becomes complex and demands the involvement of TTP [1]. Some of the schemes are either based on self-organization in MANETs without TTP [2] where the identity is resolved by nodes themselves and some are based on absolute TTP [12], while a hybrid form of these schemes can also be used [1].

Our research work is based on the optimization of a scheme known as Tseng model [1] that gets the nodes authenticated in MANET by the use of 4^{th} generation (4G) technology [10] and [11], a future technology that supports in communicating different platforms in a transparent manner. The Tseng model allows the authentication and distribution of certificates to nodes through the support of 4G technologies. The Tseng model did not take into account the CRL status of servers. The Tseng model shows further overheads if this feature is embedded in the scheme, since, the nodes need to check frequently the server's CRL status for authenticating a node and place external messages outside MANET. If a server finds its ID in the CA's CRL directory any time it renders all the certificates of nodes invalid in the MANET. The nodes ask their servers to find the CRL status of a corresponding node's server. The communicating nodes can be from same and different CA domains. In the worst case if nodes need to establish sessions with the nodes from different servers each time, the overhead grows even more. The Tseng model, not fulfilling the requirement of CRL for the nodes to be known

before authentication, can be regarded as less secure and costly for overheads when the nodes from different servers try to communicate and verify from servers with the added feature of security.

We have tried to optimize the scheme by introducing an online MANET Certificate Authority in the network. A certificate is provided to each node by MCA after testing the CRL status of each node's server. It reduces verification visits to the server frequently to a large extent for a MANET relatively larger in size and hence less overheads enhances the efficiency of the MANET.

The paper is organized as follows: In section 2, an overview of previous schemes is presented. In section 3, we present the proposed model with certificate distribution and different communication scenarios. In section 4, we compare Tseng and proposed models and give simulation analysis while in section 6, we concluded our findings.

2 Related Work

A lot of work has been done on security problems regarding MANETS so far. We now take a brief overview of some of the related previous papers.

In threshold cryptographic scheme [3], the authority of CA is distributed among many t+1 network nodes, called servers, to minimize the chance of a single CA being compromised. All the nodes' certificates are divided into *n* shares and distributed to server nodes before network formation. If a node requires other node's public key, it requests to server nodes which generate their partial signatures individually and send to combiner to form a signature and present to the asking node. In MANET it is a cumbersome process that may cost more than a MANET's formation objective.

A similar scheme [5] is an improvement over [3] on the basis of availability. Here, the CA is a fully distributed and any $t+1$ number of nodes in MANET could behave as server nodes for issuance and verification of public keys for the nodes. Despite the advantage of availability, the scheme looses on the side of robustness with the higher values of *t.* The selection of *t* should be trade-off between both of the parameters.

In KAMAN [7], multiple Kerberos servers are responsible for distributed authentication in MANET. The servers are boot-strapped with keys shared with the client nodes. The users rely upon servers for acquiring tickets after authentication to communicate with other users which is a bottleneck for its implementation in MANETs and the servers are not trusted as there is no TTP involved initially.

In self-organized MANETS [2], the nodes rely on themselves for all routing, authentication and mobility management. The nodes issue certificates to their trustees for bringing them into MANET which are verified on the basis of repositories maintained by the nodes. Though, the scheme is self-organized but has the overheads of maintaining repositories which consumes the memory and bandwidth. Secondly, the originator blindly trusts any other node for making a new entry in the MANET.

A scheme [1] based on PKI implementation, resolves identity of nodes in MANET with the help of 4G services. The server distributes certificates to nodes through a special node using 4G services. The scheme successfully embeds TTP with MANET and getting nodes authenticated. However, it shows external message overheads when nodes from different servers communicate and verify the server's CRL status frequently. The scheme can be further optimized by reducing the overheads.

One more scheme [12] is based on certificate distribution to nodes before network formation by a trusted third party. The drawback remains with the condition of certificate issuance by TTP before network formation to all the nodes in MANET.

Some more work in this regard can be viewed in [8], [9] and [10] references.

