A New Reliability Model for Evaluating Trustworthiness of Intelligent Agents in Vertical Handover

Kailash Chander
Research Scholar, Maharishi Markendeshwar University,
Mullana, Haryana, India.

Dimple Juneja
Professor, M.M Institute of Computer Technology and
Business Management (MCA) , Maharishi
Markendeshwar University, Mullana,
Haryana, India

Abstract— **Our previous works have proposed the deployment of mobile agents to assist vertical handover decisions in 4G. Adding a mobile agent in the 4G could lead to many advantages such as reduced consumption of network bandwidth, delay in network latency and reduction in the time taken to complete a particular task. However, this deployment demands that the deployed collection of agents shall be secure and trustworthy. Security of a mobile agent includes maintaining confidentiality, reality and integrity of not only the agent employed but also the system in which it is deployed. In fact, many conventional security solutions exists, however, very few of them addresses the challenge of introducing trusted computing in mobile agents, deployed in 4G, in particular. This paper proposes a new reliability model by implementing trust certificate for mobile agents in vertical handover.**

Keywords- Trust Certificate; Mobile Agents; Vertical Handover; Secure Network;

I. Introduction

All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later Mobile agent is an entity that migrates from one system to another to access remote resources or to interact with other agents. Agent technology finds its applications in wide areas such as user interfaces, mobile computing, information retrieval and filtering, smart messaging, telecommunications etc. Our previous works proposed an agent based smart solution for vertical handover in 4G [10]. Agents deployed at different level of PMIPv6 environment are responsible for managing user preferences, authentication of mobile node and buffering of user data in case of handover. Further, this vertical handover decision is mainly relies on the selection of the 'best' available network that could meet QoS requirements for the end-user and to meet the above requirement a novel approach for always best connected in future wireless networks [12] was also proposed. The work exploits intelligent agents for weight calculations after analyzing the explored parameters for various networks. Mobile agent based emigration framework for 4G (MAEF) [16] which helps to switch the network during critical situations of draining battery without interrupting the ongoing task were also proposed. However, in all of the above works, the trustworthiness of mobile agents deployed in the system is left unattended. The current works aims to propose a reliability model that would evaluate the trustworthiness of mobile agents operating in 4G.

Now, the deployed agents must be trustworthy and reliable wherein, agent should not be involved in the activities such as disclosure of information, denial of service and corruption of information with respect to interaction and cooperation [17]. In fact, trust is one of the basic parameters of evaluating a mobile agent-based system and it is usually computed through Direct Experience, Third Party References, Confidentiality, Persistence, Execution Trust etc. Literature [9] reflect that "Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather it is subject to the entity's behavior and applies only within a specific context at a given time". Using this definition the proposed work assigns weight to the mobile agents, which is further, used for calculating the credibility of a mobile agent.

The structure of the paper comprises of four sections. Section II presents the related work. Section III discusses the significance of evaluating trust in mobile agent-based frameworks. Section IV presents the new reliability model that evaluates the trustworthiness of participating agents by generating a trust certificate. Finally, conclusions and future scope is presented in Section V.

II. Related Work

The section presents the work of researchers in trusted computing in telecommunication with the aim to highlight the scope of further research in the similar direction.

When mobile agents travel from one system to another in a network, they transfer their code, data and execution state. Therefore, reliability is a vital issue for deploying the mobile agent system. Many researchers have proposed trust based reliable frameworks. For instance, MobileTrust [6] has a trust management layer added transparently on the top of the conventional security layer, which is responsible for presenting security related trust evidence for the purpose of making evaluations and decisions regarding trust relationships among mobile agents.

Work in [1] presents a fuzzy approach for reliability estimation of Mobile Agent Based Systems (MABS). It investigates the hardware oriented system reliability of MABS. The Trust Management Frame (TMF) [7] is another approach comprising of three main components i.e. trust dissemination, trust formation and trust evolution. AT-RFM [2] presents an agent tracking reliable forwarding mechanism that integrates the 'tracker' with context. The objective of tracker is to know the present status and location of the agent. Few other works such as Trust-Aware resource management model [9] uses trust in grid system. In this model overall Grid system is divided into Grid Domains, which are autonomous administrative entities consisting of a set of resources and clients managed by a single administrative authority. The study examines the integration of the notion of "trust" into resource management such that the allocation process is aware of the security implications. A trusted Certification Authority (CA) and Trusted Platform Module (TPM) [3] is proposed for authentication and delegation of identity of mobile agent environment so that entities in mobile agent environment can build trusted relationship with each other.

