Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

Towards Dependable Pervasive Systems

A Position and Vision Paper

M. Kaleem GALAMALI, Assoc. Prof Nawaz MOHAMUDALLY

Abstract -- Previously when wireless networking did not exist yet, people were awaiting wireless technologies with eagerness. Now 802.11n technology makes it a reality. Before 802.11n intermediate technologies were devised and people have had a good feel of how wireless technology operates. With this situation, several questions crop up:

i. **Are wireless technologies so suitable?**
ii. **Are wireless technologies we have yet, suitable for ubiquitous computing to be widely deployed?**
iii. **Does it mean that wired technologies have become useless? Do wired technologies have any place in this new era of computing?**
iv. **Have the wireless and ubiquitous technologies become dependable for people as customers to adopt them as compared to dependability of wired technologies?**

This paper attempts to find the features required to make the ultimate aim of ubiquitous computing become dependable and reliable.

Key words: ubicomp (ubiquitous computing), reliability, fault tolerance, policing security, Infrastrucured/Infrastructureless environment, network architectures, compression.

M. Kaleem GALAMALI,
University of Technology Mauritius (student)
Mauritius

Assoc. Prof Nawaz Mohamudally
University of Technology Mauritius,
Mauritius

1. Introduction:

1.1 Sensibilities of wireless communication.

Wireless technologies are no longer merely about convenience for applications requiring mobility. It has become a sign of sophistication for business and individuals. Other benefits like no installation costs for cables are also becoming consequent. Would it mean that everyone should just reject wires for the sake of wireless? The wise answer would be no. There needs to be a plan for changeover if ever the change is decided. With such measures certain sensibilities would be protected.

1.1.1 First sensibility is economic reason following the fact that drastic changes can be very costly. All pieces of equipment involved in wireless networking are significantly costly. [1,2]. This is coupled by another aspect of business. ICT and equipment involved is considered as a cost center, i.e. in themselves they are not money generating. It is the services that run over the network (LAN) which generates the income aimed at, in the business. Changing from wired to wireless does not bring much of change of computing functionality. Whatever was being carried out on wired network can be continued on wireless. The so-mentioned advantage of mobility may simply be over-boasted which serves mostly marketing strategy. Just how many people have large range of mobility requirements; most have only one office-table as scope [3-7]. It is understandable why many educational institutions delayed a lot in this change. What was always desired was to have significant improvement in functionality to embark on leap-frog development strategies rather than waste a lot of money into incremental changes [8]. This in turn engendered questions pertaining to reliability of emerging technologies and hence reliability guarantees had to be devised, before mass deployment of wireless LAN technologies [9,10].

1.1.2 Second sensibility, it still remains that bandwidth over wired technology is much higher than over wireless technologies [11]. This means that backbone carriers still work best on wired fiber optic cables. This gap in bandwidth will further increase with time as 10 Gbps and 100 Gbps fiber optics already exist though not fully marketed yet. Wireless technologies cannot fill this gap in foreseeable future and hence wires, mostly fiber optics will continue to exist for very long, with expected lowering of their prices [12,13]. Fiber optics have much better reliability features than wireless technologies.

1.1.3 Third sensibility, the issue of signal integrity is raised [14,15]. Wireless technologies take into consideration signal-to-noise ratio, i.e. signals must be high enough to surpass effects of noise over the transmission distance. It works best if there is less or least noise. If many devices in close proximity have wireless antennas, the level of noise will increase drastically. With each device increasing its signal intensity to surpass noise and hence adding more noise to the environment, a vicious circle of noise generation

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

will be created [16,17]. There may come a point where the transmission fails. A strategy of proper combinations of wireless technologies (unidirectional and omni-directional) together with fiber optic wiring may yield better/optimum functionality of the portion of wireless environment [18,19].

1.1.4 The issue of energy considerations will not be ignored. For wireless transmission, energy consumption varies to the square of range. It assumes electrical power is available and not limiting [20,21]. However, in case of use of battery power, as is the case for ubiquitous computing, rate of usage of available battery power is of crucial consideration. There will be limits to the distance coverable following available battery power and duration we want battery power to last. Side by side, it is also related to cost of batteries as there is a tendency for better batteries comprising characteristics like small size, longer-lasting power, better efficiency, durable, quick recharge, solar recharge, to be very costly [22,23]. It is hence wise to assume that for quite some decades, people will prefer to buy the most affordable resources, even if they are of lower power. This follows the experience that people have preferred to buy clone computers rather than purchasing genuine Apple MAC(R), HP(R) and Sun (R) workstations even if the latter category is of very superior capabilities. (The same case applied for Concorde Plane which failed much because people prefer the lesser costly airliners even if they take longer times [24]). Hence solutions involving wireless technologies must take considerations of the possibility/reality that people will invest in lesser costly ubiquitous devices for quite some time until the "better" devices become cost-effective. In the mean time, infrastructure to support long range communication should be devised. Relay antennae might be required to reduce battery consumption of devices and hence assist in longer-lasting batteries and further assist in longer available services.

1.2 Issues of Consideration

The above situation gives rise to new issues:

1.2.1 what is the granularity of transmission ranges to be considered?

History has shown that different granularity of networking has engendered different transmission equipments, different routing protocols, different architectures of infrastructure and different reliability levels. Traditionally the three terminologies LAN, MAN, WAN which were devised on wired technologies also shifted into wireless technologies. Following this trend of available technologies, what will be the delimitations applicable for ubiquitous computing? What classifications of technologies/terminologies will follow this scoping concept?[25,26] What architectures will most suit each scope delimitation? What should be the accompanying software which should be devised? To what reliability levels can these architectures and software be brought?[27] How to assess such reliability criteria? These are some questions which will help shape a vision of the future technological progresses.