3 Proposed Model

In Tseng model [1], the overhead tends to grow with higher proportions, as more and more nodes from different servers interact and establish sessions. If the nodes communicate recurrently, they can verify one another without server by storing CRL status. In the worst case, the communication of a node with nodes of a different server for each new session leads to external message overheads. We have tried to overcome weaknesses in Tseng model by lowering number of external messages for interacting nodes from different servers. Our scheme is based on the following assumptions.

3.1 Assumptions

1. A MANET Certificate Authority (MCA) is introduced as an independent entity authenticated by CA. The MCA has both, one homogeneous card for inter-nodes communication, and other heterogeneous card for accessing the 4G services.

2. A GN is a valid user of some server in the internet that generates its own public and private key pair.

3. There is only one MCA active in the MANET at one time, which may hand the charge over to a passive MCA in MANET any time due to any reason.

***Abbreviations*: MID**: MCA ID, **SID**: Server ID, **NID**: GN ID, **PKNID**: Public key of GN, **EPKS**: Encryption through public key of Server, **RNID**: Random number taken by GN, **PWNID**: Password of GN, **h**: hash, $\mathbf{Cert_{MCA}}$: MCA Certificate issued by CA, **SignPRM**: Signature through private key of MCA, $\mathbf{Cert_S}$: Server Certificate issued by CA, **SignPRS**: Server's Signature, **PKM**: Public key of MCA, $\mathbf{Cert_{AbyS1}}$: Certificate issued by Server1 to A, **EV:** Entity Verification, **SRT:** Server Restricted life Time, **EP:** Evaluation Point, **CRL:** Certificate Revocation List, **TTP:** Trusted Third Party

3.2 System Model

In existing scheme [1], we have introduced an online MCA which establishes a secure channel with servers like special nodes in Tseng model. The nodes access servers on internet through MCA and the provided logins are basis of verifiable identities for getting certificates. All GNs generate their private and public keys through built-in PKI techniques. The authorities sign public keys for issuing certificates. The procedure of issuing certificates is defined in the following section.

Certificate Issuance.

A node having a login, that wants to become part of the MANET, sends its parameters to MCA as shown in Fig. 1. MCA sends these parameters to server along with CA certificate and its own signature, as shown in Fig. 2. In Fig. 3, the server verifies MCA certificate through CA's public key and the node's identity by decrypting parameters through its private key and public key of MCA. It generates hash value by taking hash on node password, decrypted random number, node's id and public key which is matched with the received hash. Then the server generates a certificate and sends along with its own certificate as shown in Fig. 4. MCA generates a certificate by signing node's public key, Nounce, and expiry time for the lesser time period than the SRT.

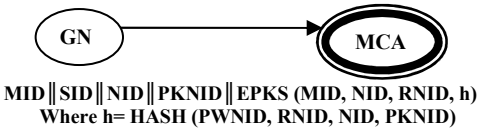


Fig. 1. Certificate Request

Fig. 2. Verification from Server

Fig. 3. Verification Acknowledgement

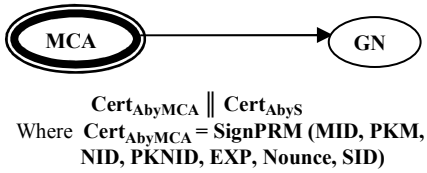


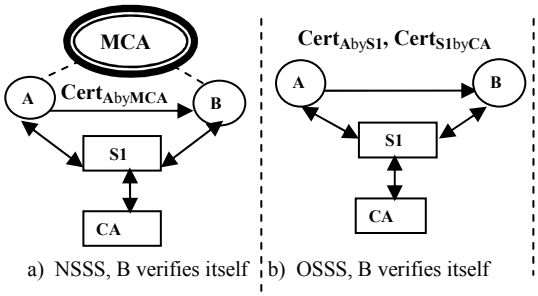
Fig. 4. Certificate Issued to GN

Whichever is lower of both server's CA issued certificate time and server's CRL time period, will be the certificate expiry time of node. A node accesses the public key of MCA through server's signed certificate which serves as a proof for MCA and GNs in authenticating one another. In Tseng model the scenario for different servers bears the overhead cost of entity verification. In proposed scheme the nodes in different servers scenario, establish sessions being under the MCA authority and the cost for finding server's CRL status and verification diminishes almost to zero as there is no external message cost for EV. The security is enhanced by taking into account the CRL status. MCA checks the CRL status of its member nodes' servers each time on certificate expiry to reissue certificates for validating authenticity.