The literature presented above clearly indicates that researchers have been demanding the trust enabled agent-based frameworks and few of them have made good attempts to incorporate trust and reliability as two separate parameters depending upon the domain of implementation. The main intent of this work is to propose a hybrid model that would ensure both reliability and trustworthiness by implementing trust certificate for mobile agents deployed in vertical handover process in 4G.

Next section presents the background of formalizing trust and reliability in our works.

III. FORMALIZING TRUST IN MOBILE AGENT-BASED FRAMEWORKS

Trust in mobile agents is usually established through identity token, provided by an X.509 public key certificate [18]. An X.509 certificate contains a public key, a subject name in the form of a multi component distinguished name (DN), a validity period and is either signed either by a trusted third party, or by certification authority (CA). Figure 1 depicts an Example of standard X.509 Certificate [15]:

Although, an X.509 certificate is good enough to identify the identity of a mobile agent but it fails to confirm the reliability and credibility of the agent under consideration. Therefore, this paper proposes a new and improved "Trust Certificate" for a Mobile Agent. The approach provides a means to work independently or, if available, in conjunction with the X.509–PKI. The work aims to evaluate the reliability, credibility and trustworthiness of agents and hence a new trust certificate representing the weight in terms of five parameters namely, Direct Experience, Third Party References, Confidentiality, Persistence, Execution Trust of a mobile agent would be generated and hence would be improving the overall performance of the system.

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/Email=server-
certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-
certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):

00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:

68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:

85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:

6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:

6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:

29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:

6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:

5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption

07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:

a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:

3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:

4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:

8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:

e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:

b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Figure 1: A Sample of CA X.509 Certificate [15]

IV. THE NEW RELIABILITY MODEL FOR GENERATING TRUST CERTIFICATE

A critical look at the literature pointed towards few parameters on which trust in trusted computing is being evaluated and those parameters are Direct Experience, Third Party References, Confidentiality, Persistence, Execution Trust etc. This work exploits these stated parameters and a trust certificate is being generated as shown in Figure 2.

The trust certificate comprises of certificate version, issuer, validity dates, previous weight, current weight, trust weight and date of weight updation. The description of the components used in trust certificates are as follows:

- Certificate Version: This field describes the version of the Trust Certificate.

- Issuer: The issuer field identifies the entity who has signed and issued the Trust certificate. Mobile agents are usually expected to have FIPA standardized certificate.
- Validity Dates: Trust certificate validity period is represented two dates: the date on which the certificate validity period begins (notBefore) and the date on which the Trust certificate validity period ends (notAfter).
- Parameter Previous Weight: This field consists of previous weight of Trust Certificate. The initial value of this field will be 0.5 for new agent. For future correspondence current weight will become previous weight for an agent.
- Parameter Current Weight: This field can be calculated based on five parameters defined in Figure 2.
- Trust Weight: Trust weight field can be calculated by getting the average of Previous Weight and Current Weight.
- Date of Weight Update: This is the date on which Trust Weight is updated

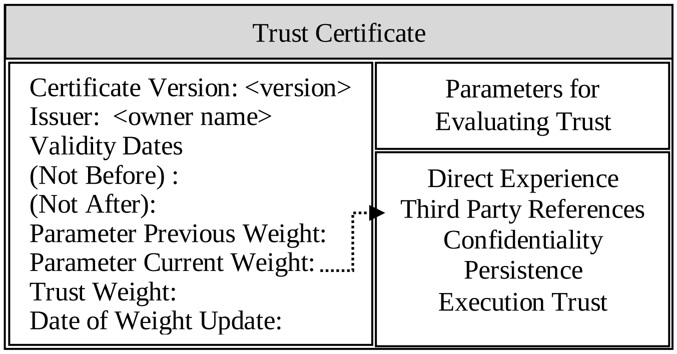


Figure 2: Proposed structure of Trust Certificate

Based on the weights i.e. previous weight (PW*i*) and current weight (CW*i*), a trust weight (TW*i*) of a mobile agent is calculated. To calculate the Current Weight (CW*i*) every parameter is assigned values in the range of [0, 1]. For instance, CW*i* =0 means distrust i.e. agent is non-trustworthy and CW*i* =1 implies agent is fully trustworthy. If the value assigned between 0 and 1 it means two entities trust each other upto an extent. In order to compute, TWi between two interacting agents, an average of PWi and CWi is calculated as given by eq.(1).

$$tw_i = \frac{\sum_{\mathrm{i=1}}^{\mathrm{n}}(\mathrm{cw_i} + \mathrm{pw_i})}{2} \qquad (1)$$

Now, the challenge is how to evaluate these weights. As depicted in Figure 2 the weights are dependent on the mentioned parameters. Now, when these agents, say Agent*i*, Agent*j*, and Agent*k* interact with each other, the weight of each parameter would be computed individually as per the matrices given in Figure.3.