1.2.2 Separation between node transmission and infrastructure transmission.

As applies to mobile/wireless networking, communication from a node will most probably be with an "Access Point" situated quite closely and the access point will take care about routing the information further. In the concept of ubiquitous computing, mostly the nodes will need a range of mobility and flexibility. What about the infrastructure? The infrastructure including "Access Points", routers, switches, gateways may not really need such mobility and flexibility. They can be built over a wired infrastructure covering from a small area to a whole building. An infrastructure over fiber optics may be very easy to install, offers very little sources of interference, can contain quite big bandwidth availability suitable for many channels of audio and video. Other characteristics like upgradability, i.e. increase of number of nodes, low delays, low congestion probability, lesser needs for retransmissions and efficient energy management will all become welcome. Furthermore the possibility of integrating very many services over the same infrastructure is also considerable. These can include telephony, messaging, internet services as well as other services like surveillance, sensor-based applications like fire detectors, location-based services, back-up services and many others, all of them at respectable Quality-of-Service.

1.2.3 How will long range wireless services accommodate ubiquitous platform.

It is expected that wireless communication technologies will be a propelling force to support ubiquitous computing. All developments involving smaller transmission devices, lesser energy consuming devices, longer range transmission devices will all be integrated in ubicomp field. Ubicomp field has two environments:

- Infrastructureless Environment.
- Environment with Infrastructure.

The first one, i.e. infrastructureless is understandable for situations like a forest, a desert etc [28]. Here ad hoc networking is the only way for the ubicomp applications to survive. For environments like a

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

building, a school, an office, a bus or railway station, the environment is not poor in infrastructure [29]. We cannot stupidly enforce ad hoc networking with all its dynamic peculiarities and uncertainties whereas investing in some infrastructure can bring in drastic improvements. Infrastructure can include surrogates, relay antennae and special purpose facilities to act as firewalls, IDS and IPS. Improvements concerned include:

a. Better Quality-of-Service.
b. Lesser delays involved in transmissions.
c. Higher bandwidth of communication.
d. More nodes accommodable in the area.
e. Longer ranges of coverage.
f. Much improved reliability of the Ubicomp network.
g. Improved security enforcements and monitoring.

The design concerns for the infrastructure here are: Should it be wired or wireless? Should different antennas, surrogates, IDS and IPS be wired or should they also depend on wireless? The obvious question to help in this decision will be "what is the reliability of each?". Till present level of technology, reliability of fiber optics is much ahead. Reliability of wireless is debatable [30,31,32]. Reliability of wireless communication can be understood in terms of its granularity/scope of ranges concerned: Reliability of wireless communication in WANs, MANs and LANs each have fairly varying reliability considerations. Of these, LAN wireless communication is claimed to have reached most respectable standards with the 802.11n standards. Reliability for fiber optic communications has mostly same considerations irrespective of range, number of nodes, amount of traffic (so long below congestion limits) and Quality-of-Service needs [33]. At least the variations are much reduced as compared to wireless communication.

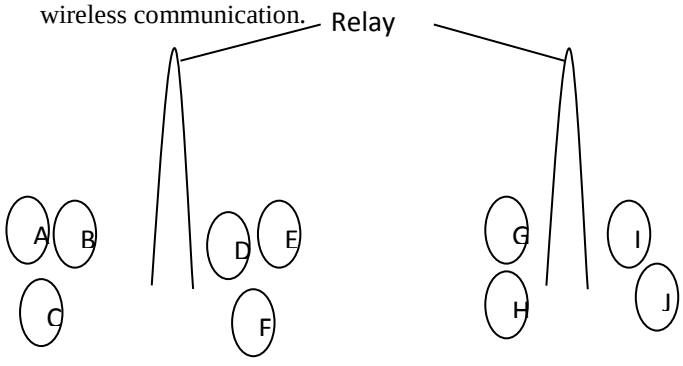

Figure 1: wireless transmission over relays

A subject of study is explained here: If relay antennas are communicating to each other via wireless, how will the resulting situation/ environment be depicted. Refer to figure 1.

The relay antenna will serve purpose of longer range communication supposedly to reduce battery consumption of nodes especially in scenarios like node A communicating bi-directionally with node J. The signals emitted by the relays will be of higher intensities and will be very frequent. An adverse/undesirable effect is that the relays will be emitting strong intensity noise for surrounding mobile and ubiquitous nodes like D,E and F. This will result in the nodes needing to emit higher intensity signals to communicate to whether the relays or their neighbours. Battery consumption will in turn increase. This is not fulfilling so well the original purpose of reducing battery consumption of nodes. It is worth mentioning that the problem will be more acute if omni-directional relay antennas are used. A situation similar to as described in section 1.1.3 will be seen. This problem must be addressed and better architectures should be devised.

It is also important to know what applications will be required in the future and to what QoS criteria will they be required [34]. Wireless networking and communication has been improved in bandwidth and throughput to enable video conferencing, video-on-demand and possibly to support Virtual Reality stuffs like museum visit over networks. Will ubicomp work with such types of application? How much data will be required to be transmitted? Sensors transmitting temperature data only might need more bandwidth. If reliance over full wireless networking is made or even on wireless ad hoc networking is sought, will such services be dependable? Or rather, would hybrid architectures be more appropriate since *combinations* of advantages will be devised. In brief, types of carriers to be chosen must match volumes of traffic expected so that dependability features can be reached [11]. Also important to know is the number of simultaneous operations/applications that the ubiquitous platform should be able to support.

