Abstract:
This paper goes for examining different exploration issues of executing the portable entryway to coordinate remote sensor system (WSN) and different systems and another strategy for actualizing cell telephones itself serve as sensor of remote sensor system and different versatile sensor system based applications. Lately, the organization of remote sensor systems are utilized as a part of mixture of fields, for example, medicinal, ecological and environment checking production lines, movement control, structure observing, flame recognition and framework security and so on. WSN comprises of sensor hubs of low power, low information rate correspondence capacity and low preparing force. So there is a plausibility of loss of information which are detected by the sensors furthermore numerous challenges to transmit the detected information to different systems effortlessly. Beat this circumstance, an advanced cell furnished with high handling force sensors are utilized as sensors as a part of WSN or utilized as a door in the middle of WSN and other system and this usefulness of coordinating WSN and different systems through PDA innovation called portable remote sensor network(MSN) is utilized as a part of numerous applications. Rich-sensor advanced mobile phones have made conceivable the late conception of the versatile detecting examination range as a major aspect of omnipresent detecting which incorporates different territories, for Example, remote sensor systems and web detecting. There are a few sorts of portable detecting: individual, participatory, artful, swarm, social, and so on. The object of detecting can be individuals focused or environment-focused. The detecting space can be home, urban, vehicular… Currently hindrances restrain the social acknowledgment of versatile detecting frameworks. Cases of social hindrances are security concerns, prohibitive laws in a few nations and the nonappearance of monetary motivating forces that may urge individuals to take an interest in a detecting crusade. A few specialized boundaries are telephone vitality investment funds and the mixed bag of sensors and programming for their administration. Some current studies mostly handle the theme of portable detecting frameworks. Distributed papers hypothetically or somewhat fathom the above obstructions. We finish the above overviews with new works, audit the boundaries of versatile detecting frameworks and propose a few thoughts for effectively actualizing detecting, combination, learning, security, protection and vitality putting something aside for any kind of portable detecting framework, and propose a few sensible exploration challenges. The fundamental goal is to lessen the expectation to absorb information in versatile detecting frameworks where the intricacy is high.

Keywords: Wireless sensor network, Blue tooth, Mobile sensor network, mobile operating systems; mobile cloud; smart phone; sensors; ubiquitous sensing; web sensing, web based architecture.

I. Introduction:
Remote Sensor system comprises of various little its own detected information and the information gathered structure WSN as well as expansive detecting remote gadgets called as sensor hubs performs some preparing if important. At that point it transmits the thickly conveyed in different areas. These sensor hubs joined information or handled information to other web applications are shift in sizes and containing different detecting capacity which are utilized as a part of different fields. In view of the above sensors, for example, a radio handset for producing radio clarification, we recommend that cellular telephones and remote waves, microcontroller which controls the observing and sensors can supplement one another to perform shared different imparting gadgets. These distinctive sorts of detecting proficiently and adequately. The reconciliation of sensor hubs perform diverse work in distinctive fields remote sensor system and advanced cell mix is effectively. The whole system comprising of diverse sorts called portable sensor system (MSN). This paper depicted of sensors sense the physical and ecological conditions itemized outline of the exploration issues in advanced mobile phone and impart themselves to accumulate worldwide data.
based sensor system (MSN) frameworks situations furthermore the Modern PDAs are outfitted with a different applications taking into account those situations. A Mobile Sensing System (MSS) obliges a client level Application (App) running on the telephone for perusing an interior telephone's sensor, or outer sensors in the WSN and reporting detected information to the Web. To do this, the telephone working framework must offer an Application Programming Interface (API) to deal with the information perusing and reporting. The App of an individual MSS just keeps running on one telephone that does not collaborate with different Apps introduced in different telephones. In a participatory MSS the App is executed on a few telephones in a circulated way and a detecting crusade is sorted out all together the telephone’s clients (members) to sense disjoint parts of the range to be detected. There is a detecting crusade overseer that is accountable for arranging the whole battle. In a group MSS a requester can begin a crusade utilizing his telephone or an expansive number of diverse MSS Apps can be composed so as to maintain a strategic distance from repetitive detecting in a decided zone. A sort of group detecting is spot driven detecting. In artful detecting, members attempt their best to take an interest full or low maintenance. The last three sorts of MSS utilize a server, regularly open through the Internet. The information contributed by various members are joined (coordinated) in this server to construct perspectives of detected information or to expand measurements. The application area of a MSS relies on upon the area of the telephone. It could be close to home (social insurance detecting), (vehicular detecting), home (savvy homes), (urban detecting) or city (shrewd urban areas), provincial, a neighborhood geographic zone or a worldwide geographic zone... The part of a man in urban detecting ought to be astute. Contingent upon the object of detecting a MSS could gather information about (individuals driven) or about the earth (environment-driven). A MSS can actualize detecting procedures consistently, trigged by a client activity, after getting a message of another member… Continuous MSS presents a few key examination challenges: (a) since a MSS depends on volunteer members, hence, gathered examples are regularly haphazardly appropriated in space and time, and are fragmented; (b) learning systems must be utilized to derive member connection and exercises. As of late, Xu et al connected unsupervised learning in the telephone utilizing receiver sensor to check the quantity of individuals talking; (c) member protection must be safeguarded; (d) assessment of reliability of the detected information; (e) guarantee the telephone vitality preservation. The Little Rock task proposed a low-control co-processor to deal with sensors' occasions. The ideal clock recurrence and entering low-control standby mode between edges was utilized for picture detecting; (f) scope control and the specific versatility examples of the members. In some beginning thoughts are introduced about controlling the development of members abstaining from driving them into zones with practically no detecting scope, taking into consideration more prominent scope with less members and higher densities of estimations in a particular district; (g) because of detecting, the exceedingly skewed spatial-transient detecting recurrence relies on upon the telephones that will take an interest in the detecting procedure; and (h) incitement of investment in light of the fact that, from the earlier, members are doing charitable work.