Communication Scenarios and Overheads. In the following the different communication scenarios for Tseng and proposed models are explained.

New Scheme, Same Servers (NSSS) and Old Scheme, Same Servers (OSSS).

In Fig. 5, part (a) and (b) the node B can verify itself the identity of A as it knows the public keys and CRL status of its server. One drawback of OSSS is removed in NSSS as CR is done within MANET as compared to CRS. In NSSS, as authentication of a node is done within the MANET like OSSS so there is not much difference in the scenarios of both models. Now, if original MCA (OMCA) moves out of the MANET, OMCA assigns a proxy certificate to a new MCA (NMCA) after verification. The GN gets a certificate from NMCA on its certificate expiry. The two nodes should be carrying the certificate from same MCA at any instant for communication.



a) NSSS, B verifies itself b) OSSS, B verifies itself

Fig. 5. Comparison of NSSS and OSSS

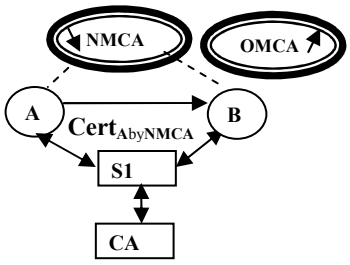
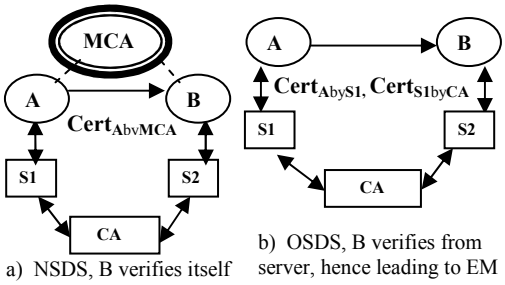


Fig. 6. NMCA replaces OMCA in NSSS

New Scheme, Different Servers (NSDS) and Old Scheme, Different Servers (OSDS).

The NSDS scenario overcomes the overhead in OSDS through MCA introduction. In OSDS, a node verifies the identity of other node by its server leading to overhead. In proposed scheme when nodes belonging to different servers come under MCA, the EV is performed by nodes within the MANET as the public key of MCA is known to all nodes. Our scheme do not incur cost for EV and overhead is reduced which leads to efficiency for the MANET as shown in Fig. 7. If OMCA moves out, the nodes switch to the NMCA as shown in Fig. 8. The nodes may regenerate certificates before the certificate expiry in case of urgent need for making contact to a node that has switched to NMCA. OMCA provides a list of node IDs to NMCA while moving out. The NMCA issues certificates to the nodes after verification of those IDs.



a) NSDS, B verifies itself b) OSDS, B verifies from server, hence leading to EM

Fig. 7. Comparison of NSDS and OSDS

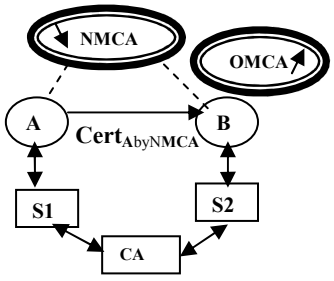


Fig. 8. NMCA replaces OMCA in NSDS

4 Comparison with Simulation Results

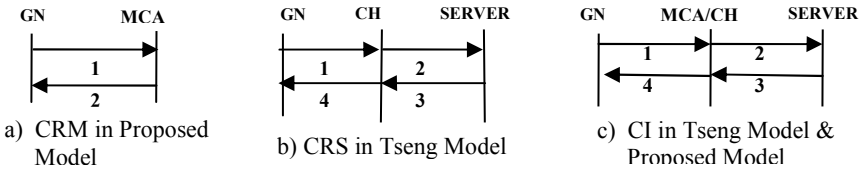
The purpose of this section is to draw the comparison of both schemes on the basis of calculations and proved results.

