Wireless Urban Sensing Systems

CENS Technical Report #65

April, 2006

Mani Srivastava*, Mark Hansen*, Jeff Burke*, Andrew Parker*, Sasank Reddy*, Ganeriwal Saurabh*, Mark Allman**, Vern Paxson**, Deborah Estrin*

*Center for Embedded Networked Sensing Systems, UCLA

**ICSI Center for Internet Research

mbs@ee.ucla.edu, cocteau@stat.ucla.edu, jburke@hypermedia.ucla.edu, adparker@cs.ucla.edu, sasank@ee.ucla.edu, saurabh@ee.ucla.edu, mallman@icir.org, vern@icir.org, destrin@cs.ucla.edu

I. Motivation & Objectives

I.A. Emerging personal, social, and urban sensing applications

Application context inevitably drives the architecture design choices and the definition of services needed in a network. Over the past decade, the emergence of unanticipated applications of the Internet, such as peer-to-peer file sharing, networked gaming, podcasting, and voice telephony, has contributed to a pressing need to rethink the core Internet infrastructure and its accompanying architectural choices. To truly lay a foundation for tomorrow's infrastructure, however, requires going beyond simply reacting to applications that have already emerged, to proactively considering the architectural implications of new *classes* of applications. A key area in this regard involves embedded sensing technology, presently poised to moved beyond scientific, engineering, and industrial domains into broader and more diverse **citizen-initiated sensing in personal, social and urban** ones. Today, applications are emerging which draw on sensed information about people, objects, and physical spaces. These applications enable new kinds of social exchange: By collecting, processing, sharing, and visualizing this information, they can offer us new and unexpected views of our communities. To achieve their potential, these applications require fundamentally new algorithms and software mechanisms, because *physical* inputs now become critical. The research described in this proposal seeks to identify and develop an overall network fabric architecture that through various services coherently embodies such algorithms and mechanisms.

The applications considered in this proposal can be divided into three categories that define how widely sensor data are shared: **Personal, social and urban**. Medical monitoring is a good example of a **personal application**; observations about a patient's personal space, their heart rate or blood sugar levels, are only shared with the patient's healthcare provider. By **social applications**, we mean situations in which data are shared among a group of participants, some, possibly all, of whom contribute data. Applications of this sort are best thought of as combinations of data services and "social networking software." For imagers and audio sensors, we see precedents in podcasting and in sites like Flickr. Finally, **urban-scale applications** involve sharing data with the general public. The scope of these applications is much larger and there might be an emphasis on identity control. In some cases participants may prefer to share data anonymously or "pseudonymously."

These emerging applications raise a host of important and challenging questions, whose answers potentially reach deep into the network architecture. What mechanisms will enable those who deploy sensors to share data in a controlled way while respecting the privacy of those being sensed? Can the network assure basic quality checks for data? By providing a suite of network services can we encourage responsible sensing practices? **We will argue that connecting these systems to provide such basic assurances requires new network architecture. Such an infrastructure**

aims not only to aid organizations in implementing a wealth of proliferating sensing applications, but also to promote citizen-initiated sensing projects. We do not propose the development of new applications per se; but to be effective, our research will require developing and deploying test cases. Through these trials, we will experiment with different architectural choices, identifying those that promote sensor-based applications to thrive.

Urban sensing applications are on the rise, in part, because of a basic technological fact: Sensing hardware is becoming more portable and more affordable. In terms of sheer numbers, sensors will completely dominate tomorrow's global networking infrastructure. An initial model might suppose groups of sensors structured as *enclaves*, in that we confine the interconnection between them and the global network through thin, controlled links, rather than broadly. However, such a dichotomy will inevitably erode with time. Much of the utility of the urban sensing applications comes from integrating disparate forms of information; sometimes quite deliberately, sometimes serendipitously. The dynamics of this underlying utility mean that we will see few natural, sustainable enclaves - instead, existing ones will over time bleed together (in terms of interconnections between them). Thus, we argue there are *two* major evolutions in the offing: from single-domain sensornets to collective/federated sensornets; and from these to their integration into the full global infrastructure.

A fundamental consideration regarding this evolution—a reality that we cannot neglect—is that this progression will proceed *regardless* of whether we architecture for it or not. The critical point, however, is that the one path towards a coherent network in the future is for us to *explicitly* architect for the progression. In addition, for the latter evolution (from federated sensornets to integration with the global infrastructure) to have coherence will require *(i)* informing the global infrastructure's architecture with the **abstractions** that arise as we construct the "sensor fabric", as well as *(ii)* importing notions into the sensor fabric from the re-architecture of the global infrastructure. Regarding these latter, we can at this point only speculate. But for the abstractions that we envision arising from our development of sensor fabrics, we anticipate a number having significant relevance to broader FIND efforts: *(i) space-time* coordinates as providing fundamental network notions of location/addressing, *(ii) policy-mediated rendezvous* based on data properties and meta-data, and *(iii) aggregation-based reliability,* in which the network supports as first-class functionality the notion of "good-enough-equivalence" for determining how to substitute one data source/sink for another when necessary. More broadly, embedding these notions into the network's operation shifts the network from a *host-centric* nature to a *data-centric* nature. Doing so in turn opens up large possibilities in terms of selective sharing of information, privacy, and accountability, as well as more traditional concerns of robustness and graceful degradation via automatic failover. On the flip side, the data-diffuse nature of the network requires rethinking notions of defining and enforcing identity.

I.B. To sense in the city: Privacy and the selective sharing of data

I.B.1. A new sensing context

In the last five years, the notion of a sensor network has changed. Scientific applications have advanced the underlying technology, expanding sensing capabilities and offering richer control dynamics. While this proposal does not draw its motivation from questions of science, the role of sensing technology in the environmental sciences provides an interesting point of comparison. At present, the human experimenter has (re)emerged as *the* important component of a scientific sensor network; new observing platforms are built on rich feedback loops that allow scientists to interactively program or task sensing hardware in response to data analysis conducted in the field. As the cost and complexity of deployments drops, more and more hardware is finding its way into the environment, alongside streams, deep into forests, atop mountains.

Unlike scientific applications, however, **sensors for urban applications are already "out there,"** watching and listening. Mobile phones provide us with sounds and with imagery from our homes and neighborhoods, and the near ubiquity of wireless access in an urban setting allows us to publish or share data easily, immediately. Soon private citizens will have access to a greater diversity of sensors, allowing them to make even more detailed observations of their communities.

Unlike scientific applications, **the hardware contributing to an urban application is not owned and managed by a small number of central authorities**. Citizens carry sensors. Citizens contribute data. Voluntarily. A single entity does not pose interesting "hypotheses," design experiments, force participation. Instead the process of learning from an urban environment can be organic and decentralized, existing more in the realm of social networking software. However, the power of this network still comes from our ability to actuate (to identify and respond to events, applying a kind of filter to events); to aggregate data in space (across blocks or neighborhoods or the entire city) and time (the last hour, week or month); and to coordinate activities.

Unlike scientific applications, **to sense in the city is to reveal its inhabitants**, and inevitably sharing data raises privacy concerns. Broadly, this proposal creates a fabric of services that, by their very functioning, protect the object of a sensor's attention. We will consider two scenarios, both with different implications for data sharing: 1) a private citizen installs sensor in their private space; and 2) a private citizen carries or deploys a sensor in a public space. While these involve private citizens, the network infrastructure proposed to support selective data sharing will help set expectations on the part of the general public, expectations that will hopefully inform the sensing practice of institutions.

I.B.2. Two scenarios

Private citizens, private spaces. We begin with a private citizen installing a sensor in their private space (to observe their home or their possessions) or on their person (to monitor their health, their physiological conditions). These are **personal** applications. In some cases, these data are strictly personal and the citizen will expect complete privacy. If divulged, the information from this sensor might reveal information about the citizen that could expose him to social or financial repercussions. Smart homes, for example, process their data locally to, among other things, adapt heating and cooling for energy efficiency; these data also implicitly carry information about when the home is occupied. Remote health monitoring requires that personal data be transmitted securely to a monitoring authority; the privacy of these data may be mandated by existing healthcare regulations.