As shown in Figure 3(a),(c) and (e) i.e. in case of direct experience, confidentiality and execution trust, an agent*i* would award a weight '1' to agent*j* as this value have to be awarded only when the respective agents have directly experienced an interaction with each other and hence are confident and can ensure the execution trust too, else the value in the cell remains 0. This computation remains same irrespective of the facts that agents are operating in homogenous or heterogeneous environments; or belong to Intranet or Internet. In contrast, the cells in figure 3(b) and (d) have values in the range of {0-1}. For instance, when an agent*i* award values to agent*j* on the basis of third party reference, it is depending on the feedback of third party and hence may not be fully satisfied while awarding a value. In such uncertain conditions such as third party reference and agent's persistence in any environment may lead to fuzzy values which has been discritized in the range {0.0.25,0.5,0.75,1}for the sake of computational simplicity.

On the basis of above computations, the current weight for an Agent*i* would be calculated as the sum of values generated for each parameter and is given as in eq.(2).

$$cw_i = \sum_{\mathrm{i=1}}^{\mathrm{n}}(\mathrm{de_i} + \mathrm{tpr_i} + \mathrm{conf_i} + \mathrm{pers_i} + \mathrm{et_i}) \qquad (2)$$

Where, the range of each parameter is as defined in the above matrix. The trust weight would then be computed as given in eq. (1)

Now, turning our attention to our proposed works [10, 12, 16] wherein, a trust certificate for various agents deployed at different level of PMIPv6 will now be generated. The agent of MN is responsible for managing user preferences through Compute*agent* [12]. Interface*agent* [12] provides information already collected from different MAGs and handover the same to the Compute*agent* for populating the preference list. In the similar way MAG*agent* [10] also interact with another MAG*agent* [10] to transfer the authentication and buffered data during handover. Moreover LMA*agent* [10] is responsible for maintaining the user profile and policy data which is updated to MN via MAG.

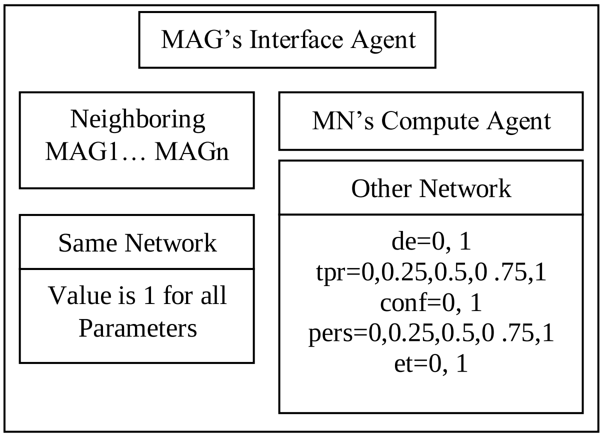


Figure 4: Interaction of Interface Agent with Compute Agent

When these agents interact, the parameters are initialized with values as given in Figure 3. As shown in Figure 4, when

Direct Experience (de_i)		
No. of Agents	$Agent_j$	$Agent_j$
$Agent_i$	1	0,1
$Agent_j$	0,1	1

(a)

Third Party References (tpr_i)		
No. of Agents	$Agent_j$	$Agent_j$
$Agent_i$	1	0,0.25,0.5, 0.75,1
$Agent_j$	0,0.25,0.5, 0.75,1	1

(b)

Confidentiality ($conf_i$)		
No. of Agents	$Agent_j$	$Agent_j$
$Agent_i$	1	0,1
$Agent_j$	0,1	1

(c)

Persistence($pers_i$)		
No. of Agents	$Agent_j$	$Agent_j$
$Agent_i$	1	0,0.25,0.5,0.75,1
$Agent_j$	0,0.25,0.5,0.75,1	1

(d)

Execution Trust (et_i)		
No. of Agents	$Agent_j$	$Agent_j$
$Agent_i$	1	0,1
$Agent_j$	0,1	1

(e)