4.1 Major Differences in Tseng and Proposed Models

The differences in both schemes are based on the number of external messages for Certificate Renewals and Entity Verifications as described under:

First Time Certificate Issuance (FCI) and Certificate Renewals in both models.

The FCI in both models takes two external messages as shown in the Fig. 9 part (c). The CR from MCA (CRM) in proposed model relies on internal messages, while in Tseng model CR from Server (CRS) relies on external messages which are an overhead cost as shown in Fig. 9 part (a) & (b).



a) CRM in Proposed Model

b) CRS in Tseng Model

c) CI in Tseng Model & Proposed Model

Fig. 9. Certificate Renewal and CI in Tseng and Proposed Models

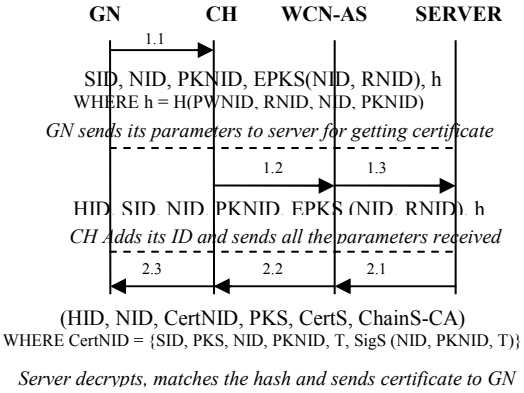


Fig. 11. Exchange of Messages in Tseng Model

Authentication Cost in Terms of External Messages.

The authentication cost varies with the scenarios of both schemes. In OSSS and NSSS, the EV cost is limited to internal messages. In OSDS, the nodes place external messages to servers as an overhead cost. In NSDS, the external messages cost is eliminated by introducing MCA in the MANET. We briefly show the exchange of messages for Tseng model in Fig. 11. The further details in this regard can be accessed from [1]. The table 1 shows the comparison of both models in terms of external messages for CRs and EVs. The NSSS and NSDS scenarios contain only internal messages without EV cost. The OSDS scenario bears the external message cost for EV.

Table 1. Comparison of EV cost for scenarios of both schemes

Activities / Scenario	Internal Messages		External Messages	
	CRM	CH	CRS	EV
OSSS	-	2	2	-
OSDS	-	2	2	2
NSSS	2	-	-	-
NSDS	2	-	-	-

Our simulation results are supported with the following case study. Assume a node N, in OSDS, authenticates the nodes by placing messages to its server. If node N establishes 4 sessions on average in an EP then the number of messages for CR and EV up to 3 EPs amounts to as following: (The EP session is taken equivalent to SRT).