A private citizen may wish to share their data with a small circle of friends; these are **social** applications. The precedents for these applications include Flickr (images), Vimeo (video), Odeo (audio) and Plazes. In these cases, the hosting service is trusted to provide access to data under conditions specified by the contributor. When dealing with sensors, groups of neighbors may collectively decide on a kind of data collection action, to perhaps measure sound levels from a nearby freeway or track congestion along side streets in the area. It is also likely that geographically dispersed communities will form around data collection, in the style of plane spotters, for example.

At an **urban** scale, citizens share their data as part of a city- or state-wide project. Initially, we looked to existing participatory science efforts for inspiration. In these applications, participants realize some larger social good by sharing data, even in an anonymous fashion. Participants in these projects record facts about their surroundings, with sponsoring organizations usually providing guarantees of anonymity and simple checks on data quality. While these examples arise in a top-down fashion, we could imagine communities forming bottom-up around data. Broadly speaking, one could view blogs as a kind of local data sharing; and this connection becomes more plausible with the recent popularity of geostamped RSS. In some of these cases, the success of the project depends on the ability of participants to share data in an anonymous or pseudononymous fashion.

Public spaces. In recent years, we have grown accustomed to being monitored in public; imagers or acoustic sensors are often used for security or crowd management purposes. Such data rarely become public but are used only by specific institutions or networks of institutions. With the rise of mobile phones equipped with cameras, we have seen detailed sensing occurring in public places by private citizens. New urban "authoring" platforms invite visitors to a city or a park to share sensed data (images, acoustics, text) publicly with other visitors. These applications create a kind of digital layer of experiences over a place. Here, too, participants may not feel comfortable disclosing their

identities, but choose to participate in a protected way. In these cases, however, the object of the sensor's attention may have a greater stake in knowing how the data are to be used.

I.B.3. Guidelines for privacy and selective sharing

Data are more valuable if they can be "verified." For example, a "subscriber" to a data feed might want to know, with some certainty, the time and location at which a measurement was taken. For some such disclosure is too invasive, and they would prefer to only reveal their location in terms of their ZIP code or county. The same kind of resolution control could apply to the time of a measurement, with some data contributors choosing only to reveal the hour or day on which data were taken. Naturally, there will always be situations in which data can be shared freely, without restrictions. The emerging network of amateur weather stations is an example of this. In fact, in such instances a participant may wish to reveal not only their precise location, but also a set of nearby sensors that should be able to corroborate their measurements. **No matter what resolution a user is comfortable with, it is important that the context assigned to data be verifiable**.

Controlling the resolution or context of a measurement, the data contributor is, in effect, defining a privacy policy. We prefer to use the term "selective sharing" because it captures the idea that participants choose the conditions under which they make data public. For the most of the examples presented so far, the sensing hardware acts in an essentially autonomous way, collecting data at regular intervals or in response to a detected event. **Therefore, policies for selective sharing must be implementable as an automated component of a sensing system**. They should also be easily changed in response to a person's changing public/private context, something that is particularly true for mobile sensors.

In both of the scenarios described above, data sharing has the most impact on the "observed." In the first example, the private citizen is observed, and he alone decided if data are ever to be shared and under what conditions; while in the second case, inhabitants or visitors to the space are observed. Ideally, they would have access to the data being collected by a sensor and could have a say in how the data are used. It is conceivable that sensors deployed in public places could be expected to provide access to the data they are collecting, but only to people within a certain distance of the device. **Here again, we see that decisions about data sharing depend on location and time.** In the next section we give a brief introduction to the proposed architecture that satisfies the basic requirements of verifiability, automated sharing policies and embed location and time into the network fabric. We will return to the specific applications that exhibit these features in Section III.D.

II. Overview and Research Plan

II.A. Overview of system architecture

Our overall technical approach is based around addressing three issues that underlie personal, social, and urban sensing (PSUS) applications: **verification, privacy, and dissemination**. These issues are intertwined; a good policy for verification might impact dissemination and privacy, while dissemination rules can provide privacy protection. By careful design we seek to embed data protections into the basic operations of the network so that data moves with rules that ultimately ensure the privacy protection and information verifiability. In this context we distinguish between the "network" and the "fabric": the former operates with an economy of mechanisms for expressing policy, while the latter provides much richer semantics for data propagation and management. Our proposed architecture incorporates the entities listed below, the precise functioning will depend on our whether they are exposed as components of the network or the fabric. In addition, the architecture will make use of existing network services such a trusted Certificate Authority to provide signed identity certificates and encryption mechanisms for secure communication.

Sensors: sources of data at the edges of the network. They may either be resource rich devices (e.g. [Ho06]) directly resident on the network as host nodes, or resource-constrained devices such as "Motes", grouped many-to-one behind a resource rich proxy gateway node. We note that sensors can have roles beyond simply pure sources of data, providing control points at their interfaces to the

external world for purposes such as configuring the sensor, providing global contextual information, and actuation in terms of local information output. As mentioned above, acoustic sensors and imagers are two widely deployed, mobile sensors in the urban environment.

***Subscribers*:** sinks of sensor data. They may be either individual users interested in data streams and event notifications from sensors, or network applications that subscribe to sensor data and provide archiving, aggregation, distillation, signal search, and other such services to their clients. A physician may subscribe to medical events associated with a remotely monitored patient; or a smart home control software may subscribe to data from sensors deployed by the homeowner. Network applications acting as hosting services could allow users to share sensor data much like Flickr (images), Vimeo (video) and Odeo (audio). Once hosting services exist, it is sensible to posit a Google-like service that facilitates searching sensor signals in terms of queries. An interesting alternative architecture choice might be to preclude sensor data subscribers other than standardized and trusted network services, such as sensor hosting services, and restricting other users to access sensor data only through these services via standard web service APIs. In effect, this will pull into the network fabric the application layer functions that are aware of sensor data semantics.

***Registries*:** network entities that help subscribers discover and bind with sensor data streams. Their role is to provide a service analogous to that of the Domain Name Service (DNS), with a model of administration and deployment-ubiquity similar to DNS servers. Sensors register with the registry metadata information about the sensor data they publish, while subscribers use the registry to search for sensor data streams based on queries over attributes such as location, type of sensor data. The registry maps the query via a tuple space search process to return a handle to the sensor data stream (or, in general, a set of handles). An interesting architectural question is the nature of the handle that is returned. Often a sensor may wish to publish data anonymously while independently providing contextual information at a specified granularity and attested by the network or other sensors for validation. In such as a case, the handle returned by the registry cannot be something that the subscriber can resolve to establish the precise identity or location of the sensor, and some sort of indirection and obfuscation would be needed as an integral part of the registry service.

Mediators: nodes in the network that provide (under application control) selected in-network functions on sensor data streams. These functions would include enhancing streams with attested contextual information at a specified resolution, performing verifications on sensor data values such as range checks or comparisons with values at proximate sensors, performing anonymization of the streams by removing device identification information, replicating streams for delivery to different nodes, and providing reliability in the presence of disconnections. Note the functions span the network, transport, and applications layers, and could broadly be classified into mediator functions relating to context verification and resolution enforcement, and mediator functions relating to stream dissemination. The two types of functions may or may not be collocated at the same physical network node, and these specifics are currently open architecture questions. The functions themselves are performed based on disclosure and verification rules specified by the sensor. Moreover, the mediator would make use of trusted network infrastructure for independently measuring the location and time of data sent by the sensor devices. Distinct from efforts such as Active Networks, the mediators do not manipulate the sensor data values carried as stream payload content, a choice motivated by the simplicity of not allowing complex applications to "program" the mediators. We believe that transformation of sensor values streams for purposes such as anonymity preservation or for scaling to presentation device is best delegated to the user application. We view the mediators to be like firewalls in terms of administration, deployment ubiquity, trust and transparency to the user, while being like distributed content caching servers in terms of inter-mediator coordination and hardware configuration (mid-range rack mount servers).