In the distributed overviews a few illustrations of MSS have been displayed. There is a plenty of MSS: some of them are business, others are just a proof-of-idea, and others are frameworks that have just been tried in examination research facilities. The run of the mill illustration of individuals driven MSS is social insurance, which utilizes consistent detecting for genuine infections, or observing individuals. Normal samples of environment-driven MSS are, among others, disasters, activity checking, communitarian climate expectation, clamor level observing in urban communities and air contamination. Mobile applications utilize the mix of diverse sensors. Each distributed study about MSS audits various frameworks, however there are numerous MSS that have not been checked on in those studies.

II. Design Issues of Mobile Sensing Systems
Continuous sensing using GPS can lead to privacy and phone energy consumption problems. If a security mechanism is computationally intensive, the battery will drain rapidly. In this section we review some works which study fusion and learning, security and privacy and energy saving inside a phone or with external sensors that do not belong to a WSN. These works are not reviewed in previous published surveys.

Fusion and Learning
Fusion can be used to design context aware applications. The context of an object is any information that characterizes its state and allows for dynamic changes in applications and/or the automatic invocation of new applications. Context information is derived from these sources: physical internal and external sensors, devices in the environment, and data sources on the user’s device or accessible via the telecoms or Internet infrastructure. Two fusion examples are: (a) an earbud to read a person’s blood oxygen level, body temperature, heat flux and heart rate, and a heart-rate monitor that can be embedded...
into a device like an iPhone to identify a user or determine the user’s mood; (b) InvenSense’s MPU-9150 is the world’s first 9-axis Motion Tracking that fuses data from the three-axis of AS, CS and GS. Indoor Navigation Systems (INS) can be enriched with the fusion of built-in sensors and external inputs such as a map of the floor, a GPS/cell based positioning, or a WiFi fingerprinting. Indoor Android phone localization can be achieved fusing several sources such as AS, magnetometer, GS and RSSI of several Wi-Fi AP.

Learning can be used for inferring the current activities of mobile users. The authors inferred actions like walking, cooking, reading, driving and eating, using the data sensed by the mobile phone and a hidden Markov model. The user’s intervention was needed to label the beginning and the end of each activity. Chen et al. showed preliminary ideas about a framework to analysis and infer human behavior patterns fusing raw WiFi RSSI readings and AS to extract fine grained significant locations in user’s daily life. Two learning examples are: (a) Koukoumidis et al. who used IS to collaboratively detect and predict the schedule of traffic signals using an iPhone in cars instead of the traditionally used sources such as GPS, AS or single axis GS; (b) Imsec is an Android proof-of-concept application which can securely capture, store, and transfer phone camera-generated images in a war zone.