Another important discussion for dependability will be the ability for the system to continue giving a service even in the advent of faults/adverse conditions, i.e. what provisions of fault tolerance should be implemented as support for ubicomp [35-37]. This feature can be investigated at several levels:

i. Fault-tolerance of sensors.
ii. Fault-tolerance of services.
iii. Fault-tolerance for wireless communication between nodes and antennas.

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

iv. Fault-tolerance for wireless communication between antennas.
v. Fault-tolerance for wireless communication between infrastructure devices like surrogates, IPS and IDS.
vi. Fault-tolerance for low processing power and hardware availability like low memory, low capacity storage devices etc...

Research is, of course, being carried out at each level and commendable progresses are being delivered. Just like for computers, the race for more powerful hardware for ubiquitous platform is also on. The researches include longer-lasting battery power, integrating solar cells in devices, attempting parallel processing in lower end devices like mobile phones [38-41]. As and when these improvements are marketed, they will be adopted. Possibilities of introducing power in infrastructure in the form of surrogates have also been explored. Surrogates have power of many orders more than nodes and hence they can prevent applications from failing due to unavailable power and add more functionalities to the overall system. Following these purposes of surrogates, it makes it worthy to introduce redundant surrogates in case the primary surrogate fails, the others can continue the services. Surrogates may also host security services like IPS, IDS and Firewalls [42,43].

The question is: will it be wise and dependable to let these support devices communicate among each other over wireless communication? Will other media like fiber optics not offer significantly more improvement in terms of reliability and dependability? This must be decided after studying certain criteria (explained in form of questions below):

1. How much mobility is needed by these support devices? Should it be completely mobile? Should it be unpluggable at one place and be pluggable at other places and what frequency it is required? Or, at its simplest, can we afford these support devices to be static? [3-7] This last situation will happen in case a very respectable number of support devices are deployed and scattered into the infrastructure.
2. What is the volume of data which will need to be transmitted and with what Quality-of-Service? This will be visible if services are spread over several infrastructure support devices as a distributed system, e.g. for security monitoring and back-up service. The synchronisation features, frequency of communication and frequency of updates of data being implemented [44].
3. What level of security is required in the communications between infrastructure support devices?[45-47] The very first level of security for data transmission is to ensure no illegitimate or third parties get a copy of the data, whether data is encrypted or not. This is better achievable in wired transmission specially in fiber optics which do not emit capturable electro-magnetic waves around its wirings. On the other hand, wireless transmissions can be captured very discretely by anyone within close proximity. This means that the first level of security is breached. Strong encryption in wireless usually engenders serious delays [48].

1.2.4 Will the police or defence institutions have a good upperhand in this technology?

This feature will act as a dissuader, preventing from causing any physical damage or illegalities like harassment, causing Denial-of-service and imposting. People like systems where the police can have a quick and easy enquiry be made and solve cases very rapidly [49-53]. We recall in Mauritius, before registration of SIM cards for mobile phones, there were many cases of phone harassment where the police would have very tedious and lengthy and unreliable ways of catching the harassers [54,55]. This problem has been nearly eradicated since all SIM cards' numbers can be very easily traceable to their owners and also with use of caller Ids. Also telephony services keep good enough records on their servers and back-ups, which can be easily recovered and used as proofs when recorded.

Implementing police powers will give impression that system is more dependable and its dissuasive effects will render it dependable [56,57]. However, to introduce the concept of policing, functionalities have to be added. Functionalities like movement/location tracking (which can serve as alibi), communication held and durations, a trusted notion of identifying and recognising users, suspicious situations detection through monitoring (e.g. a user detected at 2 separate location: one is surely "fake"), means for rapid pinpointing of problem areas, possibly face recognition system integrated in ubicomp camera surveillance, possibly also remote-administration for technicians and police who can reprogram/reconfigure to suit their security investigation needs, will all be desirable [58-60].These in turn will introduce need for more processing powers and transmission reliabilities. Again

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

which medium will give more appropriate policing powers to prevent, detect and apprehend people misusing the service?

1.2.5 What degree of service/infrastructure fault-tolerance is desirable?

To understand the concept, imagine an office room using ordinary 36 W T8 tube lights. without artificial light, the room is too dark to work in. We need to ensure availability of light. One fault can be either the tube burns or the corresponding starter or switch. In this case, we can have a second tube fitting on another switch which can still function. If the second one also burns, we can have a third. If this also burns, we can have another provision. The next fault can be: what if electricity sags too much (tube T8 will keep flicking). If we have only tubes, they will all be useless. It is therefore prudent to introduce a bulb which is not affected by electrical sags. Next fault: electricity goes out. We can thus have a bulb or tube which works on accumulated charge. If accumulated charge is depleted, use of batteries can be made. Ultimately we can see that tolerance here is built by having redundant piece of same technology and also provisions (possibly again with redundancy) of different technologies; in this case, many tubes, one or more bulbs, one or more chargeable tubes, one or more sets of batteries.

The wisdom acquired here is that engineers like to have several fallback position levels, with last level practically not arrived at [61-64]. We also recall experience from previously used bus topology as LAN. When people discovered that introducing a pin into the coaxial cable touching its core makes the whole network fail and lose a lot of time, people very widely did so and earned “free consecutive days of vacations” or at least very long lunch times and coffee breaks [65]. The star topology solved this problem by isolating the fault and letting the remaining network continue to function (unless the hub or switch burns).

What is the degree of tolerance implementable in wireless communication? How many levels of fallback is implementable?[66-69] What are the probabilities of falling to each of the fallback positions? This is particularly sensitive because devices called signal jammers and rogue access points are very easy to obtain and operate [70,71]. Businesses would appreciate a way of continuing their business despite failure of wireless communication. A minimal wiring joining several small areas each having short range wireless transmission supporting ubicomp will bring on a big improvement in fallback positions and hence in reliability and dependability.