In a typical application, upon deployment and configuration by its owner, a sensor acquires a signed ID from the certificate authority, and then registers the streams it is publishing with the registry service via the mediator Mediator1. The registration contains information about the sensor type, location, and context. It is these attributes that others will use to search and subscribe to sensor data

streams. The registration will also contain disclosure an verification rules. For example, a sensor device could register (location="boelter hall room 3440", type="microphone", format="spectrogram", UID="andrewparker_mic"). The sensor contributes to the location information in the data stream attribute, since the location may be at a finer granularity than to which the network is able to attest. The sensor may be mobile, in which case it will bind with a new mediator and also update the registry. The role of the mediator is to provide network's testimony regarding the context, and it is up to the subscriber to weigh that against the claims made by the sensor through the values in the data stream. The sensor now begins to publish its data to Mediator1, either proactively or when demanded by Mediator1 (as a consequence of a request by a subscriber). Sometime later the Subscriber sends a query to the Registry through its mediator Mediator2. The request contains disclosure rules as well. It needs to go through the mediator in order for the network to attest the location (or similar attributes) of the requestor as the sensor may have privacy controls that are a function of requestors location. The registry returns a pointer to the sensor data streams, which ultimately point to mediators that host data streams that match the request. During this process the registry reconciles the disclosure rules of the sensor publishing the data with the request and attributes of the subscriber. The Registry forwards the request to Mediator1, which then runs the rules and decides (based on additional context) to reveal itself. Pointer to the stream is revealed to Mediator2, which further negotiates with Mediator1. Now, Mediator1 forwards data to Mediator2.

II.B. Research plan

As a first step to enable exploration, we envision implementing the proposed architectural components using a collection of peer-to-peer and application-level service mechanisms. These are described in Section II.D. While such an approach greatly facilitates deployment, these overlay techniques fundamentally limit the integrity of both context verification and privacy protection. More broadly, such overlay approaches threaten to take us away from the economy-of-mechanism for which architectural efforts should strive, instead bloating the waist of the Internet's present "hourglass" architecture with application-specific semantics in order to achieve adequate performance. As such, layering our components atop the current architecture—or overlay extensions of it—can only play an effective role for exploratory experimentation

On the other hand, if we carefully identify a parsimonious set of primitives to support these new applications, we can attempt to foster a flourishing of new applications with minimal impact on the economy--and consequently robustness--of the new Internet core. The notion of parsimony-of-mechanism, however, likewise imposes a requirement that we determine which of our architectural elements truly need core support, and which can be adequately supported by edge application services layered on top of the core mechanisms.

Therefore, we propose to implement PSUS applications and supporting services first using peer-to-peer, and then evolving towards structuring on top of native network services. In particular, we will develop, implement, and deploy support for *verifiable context*, low-level *data naming*, and *selective sharing* progressively in both of these contexts. Our hypothesis is that the more radical native network services will offer greater integrity, verifiability, scalability, and robustness; while application-level services offer ease of initial deployment.

We will implement, use and evaluate sample personal, social and urban applications in our prototype wireless cloud. As the effort progresses, we can then replicate this cloud in other places around the country, capturing the cloud's traffic (both empirically and via models) for use as input to research groups studying other networking issues related to wireless and mobility.

III. Technical Approach

In the following subsections we first discuss the architecture design space in context of verification, and dissemination, and then relate it to specific instances of driver PSUS applications.

III.A. Context Verification and Resolution Control

The PSUS applications are data centric and very physical in nature. Properly interpreting sensor information requires both the data values themselves as well as some description of the physical context of the sensor's surroundings. To provide increased utility and assurance to the subscriber while preserving its own privacy, a publisher might want the network to add to the published data stream *attested* contextual information of specified resolution, such as location, time, and comparisons with measurements at nearby sensors. Likewise, a subscriber may seek from the network an audit trail of contextual information to establish data validity and authenticity.

While there is a variety of contextual information, we draw a distinction between contextual information that the network can directly measure, and contextual information that the network can only obtain from measurements at other sensor nodes. Clearly context information directly measured by the network using its own infrastructure carries a higher level of trust. Location and time belong to this category as the network can easily measure these and often needs this information for its own purposes. This suggests that space-time semantics might be directly built in the network fabric. Other contextual data are more application specific with the role of the network being delegated to assisting in the verification and authentication process according to application defined rules.

III.A.1. Spatiotemporal context

Essential to building space-time semantics into the network fabric is the ability for the network to verifiably measure location and time of a node when it injects a packet into the network. The basic measurement part, while not simple under adverse conditions, is conceptually simple and well studied. Using time-stamped message exchange based on protocols such as NTP a node the network can measure the clock offset relative to a sensor node [Mill94, Ganeriwal03]. Likewise, a basestation in the network can measure distance to a sensor node using radio time of flight or signal strength for ranging, and then use multilateration to determine the position of the sensor node [Savvides04a] using similar distance measurements made at other basestations. Even simpler would be for the device to measure its own location and time using GPS. Researchers have also explored estimating location of a node on the Internet based on latency measurements [Huffman05]. However, the key problem is one of verifiability: the location and time estimate must be robust to cheating by a malicious sensor node as well as to manipulation by an external adversary.

Recent research [Capkun05, Lazos05, Capkun06a, Capkun06b] has explored verifiable location mechanisms that exploit physical and geometric constraints together with cryptographic mechanisms. Inevitably, the precise mechanisms are dependent on the physical details. Localization mechanisms can be classified along four axes: the signal they use (RF, acoustic, ultrasound, IR etc.), the measurement they make (time of flight, time difference of flight, receiver signal strength, direction, beat frequency etc.), the infrastructure assistance they need (beacons vs. beaconless localization), and the spatial dimensions they localize in (2D vs. 3D). For the kind of PSUS applications of most interest to us, 2D localization using beacons and radios that a sensor device already has is the most likely form of localization. Within this regime, RF localization techniques based on time of flight, time difference of flight, and signal strength are used by many cellular systems and also available for WLAN and other radio technologies. For the time of flight case, [Capkun05] showed that one can combine previously known cryptographic distance bounding (which exploits the physical limit of speed of light) with geometric constraints to implement verifiable multilateration that limits the degree to which a sensor node or an external adversary can spoof the network about the location of the sensor node. For localization that uses the received RF signal strength to measure distance, our work at UCLA [Capkun06] has shown that by utilizing hidden and mobile base stations together with a challenge-response mechanism and leveraging the physics of signal propagation a network can achieve probabilistically verifiable localization to a given uncertainty. We will leverage such existing verifiable localization schemes for our applications.

While there has been recent work on secure time synchronization protocols that are resistant to external adversaries seeking to manipulate the relative time offsets measured between a pair of

network nodes [Ganeriwal05] there is no "time offset bounding" counterpart for cryptographic distance bounding [Brands93]. However, we note that the time scales in PSUS applications are coarse enough so that the simple strategy of using the time at which a packet from a sensor arrives at the network access point as the timestamp for the data is sufficient. We note that the time and location stamp associated with a specific sensor data can only be verified to correspond to when and where the sensor node sends the data and not when and where it made the measurement.

Once the network has the ability to measure location and time associated with data, one can start to consider more radical ways of using this information than merely annotating data. For example, the network may use space-time identifiers nodes in lieu of IP addresses and use them for routing. Such an approach may be beneficial to cope with mobility and with anonymity, both of which are important in PSUS applications. However, we intend to start by first exploring the use of space-time measurements as a verification mechanism and only later consider their use in moving data around. Accordingly, initially we envision that the network will simply tag the data emerging from sensors and going to mediators with attested space and time stamps.

III.A.2. Physical context based on sensor readings

The physical context of sensor data is richer than just location and time. It includes, for example the orientation of the sensor, measurement made by other sensing modalities, and measurements made by other sensors in the vicinity. Clearly, such additional physical context is of utility to subscriber in interpreting the sensor data or in checking its integrity. For example, the utility of sound level from a directional microphone at a particular location and time is significantly more if the direction that the microphone is oriented towards is also known. Likewise, physical context information may be useful in validating the integrity of information provided by a sensor. One can accomplish by making use of statistical and physical models of how measurements by transducers of different sensing modalities are related (e.g. sound level is a function of temperature), and of sensing channel models that describe how measurements made by nearby sensors relate to each other. Indeed, as the sensor infrastructure for PSUS applications proliferates, the increased spatial and temporal density of measurements will inherently provide additional physical context for validation of a specific sensor measurement. Moreover, application deployments may have "self-awareness" sensors [Kansal05] whose purpose is to acquire information about the physical context as opposed to the phenomenon that the subscriber might be directly interested in.