Security and Privacy
System security must avoid denial of service, eavesdropping and illegal physical accesses at the sensing server. Information privacy must be assured implementing data encryption, data integrity, authentication and freshness protection. The use of the phone’s GPS is normally authorized by the phone user. But GS and AS can be used by third party applications in order to infer the location of touch-screen taps without the permission of the phone user. The work presented in provides a simple example where privacy is a barrier to the acceptance of mobile sensing. It uses a framework which includes motion sensor readings, accelerometer and gyroscope sensor data combined with machine learning analysis.

Trustworthy uploading of sensed data to the sensing server is a challenge. Sensors are well calibrated, but humans are less reliable. That is, people must be well educated in the correct use of sensors. Algorithm design for obtaining the optimal solution to the discovery of the truth information reported by different participants is important. This happens when near participants in a social sensing campaign report different data about the same experiment. A theoretical algorithm presented in could be put into practice due to its potential relevant applications.

Security and privacy have also a social aspect: intellectual property laws and other important social legislation are another barrier. In that work three foundational design principles are discussed: primacy of participants, data legibility, and engagement of participants throughout the data life cycle. The expansion of the codes of fair information practice to protect privacy in MSS is proposed. This is a very important topic in MSS because in several countries, laws impose a lot of restrictions on social sensing. Security is a technical barrier and privacy is a personal barrier in telemedicine. In participatory MSS, privacy is the guarantee that participants maintain control over the release of their sensitive information, including the protection of information that can be inferred from both the sensor readings as well as the interaction of the users with the participatory MSS. Each component of the participatory MSS has its own responsibilities for assuring privacy: (a) Sensors: participants that report daily their GPS and AS movement tracking could easily be identified. To avoid this, the frequency of reporting could be varied for example, to report the position only when the street changes; (b) Administrator of sensing campaigns: A malicious admin can identify a lot of critical information about participants; (c) Reporting: If a participant does not use an anonymous proxy for example, his reported data will be easily identified knowing its Internet Protocol (IP) Address; (d) Data processing on the server: The best practice is to aggregate participants’ sensed data to avoid participant identification; (e) Social networks: Normally pictures and audios easily identify a participant. In a good introductory review of data mining and data aggregation is presented. The authors also categorized solutions using some parameters like perturbation, k-anonymity, secure multi-party computation and homomorphism encryption.

There are technical solutions for MSS security and privacy. Some solutions are theoretical proposals or obtained via simulation. An experimental approach is presented in, and others have proposed Android applications. The sensing domain is a general one in and specific for urban sensing in Healthcare is the sensing domain.

The hiding of which phone matches a query and which data is sensed is a way of implementing privacy. A large-scale system resembling a mesh network of sensors is assumed. An inconvenience for mobile phones is that they only could be connected to this mesh infrastructure using WiFi. There is a tradeoff between sensing accuracy and privacy. This tradeoff is related to the number of dimensions, categories, and participants. The server reconstructs
the probability density functions of the original distributions using the sensed values, but without knowing the participants’ actual data. These theoretical ideas must be put in practice to observe results respecting real world scenarios. In the authors focused on the safe processing of the phone sensed data in that mitigating attacks by malware and other attacking software is an important challenge. In GPS, IS and microphone were used and in external sensors connected to the phone via Bluetooth and ZigBee were used. The problem analyzed in is trustworthiness: how to verify that authenticity and fidelity are achieved. Confidentiality and integrity properties are analyzed between the outer sensors and the phone. All the reviewed works need to verify that the running Android application is safe and differ in the way they test privacy: the first two works used Taint Droid to trash the dependencies among data and applications in order to register possible alterations of data. This is a very cheap solution which does not include additional hardware; perhaps they should consider including the modern Trust Computing Platforms incorporated in recent commercial phones. On the contrary, requires additional, expensive and sophisticated mechanisms that can limit its applicability. That is, each sensor had a cryptographic key which is known to the Secure Data (SD) card which has a key also known to the outer sensors. The key distribution is done directly between the SD, without the intervention of the phone and the outer sensors. In this way, the malware will not be aware of the keys. Among the seven limitations they exposed, one curious limitation was that data cannot be displayed to the patient because it would be vulnerable to malware. They suppose the outer sensors communicate with the phone using Zigbee, Bluetooth or its secure protocol, so in practice they can only directly use Bluetooth technology, and support its secure protocol over it, because Zigbee is not directly supported in present phones. Trusted computing platform is used in recently released phones. Energy Saving Energy saving is a very important issue in mobile App design and implementation. A kernel module of the modern smart phone’s operating system manages it using energy profilers. For example, Eprof considered that optimizing energy consumption is of critical importance and it was the first fine-grained energy profiler for phone Apps. It was implemented on Android and Windows Mobile. The aim of Eprof was guessing where the energy was spent inside any App, for example in storage. Energy saving is a key issue for continuous sensing because the phone battery drains rapidly. For this reason, the main objective of energy saving in continuous sensing is to control the actions of sensors and suspend them when necessary. To do this, three different kind of sensors were identified in: (a) Basic: sensors that work continuously, for example cell identification sensors; (b) Light-Duty: software-based sensors that do not consume too much energy; (c) Heavy-Duty: sensors that are not necessarily always on, for example GPS and microphone.