This is reinforced by another notion: there are potentially more attack techniques over wireless communication than in fiber optics wired communication [72-74]. It may turn out that the cost of implementing appropriate security over wireless may cost more than implementing a secure fiber optic network infrastructure [75-77]. Also, a bundle of fiber optic cables can have more than one path which itself serve as provisions for fault tolerance.

1.2.6 What level of automatic repair of networking faults can be done?

An area of study closely associated with fault tolerance is self-healing architectures and devices [78-81]. The area is new and mostly still exploratory but quite some levels of progress is possible. The areas which can contribute in these are robotics, aeronautics, artificial intelligence including advanced pre-processing [82-84].

There are certain concepts which may help in achieving auto-healing [78-81]. Many of these concepts already exist in engineering fields including software engineering (though under different titles).

1. The number and types of problems that can occur should be known.
   Despite existence of byzantine faults, the more we know about nature of faults, the better we are to prepare an efficient and quick way of repairing it. We also expect a better preparation for automating these repair mechanism.
2. Architecture support for self-healing.
   Hardware industry has devised ways of easy repair which do not need deep engineering knowledge. This has been coupled by miniaturisation and drastic drop in prices. Devices, tend to be specialised as one set of functions in one component/card like sound cards, network cards. They are easily pluggable and unpluggable. Repairing, no longer involves finding which capacitor (or transistor) in a card has failed and replace that component. Rather, if functionalities of that card, e.g. network card not working, simply replace the network card by a new one [85-88]. Such an action can be taken by people lesser trained in computers. Such repair at coarser granularity rather than refined granularity is effected at lesser money cost, time and labour cost. This element contributes to reliability and dependability. When repair jobs

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

are reduced to such simplicities, automated repair becomes possible. A plausible scenario is robotic repair in spacecrafts, ships, planes, underwater installations (e.g SAFE cable), robotic repair of underground installations using small robots in constrained places.

The same concept applies for software repair. If a software seems to fail or corrupted, we will not go find out which line of code has failed and repair it. Rather, solutions like uninstall and reinstall software is usually chosen. Autogeneration of error reports and patches facilitating repair also is a contribution in this field [89,90]. If a solution to this error has already been uploaded on the Internet, the update of software may happen automatically and the work may continue correctly.

3. The diagnostic tools available for Ubicomp.

Diagnostic tools are very important in engineering. It allows verification of the system quite thoroughly in short time [91-94]. It applies for systems which are quite complex. Diagnostic tools consist of a series of testing techniques which have already been devised and bundled in an appropriate order following the particular environment. Several benefits are offered by these tools like low cost, high effectiveness, almost anytime running and good enough pinpointing of problem areas. Most important is that they mask the complexities of such testing strategies and reduce the usage of the software to mere clickings and high-level (easily understandable) configuration choices. They also give close recommendations about how to solve the problem. This can be used and understood by users not so trained in the field. An example is TV, CD/DVD player, radio cassette self-test runs [95,96].

Have the amount of study for diagnostic tools been studied well enough for ubicomp? What strategies of testing and diagnostic will most suit ubicomp?[97-99] How much of these strategies can be extracted from wireless communications field?

Availability of good diagnostic tools helps in getting a business market. Ease of diagnosing even with little knowledge is a decisive factor. Diagnosing and easy and rapid repair of faults will help achieve better availability of service and hence in reliability and dependability features.

The question is what such above-explained mechanisms have been devised to assist in ubicomp networking infrastructure? Have all the possible faults been identified and plan for repair established? Have these reparations been reduced to coarse grain, lesser costly means requiring less technical knowledge? Have appropriate diagnostic concepts proper to Ubicomp been well defined? Have diagnostic tools been well developed? Can these tools be operated by lesser IT trained people?

1.2.7 How will services be made fault-tolerant in ubicomp network?

This perspective is from the application-layer perspective. It will inherit most considerations from distributed systems [100-103]. Any particularity relating to ubicomp will fall into previous topics of discussion and the limits for service fault tolerance will be established from the following:

a. How important is the service?
b. How many users use the service?
c. Bandwidth needs of communication for such and such services.
d. Amount and cost of special hardware to host such service.
e. License needs/cost for installations at several hosts.

The considerations (b) and (c) have to do with proximity of service to users. More users spread over a considerable area and more bandwidth requirements might need more than one instance of the service situated close to users.

1.2.8 How reliable is "compression before communication" strategies?

Research [104] showed that processing is less costly than transmission required. For sure, the level of technology for compression over computers having abundant resources is very advanced. What is the level of compression and decompression reachable in ubicomp networks?[105-107] All compression techniques will not have same number of iterations for running the compression algorithm. The different algorithms will take different times to be executed. They will require varying amounts of "minimum memory" required. The algorithm will vary in the number of bits processed in one cycle; it can be 8 bits, 16 bits, 32 bits or 64 bits (Itanium processing). The performance and delays will vary with number of processors available. All these will decide on the amount of energy to be consumed. Coupled with these considerations is the fact that more complex and faster

Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology - CEET 2014.

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

compression and decompression will heat up the processor more and engender requirement of energy to cool down the processor (usually a fan).

For this scenario, we can analyse performance and delays from point of view of available hardware. Compression and decompression carried by software and main processor will take more time whereas compression and decompression carried by a specialised hardware or chip is much faster and consume lesser energy [108]. The problem will be that they cannot be updated as software updates. Such chips must already be present and efforts to adapt them to various ubicomp environments are continuing. Variations occur in processing capabilities, amount of RAM and energy availabilities. Efforts to include adaptability between different compression powers of ubicomp devices in an environment in one such chip should also be envisaged. More recent such chips should also be backward compatible to reduce cost and allow continued interoperability with older/lesser costly devices in the environment. Standards for such specialised chips are very much desirable.

