*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727*
*PP 47-51*
*www.iosrjournals.org*

# Challenges of mobile computing in networking: A Review

Manjiri S Dixit[1]

*Mail-id: manjiri.muley@yahoo.in*
*Computer Science Department Dharampeth M.P Deo Memorial Science College RashtrasantTukdojiMaharaj Nagpur University India*

***Abstract***: *Computers able of attaching to the Internet from many places are likely to grow in popularity until they control the population of the Internet. Protocol research has stimulated into high gear to improve appropriate network protocols for associating mobility. Large-scale networks of wireless sensors are becoming an active issue of study. Developments in hardware technology and engineering design have managed to dramatic reductions in size, power consumption and cost for digital integrated circuit, wireless communications and Micro Electro Mechanical Systems. This has assisted very compressed, self-sufficient and mobile nodes, each containing one or more sensors, computation and communication capabilities and a power supply. The mobile internet is composed to this industry, allowing numerous small, agile and focused providers of content and services to encounter embedded carriers in this new market opportunity.*

***Keywords***- *Security, structural requirement, Error Correction, Source Routing, Operational Requirement, Grey prediction*

## I. Introduction

This topic of Mobile Networking and Applications presents research examining the effects of mobility onthe Internet. Wireless communications has been another growth area marking the system design of mobile computers. As improved bandwidth becomes available and more information resources become accessible by way of the Internet, the drivefor enclosure of wireless abilities in laptop computers will become overpowering. There are several mobile computers anticipated that will not have hard disks, and many without keyboards, but these more controlled devices are not principal drivers for the mobile networking systems. On the contrary, many of the techniques and protocols established for more general purpose mobile computers can be revised as needed for the special or restricted case. Wireless and mobility are not the same, but they are types which are quite synergistic.

The new wireless media becoming accessible are among the primary drivers for the interest in mobile computing.
Thus, it is suitable to understand the nature of wireless communications, and the difference between wireless and wired media.

For wiredmedia, there is typically:
_ well defined broadcast range;
_ Low bit error rate;
_ High bandwidth;
_ Symmetric connectivity.

For wirelessmedia, there is typically:
_ Point-to-point communication only, or vague and poorly controllable boundaries for broadcast range;
_ Variable (time and distance dependent) bit error rate;
_ Low to medium bandwidth;
_ probably asymmetric connectivity.

## II. Mobile Networking Challenges

*2.1 Analogous Read-Out*

A single wide beam from the BTS can simultaneously review many dust motes. The imaging receiver at the BTS accepts multiple reflected beams from the motes, as long as they are appropriately separated in space to be fixed by the receiver's pixel array. The probe beam sweeps the three dimensional space enclosed by the

base station on a regular basis, most likely resolute by the nature of the application and its requirement for moment-by-moment sensor readings.

*2.2 Mandate Access*

Saving transmit power, if the mote must use active communications, then it is best to use the active transmitter in ahigh-bit-rate, short-burst mode. Familiar request access methods can be used to associate the low latency advantagesof active communications with the low-power benefits of the passive approach. There are as many channels (paging or data) as there are resolvable pixels at the BTS. The BTS has no wayto differentiate between simultaneously communicating dust motes if they fall within the same pixel in the imaging array. One possible way to deal with this is to acquaint time slotted techniques not unlike that found in time division multiple access (TDMA) communications systems.

*2.3 Line-of-Sight Requisite*

An unbroken line-of-sight path is normally essential for operation of free-space opticallinks for Smart Dust. Theselinks cannot work reliably using non-line-of-sight propagation, which would rely on reflections from one or moreobjects between the transmitter and receiver. The transmitted beam should have a small angular spread in order to attain a high signal-to-noise ratio wit acceptably small transmitter power. Specular reflection may not knowinglyraise a beam's angular spread, but the existence of anaccurately aligned specular reflector would be anexceptional event. Diffuse reflection scatters a beam's energy over a wide range of angles, making alignment less critical, but usually scatters inadequate energy toward the receiver. Hence, diffuse, non-line-of-sight transmission is expected to be practicable only when active transmitters are used over very short distances (probably under 1 meter). It is perhaps impossible to use diffuse, non-line-of-sight transmission with passive transmitters (based on CCRs), because both the interrogating beam and the reflected beam would be subject to scattering over a wide range of angles.