Energy saving has mainly been studied in theoretically the past, but in a report in the healthcare domain was presented which explained the lessons learnt after their system was tested with several people for a long time. There are several approaches to control energy saving. Among them we review Green Technology and specific middleware’s for energy saving. In this context energy saving in mobile devices follows three directions: (a) Energy profiling which satisfies quality of service and quality of experience; (b) Utilization of multiple radio switching to save energy still remains challenging; (c) Effective transmissions: mobile applications and services can include inherent power-saving designs, predication- based adaptation by learning the historical pattern, and proxy-based caching.

The optimization of the sensor duty cycles was studied in using different mathematical models. A Markov chains model was formulated for minimizing the expected user state estimation error, while maintaining an energy consumption budget. The results were numerically compared against uniform periodic sampling and they found that the performance gains depend upon the user state transition probabilities. Machine learning algorithms performing offline training of the inference models were used to observe the value stability provided by the sensors in order to disconnect them for some time. During that time interval, last read values were used. The calculation of the intervals of time in which to use the last read values of the sensors in order to optimize the energy saving is challenging. These theoretical models must be verified with real scenario experiments because there are several issues that influence energy consumption. Those issues can be taken into account theoretically, for example, the sporadic variation of the wireless channel in the presence of obstacles. AS sampling frequency versus sensed data accuracy impacts energy savings. This affects human activity recognition. For example, showed a sequence of moderately-long lasting activities, and many of these commonplace activities can be classified quite accurately, without requiring sophisticated features or high sampling rates. The main objective of energy saving middleware is to accommodate the energy consumption taking into
account real world problems and minimizing its energy consumption overhead. In, *Acquisitional Context Engine (ACE)* middleware observes the behavior of the participant in different physical contexts (home, driving a car, in office...) and correlates sensor values that could define the location (context attributes) in which the user could be. It dynamically learned relationships among various context attributes and basically used *inference caching* for opportunistically inferring one context attribute and try to do speculative sensing. In [103], Lee et al. designed an energy saving middleware applied to close participants avoiding them the necessity to repeat the sensing process over a shared geographical area. Group formation, the distribution of sensing planning, and the mobility of participants were identified as challenges. An identified barrier was that although the participants were closely located (less than 10 m apart) sometimes they did not easily share their resources with other unknown people. In our opinion they identified typical problems of *Mobile Ad hoc NETworks (MANET)* that still are not efficiently solved in our days. They also have to treat the problem of service disruptions due to *Bluetooth* channel issues.

A cloud can be used to balance opportunistic sensing by observing the proximity of participants and their trajectory. The authors simulated fair scheduling algorithms of sensing operations among the participants. Their objective was to eliminate redundant sensed data and improve energy savings. More work must be done to take into account more complex phone user movements and energy wasted in the communications with the cloud and close phones.

Machine learning algorithms can be used to dynamically predict device energy-efficient consumption. In this case, authors showed that the best results were obtained using neural networks and k-nearest neighbor algorithms.

### III. Design Aspects of Mobile Sensing Systems

Fusion, learning, security, privacy and energy saving are normally implemented in the phone and they are sometimes coordinated by a sensing server. In this section we will present a holistic view of the design of a MSS that can include a WSN, a cloud and a social network. There are theoretical research works that consider the optimization of the above issues when a WSN is considered for extending the sensing capacity of phones. Other works consider cloud and social network technology. We review these works that have not been included in other surveys and present some new ideas of the design of practical MSS.