Such a reliable compression and decompression mechanism will remain important even if battery power and duration increase significantly over time. This is considered valid following the trend of wired networks where compression is still a rich factor, even if fiber optics are quite widespread. Any other improvements than battery power will not reduce the importance of compression techniques.

1.2.9 How reliable are antivirus systems for ubiquitous environment?

History is full of viruses and their evolutions. As and when pieces of technology have been devised for computers, viruses also were found to be developing. Viruses which can corrupt OS and cause physical damages like burning hard disk, run CD-drive so fast that CD crumble into pieces, RAM memory filled with virus replicas [109,110]. When network has been marketed, virus propagating over network and causing all sorts of damage were experienced. The tendency for virus propagation over the Internet affecting e-commerce, e-banking, e-mails and infrastructure like web servers, database servers, DNS servers all can happen. Viruses affecting mobile phones specially PDAs are also common now [111-113]. Whichever be the reasons for malicious people writing the viruses, the existence of viruses must be taken as a fact, affecting ubicomp also as severely as other computing field [114].

Fortunately for computing and networks, antivirus software packages have also been developed and enhanced everyday to fight away new viruses. Companies like Symantec, McAffee, Avast, AVG and others are very successful in fighting viruses [115]. These packages have components specifically written according to the hardware components and architectures, OS being used, types of applications being used and purposes for which they are used, e.g. using Internet browsing for e-commerce. In brief, these packages are devised according to the peculiarities of the IT technology being used [116].

Have such antivirus packages been devised according to the peculiarities of ubiquitous environment? To what extent they have been successful?[114,117,118] The area is also open for research. Issues of concern can include:

1. PC antivirus are powerful and work on powerful hardware. Will ubiquitous antivirus packages be powerful enough since ubiquitous hardware are not so powerful?
2. Where will the antivirus be hosted? On surrogates? On the nodes themselves? Or should it be in a distributed fashion? What should be the architecture of the antivirus software?
3. How active should the antivirus be? All the time or on demand? It will also depend on how much scanning has to be done on the communications.
4. What kind of virus attacks are possible in the ubiquitous environment? This will help build an antivirus standard for ubiquitous environment.
5. What should be the ubiquitous network architecture which best suit antivirus scanning? The architecture must also allow for antivirus update. Should it therefore be connected to the Internet (and hence be open to more attacks)?

Many more issues may be identified and these will help build appropriate antivirus properties. One possibility which can apply to solve issue 1 is to subdivide antivirus into chunks of functionalities and install only the relevant chunks onto its corresponding device. E.g. a device acting as a sensor for temperature needs only the chunk required to scan its hardware communication and its sensor functionalities. Other chunks involving video monitoring, e-commerce issues need not be installed. A video camera will have only its relevant chunk. This is possible since each device will have limited functionalities and an expected limited number of possibilities for antivirus attacks. Hence only a

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

subset of antivirus will be desirable on each device. The question will then be how to chunk antivirus functionalities and ensure its reliability and completeness.

If more complex antivirus scanning is required, infrastructure support will be more appropriate solutions. The amount of wireless communication required will also have to be reduced to a minimum for this strategy to be feasible. Compression is of good help.

Commercial antivirus packages will tend to be devised assuming certain standards involving topology, number of gateways, primary and secondary backups, amount of resources available, device architectures and network architectures. Within these parameters assumed, antivirus performance will be best. Do we have good enough framework/architecture in the ubiquitous infrastructure to best enable commercial antiviruses? Research in it is still ongoing. Commercial antivirus packages are usually cheaper and easier to operate [119].

2. Conclusion:

All pieces of technology of the past and present have been through its embryonic and infancy stages. Ships, planes and road vehicles were all unreliable initially and with time and research, they were engineered to enhance reliability and dependability to such an extent that they now represent a business of millions of dollars daily worldwide. Other devices like calculator, refrigerator, cameras, mobile phones and computers have all experienced several generations of hardware designs accompanied with software with increasing reliabilities over the years. The same tendency will occur for ubicomp. We have lots of progress to make in different fields surveyed in this paper to achieve a level of rarely questioned reliability and dependability as is the case for calculators, washing machines etc. This situation may happen sooner than expected. Reliability and dependability features are key features which will enable the vision of Mark Weiser and M. Satyanarayanan to be fulfilled.

3. References:

[1] Narkes Adilbek**,** "The Cost Issues in Ubiquitous Computing", *Dublin Institute of Technology*, March 2011

[2] PCWorld, http://www.pcworld.com , July 2011

[3] James Bresler Jalal Al-Muhtadi Roy Campbell, **"Gaia Mobility: Extending Active Space Boundaries to Everyday Devices",** University of Illinois, 2003

[4] João Pedro Sousa and David Garlan, **"Aura: An Architectural Framework for User Mobility in Ubiquitous Computing Environments",** Carnegie Mellon University, 2002.

[5] Murat Ali Bayir, Murat Demirbas(University at Buffalo, USA) and Nathan Eagle (Massachusetts Institute of Technology), **"Discovering SpatioTemporal Mobility Profiles of Cellphone Users",** 2009.