The context derived from information provided by the sensors themselves is fundamentally different from location and time since the network infrastructure has an independent ability and reason to measure space and time, but has no reason to directly measure direction of a sensor or temperature in the vicinity of a sensor. The role of the network in this case is therefore one of calculating and verifying the context according to application specified rules. For example, an application may request that the network corroborate a sensor reading with the readings from nearby sensors by comparing against their average.

We envision that the mediator nodes in our architecture will provide a suite of common aggregation functions over sensor readings, and an application will specify that the results from one of these functions over sensors in a geographical region be used to associate as context. Note that while the mediator can provide secure computation of the user specified context, it has in general no control over the validity of the input data itself. An approach might be for mediators to adopt a reputation-based system, similar to that proposed in [Ganeriwal04b] for sensor data integrity and by [Allman05b] for Internet anomaly detection. Sources of context information would be tagged with a reputation metric in addition to their resolution: e.g., location measured by network would have high reputation though low resolution, while location supplied by a sensor itself may not have a high reputation but may have high resolution. The mediators will use these reputations to annotate the context information it computes with a trust or confidence levels. Further, the reputations of context sources will evolve over time based on feedback from the subscribers using the context information, and the mediators will need to provide a mechanism for such feedback. Over time, the system will converge towards weeding out untrustworthy or dishonest sources of context information.

III.A.3. Context resolution control

The final element in context verification is the ability for the application to exercise control over the context that is revealed to a subscriber. Clearly, without context sensor data is useless. At the same time however the publisher may not wish to reveal too much of the context so as to preserve desired level of anonymity. Again, mediators will act as trusted intermediary in this. Specifically, the mediators will ensure that even if they have information about the physical context at a finer details, they do not send to a subscriber more contextual information than what the publisher is willing to share. For example, the network may know the location to a few meters but the subscriber may only be willing to share the location information to the zip code level. Likewise, a sensor may be willing to share information only as part of an aggregate in a geographical region. The mediator will deliberately reduce the fidelity of the context information it measures (location, time) or derives from sensor values. In addition, to combat emerging techniques for remote device fingerprinting based on measurements of timestamp drift [Kohno05] and localization using latency measurements [Huffman05], the mediator may add random jitter to packets. Note that the mediator exercises resolution control only over the context; the sensor data values are forwarded unmodified, and it is the publisher's responsibility to a priori blur them as needed.

Besides physical context, also part of a sensor devices network context are network level identifiers such as host name or IP address. To begin with, our approach would be to rely on the level of indirection provided by the mediators to optionally hide sensors network identity from subscribers. Specifically, the subscriber will only be able to trace back the stream handle to a mediator. Normally we expect a sensor to associate with a nearby trusted mediator whose identity does indirectly reveal something about identity of the sensor. In case stronger anonymity is needed, a stream may be routed through multiple mediators, rather similar to how it is done for various anonymous routing schemes. Note that in such evolutionary overlay schemes the sensor nodes do have to trust the network infrastructure up to the nearest mediator. We will also explore more radical network architecture alternatives that perhaps do away with network identifiers and route on the basis of space, time, and local identifiers. When coupled with cryptographic keys bound to space and time, one can potentially preserve anonymity to desired level while trusting relatively little of the network infrastructure and at the same time being able to verify one's spatiotemporal context.

III.B. Application Services for Naming, Dissemination, and Aggregation

The combination of physical and personal coupling enabled by personal wireless sensing devices introduces new naming, dissemination, and aggregation requirements and constraints. In particular, personal physical sensing demands fine grain articulation of selective sharing; we begin with a description of our naming structures in subsection III.B.1. We have also suggested that urban and social sensing applications will flourish, provided a flexible sensor information fabric based on a naming, dissemination and aggregation architecture, to a wide range of data remixing, correlation and fusion applications: we describe an aggregation and processing scheme in subsection III.B.2.

III.B.1. Naming registry

Names touch on how we do dissemination, selective sharing, and verification. The items being named are the data streams published by sensor devices. For example, a mobile phone could have three data streams: an audio stream, a video stream, and a location stream (perhaps something fine grained like GPS, or course grained like reachable cell towers). The naming service, which in many ways can be treated as a publish and subscribe mechanism, is supported by the Registry, and plays a similar role to that of the DNS in today's internet. The Registry maps a tuple space of attributes to a handle (or set of handles) that may be used to operate on data streams. Attributes will typically consist of information such as the sensing modality, data format, location, orientation, etc.

When a sensor wishes to publish a new data stream, it first submits to its mediator a set of attributes and disclosure rules that apply to that stream as specified by the owner of the sensor and its context. The mediator augments the request with verified attributes before forwarding it to the Registry. When a subscriber wishes to a resolve attributes to data streams, it does so by submitting

a set of attributes to its mediator. That mediator, in turn, augments the request with verified attributes describing the requestor (location and time). When the request arrives at the Registry, the query is processed. There are two constraints that must be satisfied before returning handles to data streams. First, the attributes of the data stream and the attributes requested by the subscriber must match in some sense. There are some attributes that naturally form hierarchical relationships. Location is a primary example. These relationships must be known by the Registry. Second, the disclosure rules accompanied by the data stream must be satisfied, which takes into account some aspect of the subscriber's attributes (identity, location, and time).

A publicly browsable registry of data streams may disclose information that the publishers wish to keep confidential. It's for this reason that we leave open the ability of the Registry to act as a first point of access control for revealing the existence of data streams. In some cases, the Registry may consult with the originating mediator before revealing the data stream handle. In either case, once the matching data stream handles are disclosed, there is opportunity for further negotiation between the mediator of the publisher, and the mediator of the subscriber, before forwarding the data. The above described resolution process affords the subscriber privacy protection as well, since the subscriber also goes through its own mediator in order to negotiate the data stream handle.

III.B.2. Aggregation

Personal, social, and urban sensing applications, as experienced by the end user, will straddle both traditional web-based applications, and sensor network applications. We envision a web services architecture that provides a platform to build these applications, in much that same way that applications have sprung up around the Google Maps API and other platforms that give users access to vast amounts of data in a programmatic way over the web. We propose a component-based web architecture for the construction of PSUS applications.

The goals of the architecture are to ease and encourage publication of sensor data by independent data providers, as well as application development by 3rd parties that pull on the published data streams. The primitive functionality provided by the web services will include aggregation, processing, and querying. The elements providing these services are called Application Servers, and act as subscribers to data streams. In some cases the Application Servers will act independently and crawl the network for available data streams, much like a Google or Yahoo. In other cases, the data provider will task application servers to aggregate data, such as a Flickr or a blogging service.

RSS, ATOM and other web feed formats provide a useful, uniform interface to web sites that have stylized update mechanisms, and has enabled the construction of readers, aggregators, and other tools that enable the user to mix, filter, and otherwise experience content in customized ways. In a similar fashion, data streams from sensors should be subject to this kind of end-user manipulation as well. For scalability and robustness reasons, data stream aggregators, in the form of Application Servers, are introduced to provide this functionality.

Rarely will users wish to see the raw data from a single data stream. Rather, some level of processing and aggregation will be performed in order to return something more palatable. The API provided by the Application Servers will encourage modular construction of these applications. Components have ports, over which data streams are exchanged. Existing forms of authentication will be used to ensure that only the right processes are able to read and write to ports. The Application Server provides a web based API to declare components and how their ports are wired. Ports map to URLs, and may be read from, and written to, by performing an HTTP GET or HTTP PUT on the port. It delivers the uploaded data stream to the input ports of the other waiting components. In this way we separate component implementation, wiring, and communication.