In Figure 1 we show our MSS schema. The sensor-rich phone executes a sensing mobile *App*. This *App* is downloaded from an *App* store, uses the phone’s sensors and can access a WSN using a middleware. Moreover, several geographically near phones can communicate locally their sensing tasks to improve sensing. The WSN is not part of the MSS. The phone can receive data from the coordinator of the WSN, extending the sensing capability. Moreover, the phone can upload sensing instructions to the WSN coordinator. The phone reports data to the server application using Web services. The server always makes the presentation of the sensing results to the consumer. In case the sensing process is organized by an agency, this server will be in charge of *distributing sensing tasks* among the participants (the same applies for crowd MSS). This server can be executed in a machine or it can be executed in several geographically distributed machines in order to distribute the computing load (configured as a *cloud service*). In case the consumers were part of a social network they can use it to share sensed data, processing and visualization.

![Figure 1. System architecture of a generic MSS.](image)

We propose the following ideas for efficiently implementing sensing, fusion, learning, security, privacy and energy saving:

- **Sensing, fusion and learning.** They can be implemented in the WSN, the phone *App* or the sensing server. In the first case, the manager node of the WSN is in charge of sending the fused data processed by a simple fusion algorithm to the phone *App*. The *App* could implement low computation fusion and learning algorithms in order to save energy. The server can implement complex fusion algorithms. Fusion and learning processes can be distributed efficiently among the WSN, the phone *App* and the server in order to balance communications and computations. Web services can be used to report data to an Internet sensing server because it is the most used standard in Internet communications in our days.

- **Security and privacy.** Current WSNs allow encrypting sensed data. This mitigates the adverse
effects of the security attacks to the WSN. We have reviewed several methods to implement security and privacy in the mobile phone, but some privacy methods are implemented in the server. We propose that the WSN implements encryption, and security and privacy processes be distributed among the App and the server. This distribution can be done depending on the power of the phone and the complexity of security and privacy algorithms.

- **Energy saving.** The WSN can reduce the energy consumption of the phone. The server can efficiently distribute the sensing tasks among phones to reduce the work to be done by the phone.
- **Local communication among phones.** Normally, in opportunistic and participatory sensing the phones do not communicate locally. We argue that local communications among phones improves the energy saving and privacy by allowing the efficient distribution of sensing tasks. A mobile cloud technology can be used where relevant.

Next we present some research works that justify our proposals and our identified research challenges.

**Web Services, Cloud and Social Network**
A server can implement fusion and learning based on the sensed data coming from a phone. For example, Cui et al. show in how a server can fuse inputs from different phones with the aim of guiding the design of energy consumption awareness Apps to preserve the battery of the phone. The energy consumption awareness App makes corrective actions to control the rate, and the sampling duration of phones’ sensors. The design of accurate activity and context detection algorithms can be achieved with several Android phones collecting sensing data sets, in several parts of the World, tagged with appropriate ground truth information about the user activity. Context-aware applications can be built using cloud services for visualization and reasoning. They provide a set of tips for optimizing the communication among the application and the Internet cloud. A context oriented programming model proposed that each component, referred to as a Widget, maintain updated information about a specific context. Widgets were allocated in a cloud server or in a mobile device and communicate with each other using standardized ontology for filtering, fusing and/or aggregation of context information. A directory-based service to update information about the overall collection of Widgets was used and applications could read the last updated context accessing that directory. The main barrier to implementation of that proposal is users’ mistrust, since the privacy is not guaranteed if the mobile devices would not be under the owner’s control.

**Local Phones’ Communications and Outer WSN**
Mobile operating systems or other frameworks allow accessing the phone sensors. However, managing an external WSN is difficult, but this allows energy savings if an efficient distribution of sensing tasks among phones and WSN is done. An introduction to the design of software platforms to access external WSNs is provided in. Next, we present some research issues classified by sensing domains.

In the healthcare domain, a J2ME platform to manage a service that was aware of users’ conditions such as heartbeat, posture, and movement through monitors of physiological signals (for example, electrocardiograph, thermometer, and 3-axis AS) and environmental conditions (for example room temperatures), by communicating with environmental sensors was presented in. Its authors also presented several research issues: (a) communicating to WSN via a mobile sensor router attached to a user’s phone; (b) analyzing the sensed data derived from networks by cooperating with sensor middleware on a remote server to capture someone’s contexts and (c) providing context-aware services for mobile users. Amulet collected users’ health information and forwarded it to a health record system in a secure way. It enabled continuous sensing and actuation, requiring a wireless gateway (phone or AP) only for occasional connectivity from the WSN to back-end servers and other off-body network resources.