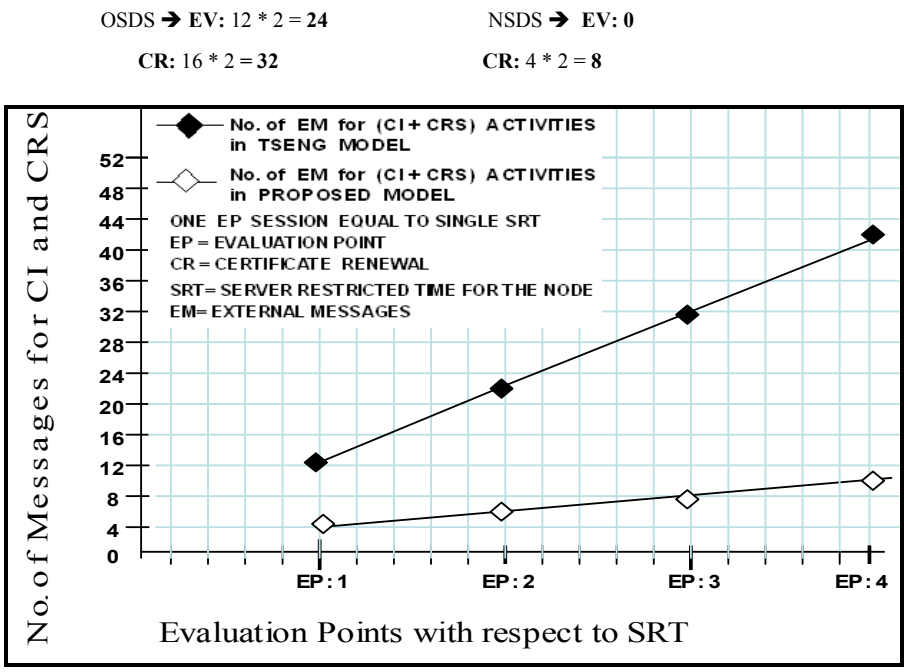


Fig. 12. Number of External Messages for CI and CRS at EPs

The number of external messages for 3 EP sessions is 56 for OSDS. In NSDS scenario there is only cost for CR as 8 external messages. We generate a function for calculating CR messages as [(E+1)*2] for proposed model and [(5E+1)*2] for Tseng model. E is the number of EP sessions. EV cost is calculated in OSDS by multiplying the number of EVs in all EP sessions with 2. The proposed scheme bears no cost in NSDS for EV activity.

In Fig. 12, the difference for number of messages based on CI and CRS in both models are shown. The curves for Tseng model rises sharply while the curves for the proposed model rises slowly which is an indicator of efficiency of proposed scheme.

In Fig. 13, the time line for certificate renewal from MCA has been drawn.

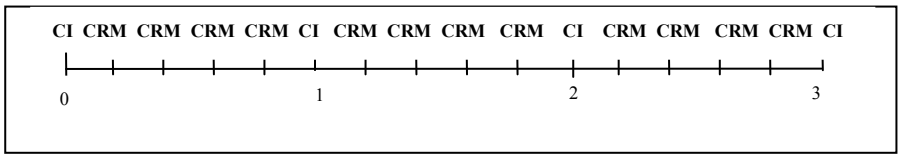


Fig. 13. Time line showing CRM for Proposed scheme

In Fig. 14, the time line for certificate renewal from server has been drawn.

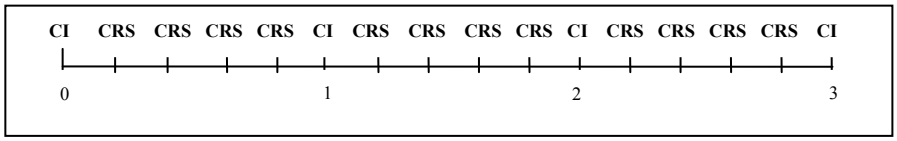


Fig. 14. Time line showing CRS for Tseng Model

The above figures support the analysis and simulation results and help us come to the conclusion that the proposed model reduces the overheads with enhanced security features of certificate revocation status.

5 Conclusion

In this paper, we have tried to overcome the weaknesses in Tseng model. This model does not take the CRL status of servers into account which leads to lack of security on the part of nodes and their servers. When this feature is embedded in Tseng model it shows no more optimal results and comes with external message overheads. In proposed scheme the nodes authenticate other nodes' servers within the MANET leaving the hassle of finding CRL status to an online authority, which helps saving the external messages to a large extent as evident by the simulation analysis. Secondly, the certificate renewal becomes more efficient and is performed within MANET without resorting to server. Our scheme can be regarded as the extension of previous scheme with improved features.