[6] Technical White Paper**, "Considerations for Planning and Deploying a Wireless LAN"**, ©2010 Research In Motion Limited

[7] Ibrahim khider, Prof.Wang Furong, Prof.YinWeiHua,Sacko**, "An overview of Geographic Restriction Mobility Models",** Ubiquitous Computing and Communication Journal

[8] Chung Oh-young, **"The Leap-Frog Strategy: A North Korean Developmental Model From the South Korean Experience"**, *EAST ASIAN REVIEW* . Vol. 15, No. 1, Spring 2003, pp. 87-105

[9] OASIS, **"Deployment Profile Template for WSReliability 1.1"**, Version 1.0 Committee Draft 01, 11 April 2007

[10] Lori Bechtold, **"Reliability Roadmap Using Quality Function Deployment (QFD)"**, Boeing Research & Technology, April 14, 2011

[11] Stan, **"The Difference between wired and wireless networks"**, August 18, 2010

[12] International Telecommunication Union, itu/mic workshop on shaping the future mobile information society, **"Broadband Mobile Communications Towards A Converged World"**, Document: SMIS/05, 19 February 2004

[13] International Telecommunication Union, **"The Future of Voice, The Future of Communications in Next Generation Networks"**, Document: FoV/02 January 2007

[14] The Cooke Corporation, Snr- signal-to-noise ratio, 2005

[15] Wei Chen, *Student Member, IEEE*, Rodney S. Tucker, *Fellow, IEEE*, Xingwen Yi, William Shieh, and Jamie S. Evans, *Member, IEEE*, **"Optical Signal-to-Noise Ratio Monitoring Using Uncorrelated Beat Noise"**, NOVEMBER 2005

[16] Nicholas W. D. Evans, John S. Mason, Roland Auckenthaler and Robert Stapert, **"Assessment Of Speaker Verification Degradation Due To Packet Loss In The Context Of Wireless Mobile Devices".**

[17] Hewlett Packard, **Wi-Fi™ and Bluetooth™ - Interference Issues,** January 2002

[18] Simone Fiori and Pietro Burrascano, **"Electromagnetic Environmetal Pollution Monitoring: Source Localization By The Independent Component Analysis".**

[19] Yavuz Erdogan, University of Marmara, Turkey, "**Electromagnetic Pollution in the Computer Labs: The Effects on the Learning Environment",** Fall 2007

[20] Kent German, **Cell phone battery life charts**, http://i.i.com.com/, July 2011

[21] Joon-Myung Kang, Chang-Keun Park, Sin-Seok Seo, Mi-Jung Choi, and James Won-Ki Hong, **"User-Centric Prediction for Battery Lifetime of Mobile Devices"**, 2008.

[22] Mobile Phone Batteries - Price Comparison http://www.shopbot.com.au/, 2011

[23] The Future of Rechargeable Batteries, http://www.electronicswarehouse.com.au, May 2011

[24] Kieran Downes, **"Can we call it Failure? *Digital Equipment Corporation and the minicomputer as an engineering success story"*.**

[25] Jan Steffan, Ludger Fiege, Mariano Cilia, Alejandro Buchmann, **"Scoping in Wireless Sensor Networks"**.

[26] Jan Steffan, Ludger Fiege, Mariano Cilia, Alejandro Buchmann, **"Towards Multi-Purpose Wireless Sensor Networks"**.

[27] Guy E. Weichenberg, Vincent W. S. Chan, Muriel Medard, **"High-Reliability Architectures for Networks under Stress"**.

[28] Scott F. Midkiff, **"Information Infrastructure Assurance in an "Infrastructure-less" Environment"**.

[29] Karen Henricksen, Jadwiga Indulska and Andry Rakotonirainy, **"Infrastructure for**

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

Challenges".

[30] Mário Jorge de Andrade Ferreira Alves, PhD thesis, **"Real-Time Communications over Hybrid Wired/Wireless PROFIBUS-Based Networks"**, October 2002

[31] Bradley Mitchell, **"Wired vs Wireless Networking"**, http://www.About.com, 2011

[32] Erik Rodriguez, **"Wired vs. Wireless"**, http://www.skullbox.net, 2011

[33] ALCOA FUJIKURA LTD, **"Reliability Of Fiber Optic Cable Systems: Buried Fiber Optic Cable Optical Groundwire Cable All Dielectric, Self Supporting Cable"**, MAY 2001

[34] Dr. Sarah Spiekermann, **"User Control in Ubiquitous Computing: Design Alternatives and User Acceptance"**, 2005

[35] Shiva Chetan, Anand Ranganathan and Roy Campbell, *University of Illinois at Urbana-Champaign*,"**Towards Fault Tolerant Pervasive Computing".**

[36] Gaurav Gupta and Mohamed Younis, *University of Maryland Baltimore County, "***Fault-Tolerant Clustering of Wireless Sensor Networks".**

[37] Farinaz Koushanfar, Miodrag Potkonjak, Alberto Sangiovanni, **"Fault Tolerance Techniques for Wireless Ad Hoc Sensor Networks**".

[38] Sumi Helal, William Mann, Hicham El-Zabadani, Jeffrey King, Youssef Kaddoura, Erwin Jansen, University of Florida, **"The Gator Tech Smart House: A Programmable Pervasive Space"**, 2005

[39] POSTnote May 2006 Number 263 Pervasive computing, The Parliamentary Office of Science and Technology,

[40] Jay McBain, Senior Vice President, Autotask Corporation, **"The Future: Pervasive Computing in Healthcare"**, May 27, 2011

[41] T. Scott Saponas, Jonathan Lester, Carl Hartung, Sameer Agarwal, Tadayoshi Kohno, University of Washington, **"Devices That Tell On You: Privacy Trends in Consumer Ubiquitous Computing"**, July 2007.

[42] Harald Vogt, Matthias Ringwald, Mario Strasser, Institute for Pervasive Computing ETH Zurich, Switzerland, **"Intrusion Detection and Failure Recovery in Sensor Nodes"**.

[43] Pradeep Kannadiga, Mohammad Zulkernine and Sheikh I. Ahamed, **"Towards an Intrusion Detection System for Pervasive Computing Environments"**, IEEE 2005

[44] Rodrigo Fonseca, George Porter, Randy H. Katz, Scott Shenker, Ion Stoica, Univ. of California, Berkeley, **"X-Trace: A Pervasive Network Tracing Framework"**, April 2007.