We recognize that the preceding web services proposal is one point in the design space, albeit one that has the advantage of allowing one to explore alternative verification and dissemination functionalities in different layers. The verification and dissemination functionalities are essential to the feasibility of PSUS Applications. Aspects of this verification and dissemination have been allocated to the network, mediators, and Application Servers (special types of subscribers). The

appropriateness of our allocation relies upon the trustworthiness, ubiquity of deployment, and resource availability of each component type. A design dimension that we will pursue is the tradeoff between the partitioning of responsibilities, and component trustworthiness/ubiquity/resources.

III.D. Experimental Validation Plans

The following personal, social and urban applications will drive experimental validation of the proposed network architecture. They are examples of the new generation of data-rich PSUS applications emerging at the intersection of location-based services, social information sharing and physical computing. Their ancestors are widely used contemporary applications in **social media sharing** (Yahoo's *Flickr*, flickr.com), **web-based GIS** (*Google Earth*, maps.google.com), **network supported participatory science** (Cornell's *eBird*, ebird.org), **blogging and citizen journalism** (Google's *Blogger*, blogger.com), **GPS-supported fleet and personnel management** (Sprint/Nextel's GPS solutions [Nextel06]). Each of these existing applications combines tagged observations, location/time stamps and contextual metadata. Their data is often manually contributed and resolution control, context verification, aggregation-based reliability and privacy protection are either unavailable or implemented at the application layer. Our **personal health monitoring** (II.D.1) and **urban-scale sound level mapping** (II.D.2) drivers explore, in tractable slices, what is enabled when these capabilities exist at the network level. They are admittedly conservative when compared to the popular applications at the 'edges' of urban culture that helped to prompt this proposal. In those, we see the potential for data-driven applications that take advantage of the new network's capabilities: **urban computing** (Intel Research's *Urban Atmospheres*, urban-atmospheres.net), **physical computing in everyday life** (UK EPSRC's *Equator*, equator.ac.uk), **location-based media sharing** (*Plazes*, plazes.com), **community connectivity** (NJIT's *SmartCampus*, smartcampus.njit.edu), **evidence-based medicine enabled by ubiquitous computing** (*Center for Pervasive Healthcare*, healthcare.pervasive.dk), **city-scale gaming** (NYU's *PacManhattan*, pacmanhattan.com), **nation-scale storytelling** (SoundPortrait's *StoryCorps*, storycorps.net). The third application, a **presence-authenticated social data sharing system** (II.D.3) takes a similarly creative perspective, using the network's new instrinsic capabilities to enable unique approaches to authentication and participation in place-based media-sharing.

These examples also serve to illustrate how the network architecture supports data sharing with privacy protection. Palen and Dourish [Palen03] draw on Altman's privacy theories [Altman75; Altman77] to point out that individuals' privacy regulation is neither static nor rule-based. Instead, "a fine and shifting line between privacy and publicity exists, and is dependent on social context, intention and the fine-grained coordination between action and the disclosure of that action." The proposed network architecture *will not* eliminate legal and policy issues, but *will* support users in determining and applying key contextual information to decision-making about their own data. Hochheiser [Hochheiser02] summarizes current U.S. policy on information privacy with the following concepts: **notice/awareness** of personal data collection and the identity of the collector, **choice/consent** about how the data is used, **access/participation** in the collection process, **integrity/security** protections against loss or unauthorized access, **enforcement/redress** in the case of violations of privacy. In developing these applications, our goal will be to explore how the network architecture design can be consistent with the extension of these concepts into the new domain of user-initiated data gathering and dissemination.

III.D.1. Personal health monitoring

The personal data application driver will be the prototype of a remote medical diagnostic and treatment system that connects health metrics of a mobile patient to a care provider. Personal medical sensing applications are a current area of research [Ng04, Malan04, DeVaul03, Konstantas04] to which the proposed network architecture adds the low-level support for data integrity, privacy and verifiability controls clearly needed for practical use. In such research, systems generally consist of three main parts we group as follows: a body area network (BAN), personal mobile hub (PMH) and application agents. The BAN connects sensors that may include, for example,

an electrocardiogram, pulse oximeter, and temperature devices [Malan04]. The hub gathers data from the BAN and forwards it to an IP network. We would implement this hub on a PDA-class device with multiple radios, (e.g., Bluetooth, Zigbee), and GPRS.

We consider the case of outpatients with chronic conditions that personal sensing (BAN/PMH) would enable to live normally while monitored by care providers. Health data would be regularly sampled as required by a physician and published to the network, relaxing manual logging burden and device storage requirements while providing location, time and context verification available from the network. The user receives the BAN/PMH from their health care provider and, with their physician's staff, selects sharing options in additional an invariant 'personal data' privacy policy. The provider embeds the names and identity verification method for its application servers in the device's firmware. The application servers are informed of the patient's data names when the BAN/PMH is provided to the patient. When the BAN/PMH comes in contact with a mediator, it advertises its data and sharing policy, providing metadata such as its own location/time information ("UCLA Medical Plaza", "2006, 05, 08, 1321"), data type tag ("ECG"), data format tag ("beats/sec"), and unique id ("Patient X"). The mediator verifies the data source's identity through a certificate authority, logs the spacetime context, then registers the data name and its sharing policy. The PMB source sends data to its mediator, which expires there if no sinks exist. Asynchronously, the provider's application servers query the registry via their local mediator and, after authentication of identity, receive the patient's data. (Obeying the sharing policy, the registry 'cloaks', or does not resolve, the data names, unless the query comes from the health care provider's application servers, as verified by the certificate authority.) Via the network, this data is forwarded from a secure application server to a physician or caregiver, or logged for future diagnostic use. As this communication is also on the network, the application servers request, receive and log the *network-verified* location, time and authenticated identity of the physician's device for auditing/enforcement purposes.

With multi-tiered disclosure rules, a variety of clients can be served. Network-level resolution control of context minimizes intrusiveness of monitoring while still providing valuable environmental context. The patient could allow only summary statistics of their health metrics at low spatiotemporal resolution to be transmitted to family members. The healthcare provider might request and receive data at the highest available accuracy and sampling rate for internal logging, auditing and reporting. Several other challenges raised by this application are also well served by the proposed network architecture. Privacy protection and uninterrupted data delivery for a mobile patient is a key advantage; with the use of multiple mediators that can 'hand off' the source as it moves, the network can seamlessly route named data from the patient to the data sinks. Finally, the ability for the data owner to access network audit trails adds oversight to the dissemination process.

III.D.2. Participatory urban planning tool

Our urban-scale experimental validation will be the creation of a framework for opt-in participation in mapping city sound levels through cell phones, a rudimentary version of a **participatory urban planning tool**. The proposed network architecture lowers the complexity of creating trustable observing applications at the metropolitan scale, which will open a whole application space for participatory science, citizen journalism and urban planning. As we write this proposal, Los Angeles is preparing for a $1.8 billion redevelopment of a portion of its downtown, the Grand Avenue Project. [Grand06] USC's Norman Lear Center has embarked on the *Grand Avenue Intervention*, inviting citizen submission of design ideas for project's park component. They have received and published hundreds of such submissions. This driver application suggests how the network architecture will enable such organizations to initiate participatory sensing projects that similarly connect people (and their data) to the planning of their own environments. Oliveira et al. [Oliveira99] discuss a GIS-based noise planning tool created by public contractors for the city of Belo Horizonte in Brazil, noting that noise is a major source of nuisance and, for many, an important quality of life metric. They develop an approach that models it as a geo-field in a GIS system but do not address how real-world data might be gathered. Filling out this application idea, we will develop a simple service that

runs on a mobile phone platform, gathering and publishing basic statistics on ambient sound at regular intervals, and create a corresponding example web application to explore this data.