**IV. Research Issues In Mobile Sensor Networks**
Among the wide range of mobile sensor network applications, we select three representative research issues for mobile phone wireless sensor deployments: Research issues of msn in biological applications, Research issues of msn in environmental monitoring, Research issues of msn in traffic accident detection system. By these research issues, we explain the utilization of both wireless sensor network and mobile phones as sensing platforms. We provide examples for the research issues and explanation for the

**A. Research issues of Msn in Biological Applications**
Wireless sensor networks (WSNs), Body area sensor networks (BASN) and smart phones are combined together to monitor the patient along with the environmental information and sent this combined information to doctors or medical centers.

1. Deployed sensors of wireless sensor network sense the environmental information such as temperature pleasure, oxygen content, humidity and other air pollutants.
2. Monitored patient wears sensors on his body or specialized sensor can be implanted in his body to measure his vital signs such as blood pressure, body temperature, body acceleration, heartbeat, blood pressure sand oxygen level in blood.
(3) Mobile phone are commonly familiar to people, and hence it is carried by them wherever, they are going outside. This allows monitoring of the person in different environmental situation without limiting the mobility of the monitored people. Combining the above said three features personal health monitoring is described in detail which is given below:

Figure : MSN in Patient Monitoring
(a) Mobile phone collects the environmental information from WSN sensors such as peak flow meter, Pollution sensor etc which are interfaced to the mobile phone via a Bluetooth connection.
(b) Body area network (ie) sensor nodes within the patient body records patient vital signs and these information are sensed by mobile phone sensor and recorded in the mobile phone.
(c) Mobile phone couple the information collected by wireless sensor network and body area sensor network and perform any processing if needed.
(d) Using the available network the mobile phone transfer the coupled information to the hospital or medical center for long term inspections and further future examination of the patient and also send to the doctor’s mobile phone to get immediate suggestions and medicines in the case of emergency.

B. Research issues of MSN in Environmental Monitoring
In environmental monitoring, the fixed Wireless sensors/Actuator Networks are integrated with web based technologies through the mobile gateway and thus creating smart phone based mobile sensor networks which are used to measure the environmental parameters accurately and instantly which is shown in figure2.

In environmental monitoring system, WSN consists of a number of sensors deployed in different environments. These sensors are programmed in different manner according to the respective applications. They have different sensing capabilities to monitor the environmental parameters such as temperature, pressure, humidity, air quality, the pollutants, the oxygen content, etc. They sense the environmental conditions and at the same time, they communicate themselves to share the collected information for the purpose of gathering the complete information about the environment and send the information to the base station or other network through normal gateway.

Since the WSN sensors have small transmission range, they are not able to send the collected meta data to the external network easily. So, there is need for the implementation of mobile gateway to collect the meta data from WSN sensors and make the meta data to well formulated data before sending to the external network.

Smart phones are equipped with powerful CPUs, different internal sensors and high range transmission tools using the internal sensors, smart phone sense some environmental parameters of the surroundings and also receive the environmental data collected by WSN sensor node through wireless transmission apparatus. Then smart phone combine its own sensed data of the surroundings and the received environmental data from deployed sensors of WSN and process the combined data and change it into complex meaningful information. After processing, the Smart phone acts as a sensor gateway and sends the d processed information to the data server over the internet. Data Server the store the information in database which is accessed by authorized users.

C. Research issues of MSN in Traffic Accident Detection System
Usually Traffic accidents are detected by in-built automatic accident detection systems which are fixed vehicles. This facility is not available in most of the vehicles. To overcome this situation, we have provided an alternative system called smart phone...
sensor Network which combines the feature of advanced computational capabilities of smart phones such as iPhones and Android phones, etc. and web services such as Facebook, Google Maps, etc. Android smart phones run Wreck Watch application helps the smart phone users to detect the car accidents in real time and hence the travelers can change their travelling route and avoid the traffic jam around the accidental area.

Figure: MSN in Accident Detection System

Wreck watch is divided into two main components.