*2.4 Probe Reenter Rates*

Probe beam reexamine rates could be determined in an application- specific manner. It is a well-known observation from statistical data management that areas where changes are happening most promptly should be revisited most regularly. If sensor readings are not changing much, then occasional samples are enough to obtain statistically significant results. So it is better to devote probe dwell time on those sensors that are undergoing the most rapid reading changes, and for which infrequent visit would lead to the greatest deviation from the current sensor values.

*2.5Source routing*

Many early methodologies to Mobile IP tried to make use of IP's loose source route (LSR) option. This seems a smart possibility, because packets sent to a mobile node can be delivered directly to the mobile node by aforeign agent if the foreign agent is specified as part of the loose source route. Moreover, if the mobile node sendsa packet to a correspondent node and embraces the care of address in the source route, the correspondent node canuse the source route to return packets to the mobile node, achieving a cheap form of route optimization. Since IP specifies that higher-level protocols should inverse source routes, such source routing methods accomplish mobile networking without creating any new protocol.

Since all IPv6 nodes are required to maintain authentication and privacy protection at the networklayer, binding updates can be supplied in a secure fashion to the correspondent nodes that need them. This meansthat route optimization fits naturally within the framework offered by IPv6, and does not have to be done as an upgrade to a huge installed base as with IPv4. Since future Internet nodes are anticipated to be capable of mobility this represents a substantial reduction in the network load to be constant by the IPv6 Internet.

## III. REQUIREMENTS FOR MOBILE COMPUTING INCHALLENGING ENVIRONMENTS

There are two basic requirements for the mobile computing inchallenging environment.

*1. Structural Requirements*

Structural requirements of the system mandate that the mobile devices should practice a social group or information configurations during. Most mobile devices have less memory budget and limited processing power. The emergency management software in order to cover most people must consider this alternative in order to deploy the software across various devices. Due to the escalation of various software platforms the

software must be recognized in a way that it reports the issue of platform independence. Shopping assistants and people in aequivalent family have several devices.

*2. Operational Requirements*

Software must be able to form a swarm expending ad-hoc networking technologies such as Bluetooth. Network congestion may causenon accessibility of the services. During the emergency conditiondue to urgency or users disability; mobile devices are not used efficiently. Software during its operation must act automatically to apprehend and respond to user's condition. It encompasses information of nearest mobile devices and maintain to explicit and implicit user input. Reliable mobile computing requires to that the mobile devices software must be responsible and fault tolerant. Even in markets if internet is not accessible the mobile should form an ad-hoc swarm in order to enquire prices in the local area.

## IV. MOBILE USAGE AND RELATED CAUSES

The capacity to use mobile depends upon:

1. Credit balance
2. Signal strength
3. Users abilities and disabilities
4. Number of SIM with a user at a time
5. Mobile devices capabilities such as GPS and internet.
6. Short range communication
7. Power/ electricity / charge

Balance and package are most vital factor in communication during emergency management. The user can call more people and release agencies. In some cases the SOS calls are conventional to permit the people. Network congestion can also be a cause for non-available services. The user might be incapable to use mobile device. Most people carry one or many SIM at a time of same or different companies. This raises the chances of survivability of person even if one network is not available. It succeeds usage of services such as map and other location software. Elderly people can be taken care by establishing a swarm over the regular online systems. But ad-hoc networks are tough to maintain for a long time.

## V. Mobile nodes Model Based on Grey Prediction and RRM Strategy

The mobile nodes model is assumed. A given geographical area consists of a number of hexagonal mobile nodes, each served by the mobile node. The base station and the mobile host interconnect through the wireless links using carrier. Each mobile node is assigned with a fixed set of carriers CR and the same set of carriers is reclaimed by those identical mobile nodes which are sufficiently far away from each other in order to evadeinterloping. The base station is a mobile node,In mobile nodes, the arrival time of the tasks, their tasks interval time and the message passing overhead among the mobile nodes are imprecise and uncertain. The notion of control of grey predictions is used to calculate future behaviors of a system based on a collection of data regarding the system in order to discover the development law, if any, of the system, and to implement pre-controls on relevant controlling decisions, by using the predicted future development tendency of the system. In this way, it becomes probable forload balancing to inhibit a predicted adversity before it actually occurs, and to enforce controls in a suitable fashion. Using grey prediction can prevent receiving or transferring tasks when mobile nodes load is moderate in the timely future and elude the system is busy in transferring tasks.

## VI. Security an Issue

Security is a necessity for every network, but mobile computing presents more security issues than traditional networks due to the surplus constraints carried out by the characteristics of wireless transmission and the demand for mobility and portability. We can report the security problems for both infrastructure-built WLANs and infrastructure-less ad hoc networks.