In our test scenario, an end-user downloads and installs sound measurement software on their mobile phone in order to participate. They configure simple sharing options to choose when and where samples are taken to calculate average sound amplitude, as well as the spatial and temporal resolution acceptable for network context tagging, providing choice/consent even for this anonymous data. Data dissemination of the average amplitude statistics follows the process described in previous sections, configured such that no identifying information is in the data name or data itself and no restrictions are placed on who can query and receive the data. At registration, the mobile application indicates that its data can be corroborated by other nearby data of the same type. For example, the device may sample for two minutes every half-hour and then publish the statistics for this sample. During registration, it indicates that its samples can be corroborated by other data of the same type captured at +/- one minute within one hundred feet, ensuring spatial and temporal overlap. Doing such corroboration at the network layer distributes processing and, more importantly, allows devices whose sharing policies do not allow data to be published above the trusted network layer to still corroborate the data of those who do. To enable this corroboration, the mediator caches other samples of this type of data for one minute. The web application provides a simple storage mechanism and GIS-based presentation of this data, drawing from CENS experience with both. This web application will allow the spacetime history of noise in the city to be explored at many resolutions. Many interesting visualization options would be possible beyond basic map-based one.

III.D.3. Presence-authenticated social data sharing system

For our third application, we consider **presence-authenticated social data sharing**. We will develop an image, sound and text sharing application, roughly a location-tagged *Flickr*, that explores how PSUS can facilitate rich experience and dialogue in places that are both *moved through* and *lived in*. This complements research in spatial tagging [Mark99] by using verifiable location and time spent in the location to authorize publishing about it. *Network verification of time spent in a place will be the sole method of authentication for documenting that place.* We envision a rich progression of responsibility enabled by the simple network primitives available. To use the web service on their mobile device, a person allows it access to their spacetime context information according to sharing rules of their choosing. As they move through their day, whenever they have enabled location context to be published, they 'accumulate' presence in places, as managed by this application. This accumulation could be implemented by a trusted application or a fabric-level service that aggregates time spent in areas without revealing patterns of activity to the application layer. In this service, through accumulation of time spent in a place, the user gains the capability to 'annotate' the place with media, anonymously, and the annotations may gain 'value' in the sharing environment. Gradually, the sharing rules allow trust to build and the user's capability in the social application is increased. Long-term familiarity with the place might open up moderation access. *Simply being there*, which is still an investment of one's *presence*, would allow read-only access to content that might not be freely published on the web. Through the proposed network architecture, all of this can be achieved without requiring identifying information or storage of timestamped location. Finally, through 'offline' address verification, those with legally recognized responsibility for a location could 'speak up' to the web service, define boundaries and even adjust the associated sharing rules.

This application illustrates how combining the capabilities of existing social applications with a new capacity to confirm presence can support the unique relationships and trust that emerge through time spent in proximity. Paulos and Goodman propose that mobile technology should explore the role of 'familiar strangers', whose recurring physical proximity (but not interaction) add comfort to crowded city lives. [Paulos04] Our similar forum that facilitates those who really spend time in places to gain the ability to document their experience may be a unique venue for building 'weak ties' for place-based communities themselves. 'Weak ties' between community members and those who come in contact with them are what bridge communities, providing exposure and access to resources.

(They are thus more important in building effectiveness than 'strong ties' internal to the community.) [Granovetter73] By using anonymized but verified presence to build trust and enable spatial tagging in this open but vetted community, this PSUS application suggests an important role that verifiable location and time may have in the creation of trusted social networking.

III.D.4. Application authoring

Application development will require authoring at three layers: (1) end-user data source applications, typically running on embedded/mobile devices, (2) web services that use the network architecture to build up commonly needed capabilities including storage and caching, search, streaming, aggregation and group sharing, (3) end-user sink applications, typically run on public or personal servers, but also on mobile devices. For our driver applications, we will approach web services development traditionally, using high-level languages with APIs created to expose network functionality. For the end-user source and sink applications, we'll consider the unique authoring requirements for applications using resolution-controlled, location-tagged data passing to and from physical devices, and the related challenge of exposing that functionality to developers with varying level of need/expertise for low-level coding. Previous experience of the PIs in creating authoring approaches for physical computing systems will be applied and extended. [Burke06, Mendelowitz05] Prototype toolsets created to facilitate application development will use a layered approach with traditional high-level languages, 'scripting' and graphical configuration. This will allow us not only to build the applications described below, but also to explore how key network capabilities can be expressed to and used by developers and end-users. In similar distributed, physical computing applications we have previously noted the need for *closeness of mapping to device parameters*, *rapid online modifications during development and testing*, and *tools for managing time and distributed state* [Mendelowitz05]. We've also noted that a fundamental *sense of space* and *sense of time* needs to be invested in devices for such pervasive computing applications. These features are available in the new network, along with notion of *data privacy, verifiable context,* and *resolution control*. New authoring tools should expose these device and network capabilities, and allow the developer to grasp the intrinsic notions of space, time, privacy and resolution control available. The current compile-run-and-download programming of embedded, data-driven applications will be complemented by approaches that use the streaming capabilities of the network to incorporate live data and network-supplied context in the development process. Existing privacy preference models, e.g., the W3C's Platform for Privacy Preferences (P3P) [P3P05] will serve as references for creating a sharing policy framework exposed to the end user and supported by the development tools.

III.D.5. Deployment platforms

Mobile and embedded data sources will be built using currently available platforms, some commercially available, and some developed within CENS. We envision two typical deployment configurations. The first configuration centers around Intel X-Scale based platforms such as HP iPAQ Pocket PCs, Crossbow Stargates, or the CENS Low Power Energy Aware Processing (LEAP) nodes [Ho06]. Internet connectivity will be through cell phone networks, like GPRS or 3G networks, or through wireless LAN. Sensors may be directly attached to the devices, such as microphones and imagers, and/or may anchor a cloud of wireless sensors. The second scenario involves programmable cell phones running Symbian OS or Linux. CENS is participating in Nokia's sensor plcanet effort, through which access to hardware and support on this class of mobile devices may be gained. Our focus will be on the software corresponding to our network architecture and the three driver applications. From a network perspective, we will start with a peer-to-peer overlay approach and do a deployment in the LA metro area. Over time, we will push things down deeper in the network and perhaps expand geographically if other deployments emerge at Berkeley or other FIND participants.

REFERENCES

[Allman05a] Mark Allman and Ethan Blanton, "Notes on Burst Mitigation for Transport Protocols," Computer Communication Review, 35(2), April 2005.

[Allman05b] Mark Allman, Ethan Blanton and Vern Paxson, "An Architecture for Developing Behavioral History," Proceedings of USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet, 2005.

[Altman75] Altman, I. 1975. The Environment and Social Behavior:Privacy, Personal Space, Territory and Crowding.Monterey, CA: Brooks/Cole Pub. Co., Inc.7.

[Altman77] Altman, I. 1977. Privacy Regulation: Culturally Universalor Culturally Specific? Journal of Social Issues, 33 (3),66-84.

[Blanton04] Ethan Blanton and Mark Allman, "Using TCP Duplicate Selective Acknowledgement (DSACKs) and Stream Control Transmission Protocol (SCTP) Duplicate Transmission Sequence Numbers (TSNs) to Detect Spurious Retransmissions," RFC 3708, 2004.

[Blanton05] Ethan Blanton and Mark Allman, "On the Impact of Bursting on TCP Performance," Passive and Active Measurement Workshop, 2005.

[Brands94] S. Brands and D. Chaum, "Distance-bounding protocols," in Workshop on the theory and application of cryptographic techniques on Advances in cryptology. Springer-Verlag New York, Inc., 1994, pp. 344–359.

[Burke06] J. Burke, J. Friedman, E. Mendelowitz, H.Park, M. B. Srivastava. "Embedding expression: Pervasive computing architecture for art and entertainment." Journal of Pervasive and Mobile Computing 2(1):1-36, 2006.

[Capkun05] S.Capkun, J.P. Hubaux, □"Secure positioning of wireless devices with application to sensor networks," □in Proceedings of IEEE INFOCOM 2005

[Capkun06a] S. Capkun, J. P. Hubaux, "Secure positioning in wireless networks," IEEE Journal on Selected Areas in Communications: Special Issue on Security in Wireless Ad Hoc Networks, February 2006.

[Capkun06b] S.Capkun, M. Cagalj, M. Srivastava, □Securing Localization With Hidden and Mobile Base Stations, □to appear in Proceedings of IEEE INFOCOM 2006.