1. Wreck watch client
2. Wreck watch server.

Wreck watch Android client detects car accidents based on the data received from internal sensors of smart phones such as GPS receiver and accelerometers and hardware such as camera, microphone, speaker phone, etc. Accelerometer measures the vibrations, microphone records sounds and camera takes the accidental photos. Apart from these sensors, interfaces and hardware, Android phones have different Android application activities. Using these application activities, wreck watch Android client test the received accidental data and post them to wreck watch server via HTTP post. As soon as wreck watch server receives the accidental information, it immediately post them to web services such as Amazon S2, XML / Json and Google map from which the first responder receives the accidental information. The accidental information is also uploaded in appropriate servers that are received by the family members. The travelers around the accidental area also receive the accidental information and thus preventing the traffic jam.

V. Key Factors For The Implementation Of Mobile Phones In Wsn

In this, we discuss the technical factors for using mobile phones as sensors instead of deploying sensors in WSN and mobile gateway between WSN and external networks.

Technical Factor

We compare smart phone and WSN wireless devices based on their processors, storage devices, energy resources, sensors, OS and other capabilities.

(a) Processors, Storage devices and Energy resources of Smart phones

In terms of processing and storage, the mobile phones are more resourceful in comparison with WSN wireless devices. Mobile phones are equipped with powerful processors and a considerable amount of memory space. WSN sensor nodes have less powerful CPU and smart phone sensors have powerful CPUs. WSN sensors have memory ranging from 1MB to 8MB and those of smart phones have nearly 16GB. Energy resources are also very low in WSN sensor node and because of this reason, these sensor nodes often cycle to sleep to recover energy. According to user requirements, powerful batteries can be used in smart phones.

(b) Embedded Sensors of Mobile phones

The sensor nodes of WSN capture only primitive data types. But, the mobile phone sensors collect complex data types, such as audio, video and pictures and photos. When compared to WSN sensors, mobile phones can provide rich information about their environment using the advanced sensors. Most of the WSN sensors have only humidity sensors, temperature sensors, light sensors and proximity sensors alone. But smart phones are equipped with more advanced sensors. If we require some extra types of sensors which is not available in smart phones, we can easily attach the required sensors in smart phone via Bluetooth. But in the deployed sensor, it is not easily possible. Furthermore, mobile phones also contain positioning systems such as GPS, Wi-Fi, digital compass, and cellular triangulation, which perform automatic annotation of the sensor readings in the locations where the smart phone resides.

(c) Wireless Technologies

WSN sensor supports the wireless technology of IEEE802.15.4 only. But smart phones support the variety of the wireless technologies such as IEEE 802.15.4, Bluetooth, and GSM/CDMA IEEE 802.11. Bluetooth standard is very useful to interface with external sensors. Using different communication standards in smart phones, we can easily communicate with external networks and communicate with other smart phones and widely deployed sensor nodes of WSN.

VI. Conclusion

In this paper, we have presented various applications based on the smart phone feature of its larger number of embedded sensors, wireless standards, and interfaces. Using mobile gateway and mobile sensor.
networks, an application designer develop new applications and implement them based on web based wireless sensor network architectures. We have also discussed the mobile gateway concept for metadata retrieval of sensor nodes of WSN, its enrichment with smart phone information and sending combined information to the server side which is used by web applications. Data from many smart phones can be also combined and in conjunction with web services to create powerful real time applications and share this applications with multiuser through distribution networks. Implementing smart phone based sensor networks become familiar in recent years due to increasing number of smart phones and increasing sensing capabilities, different types of hardware, standards and interfaces equipped in smart phones. The efficient implementation of mobile sensing systems is hard. We finally present some learnings:

1. Sensor fusion (producing software sensors) is still in its infancy. Learning must be used to empower mobile sensing systems.
2. Healthcare external sensors may be included in the long term in phones.
3. Communications between phones and wireless sensor networks (or single external sensors or other phones) must overcome the present limitations of Bluetooth, Wi-Fi Direct or Wi-Fi Tethering technologies to form efficient multihop Wi-Fi (or other technology) communication networks. Research trends on machine to machine communications could improve the current ad hoc communication among phones.
4. The middleware to access sensors in the wireless sensor network may fuse different physical sensors values in order to provide high level semantic information for context awareness applications. It must be also be cross-platform and manage multitasking applications in the phone. Consumers should be enabled to subscribe to sensing event campaigns in order to receive alarms when appropriate.

References