[45] Sandeep S. Kumar, dissertation for Degree of Doktor-Ingenieur, **"Elliptic Curve Cryptography For Constrained Devices"**, June 2006

[46] Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith, **"The Hummingbird-2 Lightweight Authenticated Encryption Algorithm"**, 2011

[47] Helena Rifa-Pous and Jordi Herrera-Joancomarti, **"Computational and Energy Costs of Cryptographic Algorithms on Handheld Devices"**, 2011.

[48] Dina Kamel, François-Xavier Standaert, Denis Flandre, **"Scaling trends of the AES S-Box low power consumption in 130 and 65 nm CMOS technology nodes"**,

[49] SANS Institute InfoSec Reading Room, **"Community Policing on the Internet"**, 2003,

[50] Dean Wilson, **"ISP internet policing resulting in corporate censorship – report"**, http://www.techeye.net, Jan 2011

[51] Mike Yamamoto , **"Policing the Internet"**, http://www.cnet.com/, December 13, 1996

[52] Dr Julia Davidson Elena Martellozzo, **"Policing The Internet And Protecting Children From Sex Offenders Online: When Strangers Become 'Virtual Friends'"**, September 2005

[53] MARCO ISLAND POLICE DEPARTMENT, Case Study on NovaRoam® Mobile Routers.

[54] Edward P. Deveau and Michael P. Lawn, WATERTOWN POLICE DEPARTMENT DETECTIVE DIVISION, **"Annoying/Harassing Telephone Calls"**.

[55] Richard Clayton, *Technical Report,* **"Anonymity and traceability in cyberspace"**, November 2005

[56] Dr. Vincent E. Henry, **"Compstat Management In The Nypd: Reducing Crime And Improving Quality Of Life In New York City"**, 2005

[57] Anthony Minnaar, **"The implementation and impact of crime prevention / crime control open street Closed-Circuit Television surveillance in South African Central Business Districts"**, http://www.surveillance-and-society.org, 2007

[58] Sylvia Mercado Kierkegaard, **"Cracking Down On Cybercrime Global Response: The Cybercrime Convention"**, *2005*

[59] Nigel Morris, Deputy Political Editor, **"New powers for police to hack your PC"**, *January 2009*

[60] Tris Hussey, **"Canadians are you ready for expanded lawful access laws?"**, May 4, 2011

[61] Bryan Cunningham and Tobias Maisch, **"CAD/AVL System Fault Tolerance System Fallback Levels And Concepts"**.

[62] Harichandan Roy, Shuvo Kumar De, Md.Maniruzzaman, and Ashikur Rahman, **"Fault-tolerant Power-aware Topology Control for Ad-hoc Wireless Networks"**.

[63] Sanjay Bansal, Sanjeev Sharma and Ishita Trivedi, **"A Detailed Review of Fault-Tolerance Techniques in Distributed System, (IJIDCS) International Journal on Internet and Distributed Computing Systems"**. Vol: 1 No: 1,

[64] Ben Y. Zhao, John Kubiatowicz, and Anthony D. Joseph, **"Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing"**, April 2001

[65] Donald V. Glen, **"Local Network Assessment"**, NTIA Report 85-174, April 1985

[66] N. Eva Wu, Xiaohua Li, and Timothy Busch, "**Fault Tolerance Ofmultihopwireless Networks**".

[67] Luciana Moreira Sa de Souza, **"FT-CoWiseNets: A Fault Tolerance Framework forWireless Sensor Networks"**.

[68] Richard Alena, Ray Gilstrap, Jarren Baldwin, Thom Stone, Pete Wilson, "Fault Tolerance in ZigBee Wireless Sensor Networks", December 2010

[69] Guangyan Huang ,Yanchun Zhang, Jing He and Jinli Cao, **"Fault Tolerance in Data Gathering Wireless Sensor Networks"**, February 2011.

[70] Sami Azzam, Ahmad Hijazi and Ali Mahmoudy, **"'Smart' Jammer for Mobile Phone Systems"**.

[71] Ahmad Jisrawi, **"GSM-900 Mobile Jammer"**.

[72] Qijun Gu, Peng Liu and Chao-Hsien Chu, **"Hacking Techniques in Wired Networks"**, 2004

[73] Prabhaker Mateti, Wright State University Dayton, Ohio, **"Hacking Techniques in Wireless Networks"**, 2005

[74] Partha Dasgupta and Tom Boyd, Arizona State University, **"Wireless Network Security"**, 2004

[75] SonicWALL(R) , **"Best Practices in Deploying a Secure Wireless Network"**, 2005

[76] ReefEdge, Inc. White Paper: **"Understanding In-Building Wireless LAN Security"**, Nov-2001

[77] Bradley Mitchel, **"Wired vs. Wireless Networking"**, 2005

[78] Giljong Yoo, and Eunseok Lee, *Sungkyunkwan University*, **"Self-Healing Methodology in Ubiquitous Sensor Network"**, February, 2009

[79] Themistoklis Bourdenas, Morris Sloman, and Emil C. Lupu, **"Self-healing for Pervasive Computing Systems"**.