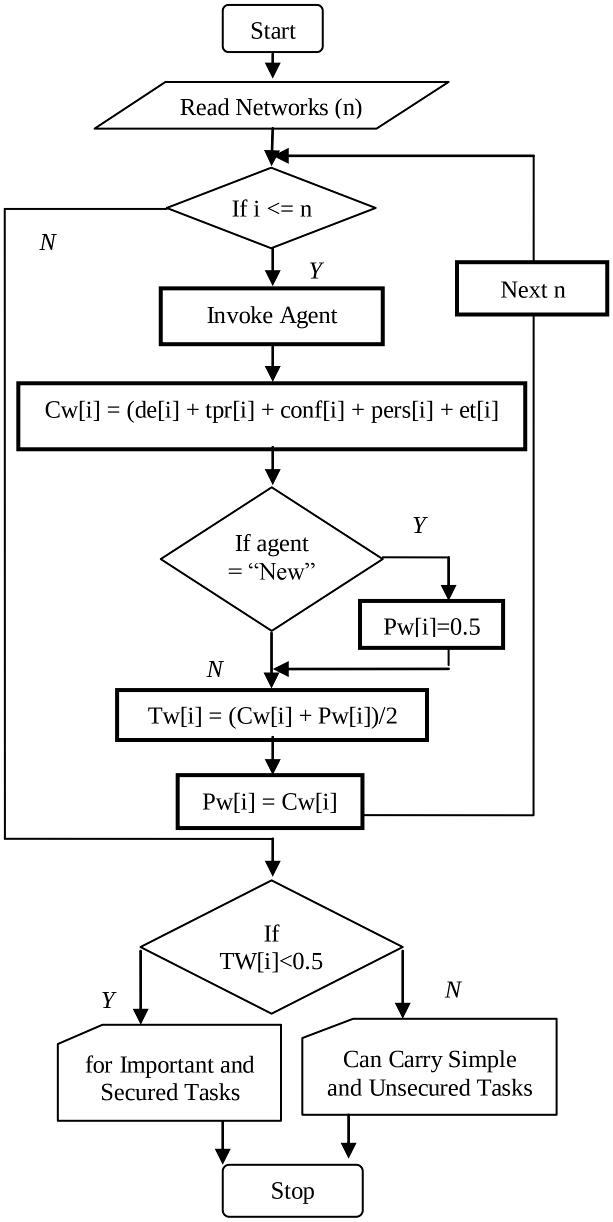
Figure 3: Computation of Weights of Various Parameters

MAG's Interface*agent* is interacting with other MAG's agents to collect the information for best available network. The same information is then handover to Compute*agent* of MN to set the preference list for Always Best Connected. In both interactions

MAG vs MAG and MAG vs MN the network type may be same or it may be of different type. The values for all the parameter is set accordingly to calculate the current weight.

```
Algorithm: Agent TC (Trust Certificate)
----------------------------------------------------------------------
begin
read Networks (n)
while (has more n)
invoke agent[i]
compute Cw[i]=sum(de[i], tpr[i], conf[i], pers[i], et[i])
        if (agent is new)
                Pw[i]=0.5
        else
                Pw[i]=Cw[i]
        Trust Weight Tw[i] = (Pw[i]+Cw[i]) / 2
next  n
        if (Tw[i] < 0.5)
                for Simple and Unsecured Tasks
        else
                for Important and Secured Tasks
        end if
$LMA_{agent}|MAG_{agent}|Compute_{agent}|Interface_{agent} \leftarrow$ TC
end
----------------------------------------------------------------------
```

Now, in order to calculate the TW$_i$ of any mobile agent for a particular network, the value of previous weights is also required. However, if an agent is interacting for the first time then default value of previous weight will be 0.5. However, current weight will become the previous weight for future interaction as shown in flow chart Figure 5. Now, as is clear from the computations, a trust certificate will be generated for each agent willing to participate and hence carry out a particular task. An agent will be assigned an important task such as secured transactions if, it scores a minimum threshold value of TW$_i$ i.e. 0.5. An agent scoring less than this would may be allowed to carry simple and unsecured tasks such as internet surfing and voice data. However, in case of more than one agent bidding for a particular task, an agent having the


Start
Read Networks (n)
If i <= n
N
Y
Invoke Agent
Next n
Cw[i] = (de[i] + tpr[i] + conf[i] + pers[i] + et[i]
If agent = "New"
Y
Pw[i]=0.5
N
Tw[i] = (Cw[i] + Pw[i])/2
Pw[i] = Cw[i]
If TW[i]<0.5
Y
N
for Important and Secured Tasks
Can Carry Simple and Unsecured Tasks
Stop

maximum TW_i value and the oldest Trust certificate will be treated as the most experienced and hence learned agent for the task to be performed successfully. The Trust certificate needs to be embedded as add-ons to the mobile agent.