References

[1] Tseng, Y. Min.: A heterogeneous-network aided public-key management scheme for MANETS. Published in Wiley InterScience, Int. J. Net. Mgmt v.17: pp.3–15 (2006)

[2] Capkun, S., Buttyan, L., Hubaux, J.P.: Self-Organized Public-Key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing, V. 2, no.1, pp. 52-64 (2003)

[3] Zhou, L., Haas, Z.J.: Securing Ad Hoc Networks, IEEE Net. J., v.13, no.6, pp. 24-30 (1999)

[4]Brandt, I., rd, D., Landrock, P., Pedersen, T.: Zero- Knowledge Authentication Scheme with Secret Key Exchange. Journal of Cryptology (1998)

[5] Kong J, Zerfos P, Luo H, Lu S, Zhang L. Providing robust and ubiquitous security support for mobile ad hoc networks. IEEE (ICNP'01), pp. 251–260 Nov. (2001)

[6] Stajano, F., Anderson, R. J.: The resurrecting duckling: Security issues for ad-hoc wireless networks. In 7th Security Protocols Workshop, United Kingdom, Springer-Verlag, Berlin Germany (1999)

[7] Pirzada, A., Mc Donald, C.: Kerberos Assisted Authentication in Mobile Ad-hoc Networks, the 27th Australasian computer science conference (2004)

[8] Weimerskirch, A., Thonet, G.: A Distributed Light-Weight Authentication Model for Ad-hoc Networks, The 4th International Conference on Information Security and Cryptology, pp 6-7 ICISC (2001)

[9] Zhu, S., Xu, S., Setia, S., Jajodia, S.: Establishing pair wise keys for secure communication in ad hoc networks: a probabilistic approach, The 11th IEEE International Conference on Network Protocols (2003)

[10]Schulzrinne. H., Wu, X., Sidiroglou, S.: Ubiquitous Computing in Home Networks. IEEE Commun. Mag., pp. 128-135, November (2003)

[11] Hui, S.Y., Yeung, K.H.: Challenges in the Migration to 4G Mobile Systems. IEEE Commun. Mag., pp. 54-59, December (2003)

[12] Varadharajan, V., Shankaran, R., Hitchens, M.: Security for cluster based ad hoc networks. Computer Communications; 27(5): 488–501. (2004)

Azeem Irshad has been doing Ph.D after completing MS-CS from UIIT, PMAS Arid Agriculture University Rawalpindi. and is currently working as a Research Associate for the research department of UIIT. His research interests include MANET security, merger of Ad hoc networks with other 4G technology platforms, multimedia over IP and resolving the emerging wireless issues.

Wajahat Noshairwan is currently working as a Assistant Professor of Wireless Networks in UIIT, PMAS, Arid Agriculture University Rawalpindi, Pakistan. He provides professional consultancy in cutting edge aspects of Wireless Security. He has the extensive knowledge on networks related disciplines. He is a gold medalist at MAJU University in MS-CS programme. His research interests include MANET security, mobility, vertical handoff for 4G Networks, latest issues in multimedia over IP.

Muhammad Shafiq has been doing Ph.D after completing MS-CS from UIIT, PMAS Arid Agriculture University Rawalpindi. He has also done MIT from University of the Punjab. He is currently serving as an Assistant Professor in Raees-ul-Ahrar College in computer science department. His research interests include issues in Ad hoc Networks, Telecom Networks Management and Wireless Security.

Ehtsham Irshad. The author has done MS-CS (Networks) from UIIT, PMAS, Arid Agriculture University, Rawalpindi, Pakistan. He has completed BS-CS from AIOU, Islamabad. He has been serving as Networks Administrator in International Islamic University, Islamabad. The area of research is wireless networks, mobility and security in Ad hoc networks and seamless vertical handoff among heterogeneous networks.

Shahzada Khurram has done MS-CS (Networks) from UIIT, PMAS, AAUR. He is currently working as a Networks Administrator in the UIIT, PMAS, Arid Agriculture University Rawalpindi. He has been organizing LINUX, CCNA and CCNP courses under TEVTA, Govt. of Pakistan. His research interests include WIFI security, multimedia over IP and issues in the recent developments on (IEEE 802.11n) standards for wireless.

Muhammad Usman has done MS-CS (Networks) from UIIT, PMAS Arid Agriculture University Rawalpindi and is currently working as a Research Associate for the research department of UIIT. He has recently contributed for seamless handover techniques for GPRS and WLAN platforms. His research interests include resolving the wireless handover problems and ongoing issues in multimedia over IP.