[80] Shameem Ahmed, M Sc. Thesis, **"Self-healing for Autonomic Pervasive Computing"**, August 2006

[81] Shameem Ahmed, Sheikh I. Ahamed, Moushumi Sharmin, and Chowdhury S. Hasan, **"Self-healing for Autonomic Pervasive Computing"**, 2006

[82] Minkoo Kim, We Duke Cho, Jaeho Lee, Rae Woong Park, Hamid Mukhtar, and Ki-Hyung Kim, Ubiquitous Korea Project, 2010

ISBN: 978-1-63248-005-7 doi: 10.15224/ 978-1-63248-005-7-40

[83] Yan Meng, Kerry Johnson, Brian Simms, and Matthew Conforth, **"A Modular-based Miniature Mobile Robot for Pervasive Computing"**, January, 2008
[84] Vijay Kumar, Daniela Rus, Sanjiv Singh, **"Robot and Sensor Networks for First Responders"**, 2004
[85] Kypros Constantinides, Onur Mutlu, Todd Austin, Valeria Bertacco, **"Software-Based Online Detection of Hardware Defects: Mechanisms, Architectural Support, and Evaluation"**.
[86] Lui Sha, University of Illinois at Urbana-Champaign, **"Using Simplicity to Control Complexity"**, August 2001.
[87] Donald J. Reifer, Reifer Consultants, Inc., **"Industry Software Cost, Quality and Productivity Benchmarks"**, April 2004
[88] Principled Technologies, Inc.: **"Options for reducing manageability risks"**, White Paper 2007.
[89] Michael Lam, **"Automatic Patch Generation"**, December 2007
[90] Microsoft Corporation, **"How to: Configure Microsoft Error Reporting"**, December 2006
[91] Brian Peacock IBM Java Technology Centre, **"IBM Monitoring and Diagnostic Tools for JavaTM"**, 2009
[92] Jim Collins, **"Where are you on your journey from *Good to Great*?, *Good to Great*™ Diagnostic Tool"**, 2006
[93] Book: Susan Powers, Andrei Matetic, Mark Roy, **"i5/OS Diagnostic Tools for System Administrators"**, March 2008
[94] Dean Askin, **"Keeping up to date with diagnostics"**, April 2007
[95] Scott MacKenzie and Shaidah Jusoh, **"An Evaluation of Two Input Devices for Remote Pointing"**.
[96] James A.Mears, **"An Evaluation of Two Input Devices for Remote Pointing, 2000"**.
[97] Doreen Cheng, Henry Song, and Alan Messer, Samsung Information Systems America, **"Reliability, Diagnosis – Challenges to Pervasive Computing"**.
[98] Stephen S. Intille, MIT School of Architecture and Planning, **"Designing a Home of the Future"**, 2002
[99] Lynne Rosenthal and Vincent Stanford, **"NIST Smart Space: Pervasive Computing Initiative"**, July 27, 2009
[100] Wilfredo Torres-Pomales, Langley Research Center, Hampton, Virginia, **"Software Fault Tolerance: A Tutorial"**, October 2000
[101] Z. Kalbarczyk, R.K. Iyer, S. Bagchi, K. Whisnant, **"Chameleon: A Software Infrastructure for Adaptive Fault Tolerance"**.
[102] Zaipeng Xie, Hongyu Sun and Kewal Saluja, **"A Survey Of Software Fault Tolerance Techniques"**.
[103] Chris Inacio, Carnegie Mellon University, **"Software Fault Tolerance"**, http://www.ece.cmu.edu/~ece849b , Spring 1998.
[104] Pottie, G.J. and Kaiser, W.J. (2000). **"Embedding the internet: wireless integrated network sensors. *Comms. ACM"***, Vol. 43, No. 5, May, pp. 51-58.
[105] Mikael Degermark, Mathias Engan, Bjorn Norddren and Stephen Pink, **"Low-loss TCP/IP Header Compression for Wireless Networks"**.
[106] Tomasz Podlasek, Joanna Sliwa, Marek Amanowicz, **"Efficiency of Compression techniques in SOAP"**, 2010.
[107] Andreas Reinhardt, Matthias Hollick and Ralf Steinmetz, **"Stream-oriented Lossless Packet Compression in Wireless Sensor Networks"**, June 2009
[108] Bhavin Shah, Jay Gheewala, Jui Shah, Viral Barot, Prof. Young Cho, Andrew Goodney, **"Compression Technique For PCI Performance Enhancement Team Dynamo"**, 2010.
[109] Clay Wilson, **"Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress"**, April 2005
[110] Bob Carnaghi, **"Viruses, Worms, & Trojan Horses"**, www.webpointmorpheus.com, July 2004.
[111] AnthaVP, Antivirus for Mobile Devices V1.0 Ed. 1
[112] Kyle D.Lutes, Charles N. Thurwachter, **"Wireless Viruses: Coming soon to a PDA near you?"**,2001.
[113] By Russell Bourke, **"Protecting Hospital Smart Devices from Viruses"**, December 2006
[114] Yean Li Ho, Swee-Huay Heng, **"Mobile and Ubiquitous Malware, IST-AWSN"**, 2009
[115] Fernando de la Cuadra, **"How an Antivirus Program Works"**, "http://www.net-security.org/", May 2003.
[116] Helen Akers, **"What Are the Different Types of Antivirus Software for Servers?"**,August 2011
[117] Dr. Byeong-Ho KANG, **"Ubiquitous Computing Environment Threats and Defensive Measures"**, January, 2007
[118] January, 2007, **"Ubiquitous Insecurity? How to "HACK" IT Systems"**, 2001.
[119] Elena Vildjiounaite, Petteri Alahuhta, Pasi Ahonen, David Wright, Michael Friedewald, **"Design Guidelines for Analysis and Safeguarding of Privacy Threats in Ubicomp Applications"**

About Author (s):

Associate Professor Nawaz Mohamudally works at University of Technology, Mauritius and has undertaken supervision of MPhil/PhD Students for many years.

M. Kaleem Galamali is a part-time student at University of Technology, Mauritius under the supervision of A.P. Nawaz Mohamudally.