V. Conclusion And Future Work

This work proposed a new reliability model for generating trust certificate for all agents participating in vertical handover procedure happening in 4G. Trusts amongst agents have always been an important and unaddressed challenge. The trust certificate generated by the proposed model not only improved the reliability and trustworthiness of agents but also added to improving robustness of the whole agent-based framework. Now, the agents can be categorized and be given a task according to their credibility. For instance, an agent with low trust weights will be assigned a task which does not demand high security whereas an agent with high trust weight may be assigned a task of carrying out financial transactions. The only limitation of this work is that it demands embedding of trust certificate in the data section of mobile agents, thus adding an overhead and increasing the complexity of mobile agent.

References

[1] Mosaab Daoud and Qusay H. Mahmoud "A Fuzzy Approach to Reliability Estimation of Mobile Agent-Based Systems", Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on Oct. 2007 p.p. 2854 – 2859.

[2] U.P.Kulkarni, Prof A R Yardi, "Agent Tracking: A Reliable Agent Forwarding Mechanism", Proceedings of the 2005 International Conference on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'05)

[3] Zhidong Shen, XiaopingWu, "The Authentication and Identity Delegation about Mobile Agent System based on Trusted Computing Platform", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on July, 2010 p.p. 672 - 676

[4] Zhidong Shen et.al., "Trust Management for Mobile Agent System Based on Trusted Computing Platforms", Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on June, 2010 p.p 717 - 721

[5] Zhen Ye et.al., "Dynamic Trust Model Applied In Mobile Agent" Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on July 2008 p.p. 536 - 540

[6] Ching Lin and Vijay Varadharajan , "Trust Enhanced Security - A New Philosophy for Secure Collaboration of Mobile Agents", International Conference on Collaborative Computing: Networking, Applications and Worksharing, ISBN: 1-4244-0428-2, IEEE 2006

[7] Suzhen Wang et. al. "A Trust Evaluation Method of Mobile Agent System", Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on Sep. 2007 p. p. 6317 – 6320.

[8] Ching Lin et. al. "Trust Enhanced Security for Mobile Agents", Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05), 2005

[9] Farag Azzedin and Muthucumaru Maheswaran "Towards Trust-Aware Resource Management in Grid Computing Systems" Cluster Computing and the Grid, 2002. 2nd IEEE/ACM International Symposium on May 2002 p. p. 452-452

[10] Kailash Chander, Dr. Dimple Juneja et. al. "An Agent Based Smart Solution for Vertical Handover in 4G", International Journal of Engineering Science and Technology, Vol. 2(8), 2010, p.p. 3381-3390

[11] Internet Engineering Task Force (IETF). www.ietf.org

[12] Kailash Chander, Dr. Dimple Juneja "A Novel Approach for Always Best Connected in Future Wireless Networks", Global Journal of computer Science and Technology, Issue 11, Vol 05, 2011.

[13] R.Koodli, "Mobile IPv6 Fast Handovers," RFC 5268, June 2008

[14] D. Premec, NetExt Working Group, Internet Draft "Inter-technology handover in PMIPv6 domain" at www.ietf.org, March 9, 2009.

[15] http://www.pentaware.com/pw/x509.htm

[16] Kailash Chander, Dr. Dimple Juneja "Mobile Agent based Emigration Framework for 4G: MAEF" communicated to International Journal of Information and Computing Science, UK

[17] Zhidong Shen, Xiaoping Wu "A Trusted Computing Approach to Building Trusted Connect between Entities in Mobile Agents Environment"2nd International Conference on Education Technology and Computer (ICETC)- 2010.

[18] R. Housley et.al "Internet X.509 Public Key Infrastructure Certificate and CRL Profile" http://www.ietf.org/rfc/rfc2459.txt

AUTHORS PROFILE

Dr. Dimple Juneja is the Principal and Professor of Computer Science at Maharishi Markandeshwar University, Mullana-Ambala, India. Her publications include more than 42 research papers in various National and International Journals and conferences. Her research interests include Agent Technologies, Semantic Web, Sensor Networks and Intelligent Systems. She is a member of Computer Society of India and International Association of Engineers, Hongkong. She is a recipient of best paper awards and the Distinguished Faculty award. Her research has been funded by Ministry of Czech Republic and Haryana State Council of Science and Technology, India. She has served on various selection and review panels. Dr. Juneja has also worked as postdoctoral researcher in computer science at Louisiana State University. She is on the editorial board of various international journals of repute and has chaired sessions at various International conferences.

Kailash Chander is the Resarch Scholar at Maharishi Markandeshwar University, Mullana-Ambala, India. His publications include more than 10 research papers in various National and International Journals and conferences. His research interests include Mobile Communications and Agent Technologies.