[Casado05] Martin Casado, Tal Garfinkel, Weidong Cui, Vern Paxson and Stefan Savage, "Opportunistic Measurement: Extracting Insight from Spurious Traffic," ACM SIGCOMM HOTNETS, 2005.

[Chen03] A. Chen, R. Muntz, and M. B. Srivastava, "Self-aware actuation for fault repair in sensor networks," In "Smart Rooms" in Smart Environments: Technologies, Protocols and Applications (ed. Diane J. Cook and Sajal Das), John Wiley & Sons, Inc., 2003.

[Chen02] A. Chen, R.R. Muntz, S. Yuen, I. Locher, S.I. Park, and M.B. Srivastava, "A support infrastructure for the smart kindergarten," In Pervasive Computing, pages 49–57, 2002.

[Cui06a] Weidong Cui, Vern Paxson, Nicholas Weaver and Randy Katz, "Protocol-Independent Adaptive Replay of Application Dialog," NDSS, 2006.

[Cui06b] Weidong Cui, Vern Paxson and Nicholas Weaver, "GQ: Realizing a System to Catch Worms in a Quarter Million Places," 2006. In submission.

[DeVaul03] R. DeVaul et al., "MIThril 2003: Applications and Architecture," Proc. 7th Int'l Symp. Wearable Computers, IEEE Press, 2003, pp. 4-11; www.media.mit edu/wearables.

[Dharmapurikar05] Sarang Dharmapurikar and Vern Paxson, "Robust TCP Stream Reassembly in the Presence of Adversaries," USENIX Security Symposium, 2005.

[Dreger04a] H. Dreger, A. Feldmann, V. Paxson and R. Sommer, "Operational Experiences with High-Volume Network Intrusion Detection," ACM CCS, 2004.

[Dreger05] Holger Dreger, Christian Kreibich, Vern Paxson and Robin Sommer, "Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context," GI SIG SIDAR Conference on Detection of Intrusions and Malware and Vulnerability Assessment, 2005.

[Dreger06] Holger Dreger, Anja Feldmann, Michael Mai, Vern Paxson and Robin Sommer, "Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection," 2006. In submission.

[DeVaul03] R. DeVaul et al., "MIThril 2003: Applications and Architecture," Proc. 7th Int'l Symp. Wearable Computers, IEEE Press, 2003, pp. 4-11; www.media.mit edu/wearables.

[Eddy04a] Wesley Eddy, Shawn Ostermann and Mark Allman, "New Techniques for Making Transport Protocols Robust to Corruption-Based Loss," ACM Computer Communication Review, vol 34, no 5, 2004.

[Ganeriwal03] S. Ganeriwal, R. Kumar, M. B. Srivastava. Timing Sync Protocol for Sensor Networks. In Proceedings of the First ACM International Conference on Embedded Networked Sensor Systems (ACM SenSys), Los Angeles, CA, November 2003.

[Ganeriwal04a] Saurabh Ganeriwal, Aman Kansal, and Mani Srivastava, "Self-aware actuation for fault repair in sensor networks," In IEEE International Conference on Robotics and Automation (ICRA), 2004.

[Ganeriwal04b] Saurabh Ganeriwal and Mani Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), October 2004.

[Ganeriwal05] S. Ganeriwal, S. Capkun, S. Han, M. Srivastava, □"Secure Time Synchronization Service for Sensor Networks,"□in Proceedings of ACM Wireless Security Workshop (WiSe), 2005.

[Gonzalez03a] J. Gonzalez and V. Paxson, "pktd: A Packet Capture and Injection Daemon," Passive and Active Measurement Workshop, 2003.

[Gonzalez06a] Jose M. Gonzalez, Vern Paxson and Nicholas Weaver, "Shunting: A Hardware/Software Architecture for Flexible, High-Performance Network Intrusion Prevention," 2006. In submission.

[Gonzalez06b] Jose M. Gonzalez and Vern Paxson, "Enhancing Network Intrusion Detection With Integrated Sampling and Filtering," 2006. In submission.

[Govindan02] Ramesh Govindan and Vern Paxson, "Estimating Router ICMP Generation Delays," Proceedings of Passive and Active Measurement, 2002.

[Granovetter73] M. Granovetter. The Strength of Weak Ties. In American Journal of Sociology (1973), vol. 78, p. 1360-1380.

[Grand06] http://www.learcenter.org/html/projects/?cm=grand Accessed 2/28/06.

[Ho06] K. Ho D. McIntire, B. Yip, A. Singh, W. Wu, and W. J. Kaiser, "The low power energy aware processing (leap) embedded networked sensor system," Proceedings of ACM/IEEE IPSN (SPOTS Track), April 2006.

[Hochheiser02] Hochheiser, Harry. "The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context." ACM Trans. Internet Technology 2(4):276-306, November 2002.

[Huffman05] S.M. Huffman, and M.H.Reifer, "Method for geolocating logical network addresses," United States Patent 6947978, September 20, 2005.

[Ibarra99] Robert A. Ibarra, “Multicontextuality: A New Perspective on Minority Underrepresentation in SEM Academic Fields,” In Research News on Minority Graduate Education, Vol. 1, No. 3, October 1999.

[Jea05] David Jea, Arun Somasundara, and Mani Srivastava, “Multiple controlled mobile elements (data mules) for data collection in sensor networks,” In IEEE/ACM International Conference on Distributed Computing in Sensor Systems (DCOSS ’05), 2005.

[Jung04a] Jaeyeon Jung, Vern Paxson, Arthur W. Berger and Hari Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," IEEE Symposium on Security and Privacy, 2004.

[Jung06] Jaeyeon Jung and Rodolfo A. Milito and Vern Paxson, "On the Adaptive Real-Time Detection of Fast-Propagating Network Worms," 2006. In submission.

[Kannan05] Jayanthkumar Kannan, Jaeyeon Jung, Vern Paxson and Can Emre Koksal, "Detecting Hidden Causality in Network Connections," Technical Report, University of California, Berkeley, 2005.

[Kansal05]Aman Kansal and Mani Srivastava, “Energy harvesting aware power management,” In Book Chapter, in Wireless Sensor Networks: A Systems Perspective,Eds. N Bulusu and S Jha, Artech House, 2005.

[Kansal04a] Aman Kansal, Arun Somasundra, David Jea, Mani Srivastava, and Deborah Estrin, “Intelligent fluid infrastructure for embedded networks,” In ACM International Conference on Mobile Systems, Applications and Services (MobiSys), 2004.

[Kansal04b] Aman Kansal, Dunny Potter, and Mani Srivastava, “Performance aware tasking for environmentally powered sensor networks,” In ACM Joint International Computer Systems (SIGMETRICS), 2004.

[Kansal05] A. Kansal, J. Carwana, W.J. Kaiser and M.B. Srivastava, "Acquiring Medium Models for Sensing Performance Estimation," IEEE SECON, Sept 2005.

[Kohno05] Tadayoshi Kohno, Andre Broido, and K.C. Claffy, “Remote physical device fingerprinting,” IEEE Transactions on Dependable and Secure Computing, 2(2), 2005.

[Krishnan04a] Rajesh Krishnan, James Sterbenz, Wesley Eddy, Craig Partridge and Mark Allman, "Explicit Transport Error Notification (ETEN) for Error-Prone Wireless and Satellite Networks", Computer Networks,vol. 46, no. 3, 2004.

[Konstantas04] D. Konstantas, A.Halteren,R. Bults,K.Wac, I.Widya, N. Dokovsky, G. Koprinkov, V. Jones, and R. Herzog, “Mobile patient monitoring: the mobihealth system,” in Proc. Int. Conf. on Medical and Care Compunetics, NCC’04, 2004.

[Kornexl05] Stefan Kornexl, Vern Paxson, Holger Dreger, Anja Feldmann and Robin Sommer, "Building a Time Machine for Efficient Recording and Retrieval of High-Volume Network Traffic," ACM Internet Measurement Conference, 2005.

[Kreibich05a] Christian Kreibich, "Brooery: A Graphical Environment for Analysis of Security-Relevant Network Activity," FREENIX, 2005.