Security Risks of Infrastructure-based WLANs because a wireless LAN signal is not restricted to the physical frontier of a building, potential exists for unauthorized access to the network from personnel outside the proposed coverage area. Most security distresses arise from this aspect of a WLANs and fall into the following basic categories: Limited Physical Security: Unlike traditional LANs, which require a wire to connect a user's computer to the network, a WLAN fixes computers and other components to the network using an access point (AP) device.

Security Counter methods protect mobile computing is critical in the development of any application of wireless networks. Security Requirements analogous to traditional networks, the goals of securing mobile computing can be well-defined by the following elements: availability, confidentiality, integrity, authenticity

and non-repudiation. Availability confirms that the proposed network services are accessible to the anticipated parties when needed. Confidentiality guarantees that the transferred information can only be retrieved by the planned receivers and is never revealed to unauthorized bodies. Authenticity lets a user to certify the uniqueness of the unit it is communicating with. Without authentication, a challenger can cover-up a authentic user, thus attaining unofficial access to resource and delicate information and meddling with the task of users. Integrity assures that information is never degraded during communication. Only the approved parties are able to adapt it.

Non-repudiation makes sure that an unit can verify the transmission or response of information by another object i.e., a sender/receiver cannot deceptivelydisagree having acknowledged or sent definiteinformation.

## VII. Service Availability Protection

The Collaborative Reputation Mechanism (CORE) is offered, in which node cooperation is motivated by acollaborative monitoring and a reputation mechanism. Each network object keeps track of other entities' collaboration using a technique called reputation. The reputation is calculated based on various types of information.

Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using collaborative technique itself are prevented.

## VIII. Trust and Key Management

Most of the protocols make an supposition that efficient key distribution and management has been executed by some kind of key distribution center, or by a certificate authority, which has power to keep linking to the network and cannot be negotiated, but how to sustain the server safely and keep it accessible when needed grants another major production and cannot be simply solved. To keep the n special nodes obtainable when needed and how the normal nodes know how to localize the server nodes make the system maintenance challenging.

## IX. Conclusion

Mobile computing technology offers anytime and anywhere service to mobile users by merging wireless networking and mobility, which would stimulate various new applications and services. However, the in-built characteristics of wireless communication and the request for mobility and portability make mobile computing more exposed to severalextortions than traditionalnetworks. Securing mobile computing is precarious to develop viable applications.In this article, we discussed the security issues faced by mobile computing technology. We analyzed the various security threats and describe the existing current countermeasures. We have seen that many security solutions have been proposed to securing WLANs, but no one is able to claim that it solves all the security problems, or even most of them.

## References:


[1]. "LAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE Standard 802.11, 1999 Edition," 1999.

[2]. D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole publisher, 2002.

[3]. J. Walker, "Overview of IEEE 802.11b Security", http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.

[4]. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11", http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[5]. B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[6]. M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 6 , No. 3, pp. 106-107, 2002.

[7]. Y. C. Hu and D. B. Johnson and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02),pp. 3-13, 2002.

[8]. Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, September, 2002.

[9]. A. Perrig, R. Canetti, B. Whillock, "TESLA: Multicast Source Authentication Transform Specification", http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-spec-00.txt, October 2002.

[10]. L. Venkatraman and D. P. Agrawal, "Startegies for Enhancing Routing Security in Protocols for Mobile Ad hoc Networks," JPDC Special Issue on Mobile Ad Hoc Networking and Computing, Vol. 63, No. 2, Feb. 2003, pp. 214-227.

[11]. P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2002.

[12]. Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proceedings of the *6th* International Conference on Mobile Computing and Networking (MobiCom'2000), Aug 2000.

[13]. [13] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of the 6th International Conference on Mobile Computing and Networking (MOBICOM'00*)*, pp.255-265, August 2000.

[14]. H. Deng, Q-A.Zeng, and D. P. Agrawal, "SVM-based Intrusion Detection System for Wireless Ad Hoc Networks," IEEE Vehicular Technology Conference, Orlando, October 6-9, Fall, 2003.

[15]. L. Zhou and Z. J. Hass,"Securing Ad Hoc Networks," IEEE Networks Special Issue on Network Security, November/December, 1999.
[16]. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," Proceedings of the IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.
[17]. LeventeButtyan and Jean-Pierre Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000.
[18]. PietroMichiardi, RefikMolva, "Core: A COllaborativeREputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks," Proceedings of the Conference on Communication and Multimedia Security, 2002.