[Kreibich05b] Christian Kreibich and Robin Sommer, "Policy-controlled Event Management for Distributed Intrusion Detection," 4th International Workshop on Distributed Event-Based Systems, 2005.

[Kumar05] Abhishek Kumar, Vern Paxson, Nicholas Weaver, "Exploiting Underlying Structure for Detailed Reconstruction of an Internet-scale Event," ACM Internet Measurement Conference, 2005.

[Lazos05] Loukas Lazos and Radha Poovendran, SeRLoc: Robust Localization for Wireless Sensor Networks, ACM Transactions on Sensor Networks (TOSN), August 2005, Vol. 1, pp. 73 - 100.

[Malan04] D. Malan et al. CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. In Intl. Workshop on Wearable and Implantable BodySensor Networks, Apr. 2004.

[Mark99] Mark, W. "Turning pervasive computing into mediated spaces," IBM Systems Journal 38(4):677-692, 1999.

[Medina04a] Alberto Medina, Mark Allman and Sally Floyd, "Measuring Interactions Between Transport Protocols and Middleboxes," ACM SIGCOMM/USENIX Internet Measurement Conference, 2004.

[Medina04b] Alberto Medina, Mark Allman and Sally Floyd, "Measuring the Evolution of Transport Protocols in the Internet," 2004.Under submission.

[Mendelowitz05] E. Mendelowitz and J. Burke. "Kolo and Nebesko: A Distributed Media Control Framework for the Arts." First Intl. Conference on Distributed Frameworks for Multimedia Applications (DFMA '05), February 6-9, 2005, Besançon, France.

[Mills94] D. L. Mills, "Internet time synchronization: The Network Time Protocol" In Z. Yang and T.A. Marsland, editors, Global States and Time in Distributed Systems. IEEE Computer Society Press, 1994.

[Moore00] David S. Moore, George W. Cobb, "Statistics and Mathematics: Tension and Cooperation," In The American Mathematical Monthly, vol. 107, no. 7, pp. 615-630, August – September 2000.

[Moore03a] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, "The Spread of the Sapphire/Slammer Worm," 2003.

[Moore03b] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver, "Inside the Slammer Worm," IEEE Security and Privacy, vol. 1, no. 4, pp. 33-39, 2003.

[Nextel06] http://www.nextel.com/en/solutions/gps/telenavtrack.shtml Accessed 2/28/06.

[Ng04] Ng, J. W. P.; Lo, B. P. L.; Wells, O.; Sloman, M.; Toumazou, C.; Peters, N.; Darzi, A.; and Yang, G. Z. 2004. Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon). In International Conference on Ubiquitous Computing (Ubicomp).

[Oliveira99] Oliveira, M. P. G., E. B. Medeiros, and C. A. Davis Jr. "Planning the Acoustic Urban Environment: a GIS-Centered Approach." ACM GIS '99, Kansas City, MO, 128-133, November 1999.

[P3P05] W3C. "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Draft 1." July 2005, http://www.w3.org/TR/2005/WD-P3P11-20050701/, accessed February 26, 2006.

[Palen03] Palen, L. and Dourish, P. 2003. Unpacking "privacy" for a networked world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM Press, New York, NY, 129-136. DOI= http://doi.acm.org/10.1145/642611.642635

[Pang03a] Ruoming Pang and Vern Paxson, "A High-Level Programming Environment for Packet Trace Anonymization and Transformation," ACM SIGCOMM, 2003.

[Pang04a] Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson and Larry Peterson, "Characteristics of Internet Background Radiation," ACM Internet Measurement Conference, 2004.

[Park02] S. Park, I. Locher, and M. Srivastava, "Design of a wearable sensor badge for smart kindergarten," In Proocedings of the 6th International Symposium on Wearable Computers (ISWC2002), Seattle, WA, October 2002.

[Paulos04] E. Paulos and E. Goodman. "The Familiar Stranger: Anxiety, Comfort, and Play in Public Places." In Proceedings of CHI 2004, Vienna, Austria. 2004.

[Paxson00a] Vern Paxson, Andrew Adams and Matt Mathis, "Experiences with NIMI," Proceedings of Passive and Active Measurement, 2000.

[Paxson04a] Vern Paxson, "Strategies for Sound Internet Measurement," ACM SIGCOMM Internet Measurement Conference, 2004.

[Paxson98d] Vern Paxson, Jamshid Mahdavi, Andrew Adams and Matt Mathis, "An Architecture for Large-Scale Internet Measurement," IEEE Communications, 1998.

[Raghunathan05] Vijay Raghunathan, Aman Kansal, Jason Hsu, Jonathan Friedman, and Mani B Srivastava, "Design consideraions for solar energy harvesting wireless embedded systems," In IEEE International Symposium on Information Processing in Sensor Networks (IPSN), 2005.

[Savvides04a] A. Savvides, M. B. Srivastava, L. Girod, and D. Estrin, "Localization in Sensor Networks," in Wireless Sensor Networks (ed. C. S. Raghavendra, K. M. Sivalingam, and T. F. Znati), Kluwer Academic Publishers, April 2004.

[Savvides04b] A. Savvides and M. B. Srivastava, "A self-configuring location discovery systems for smart environments," In Advances in Pervasing Computing and Networking (ed. B. Szymanski and B. Yener), Kluwer Academic Publishers, 2004.

[Somasundra04] Arun Somasundra, Aditya Ramamoorthy, and Mani Srivastava, "Mobile element scheduling for efficient data collection in wireless sensor networks with dynamic deadlines," In IEEE Real Time Systems Symposium, 2004.

[Somasundra05] Arun A Somasundara, Aman Kansal, David Jea, Deborah Estrin, and Mani B Srivastava, "Controllably mobile infrastructure for low energy embedded networks." Accepted in IEEE Transactions on Mobile Computing, 2005.

[Sommer05] Robin Sommer and Vern Paxson, "Exploiting Independent State For Network Intrusion Detection," ACSAC, 2005.

[Srivastava01] Mani Srivastava, Richard Muntz, and Miodrag Potkonjak, "Smart kindergarten: Sensor-based wireless networks for smart developmental problem-solving environments," In Proceedings of the ACM SIGMOBILE 7th Annual International Conference on Mobile Computing and Networking (Mobicom), Rome, Italy, 2001.

[Staniford04] Stuart Staniford, David Moore, Vern Paxson and Nicholas Weaver, "The Top Speed of Flash Worms," ACM CCS WORM, 2004.

[Steurer03] P. Steurer and M.B. Srivastava, "System design of smart table," In Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom 2003), 2003.

[Vasu05] B. Vasu, M. Varshney, R. Rengaswamy, M. Marina, A. Dixit, P. Aghera, M. Srivastava, and R. Bagrodia, "sQualNET – A Scalable Simulation Framework for Sensor Networks." ACM Sensys, 2005.

[Weaver03a] Nicholas Weaver, Vern Paxson, Stuart Staniford and Robert Cunningham, "Large Scale Malicious Code: A Research Agenda," 2003. DARPA-sponsored report.

[Weaver03b] Nicholas Weaver, Vern Paxson, Stuart Staniford, Robert Cunningham, "A Taxonomy of Computer Worms," First ACM CCS Workshop on Rapid Malcode (WORM), 2003.

[Weaver04a] Nicholas Weaver, Ihab Hamadeh, George Kesidis and Vern Paxson, "Preliminary Results Using ScaleDown to Explore Worm Dynamics," ACM CCS WORM, 2004.

[Weaver04b] Nicholas Weaver, Stuart Staniford and Vern Paxson, "Very Fast Containment of Scanning Worms," USENIX Security Symposium, 2004.

[Weaver04c] Nicholas Weaver, Dan Ellis, Stuart Staniford and Vern Paxson, "Worms vs. Perimeters: The Case for Hard-LANs," Hot Interconnects 12, 2004.

[Weaver04d] Nicholas Weaver and Vern Paxson, "A Worst-Case Worm," Third Annual Workshop on Economics and Information Security (WEIS04), 2004.

[Yegneswaran05] Vinod Yegneswaran, Paul Barford and Vern Paxson, "Using Honeynets for Internet Situational Awareness," ACM SIGCOMM HOTNETS, 2005.