Smart Community: An Internet of Things Application

Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, University of Waterloo
Jiming Chen, Zhejiang University
Xiaodong Lin, University of Ontario Institute of Technology

ABSTRACT

In this article, we introduce an Internet of Things application, *smart community*, which refers to a paradigmatic class of cyber-physical systems with cooperating objects (i.e., networked smart homes). We then define the smart community architecture, and describe how to realize secure and robust networking among individual homes. We present two smart community applications, *Neighborhood Watch* and *Pervasive Healthcare*, with supporting techniques and associated challenges, and envision a few value-added smart community services.

INTRODUCTION

The Internet of Things (IoT) is an emerging concept referring to networked everyday objects that interconnect to each other via wireless sensors attached to them. *Smart homes* are an appealing IoT practice. It pushes forward a future home environment where embedded sensors and actuators (e.g., in consumer electronic products and systems) are self-configured and can be controlled remotely through the Internet, enabling a variety of monitoring and control applications. These devices sense and record user activities, predict their future behavior, and prepare everything one step ahead according to the user's preference or needs, giving him/her the most convenience, comfort, efficiency, and security. Extensive research efforts have been made to develop various smart home systems [1]; commercialization (e.g., www.smarthome.com, www.smarthomesystems.com) has also been observed. These research and development activities focus on individual homes.

We propel the smart home concept to a further extent and introduce the notion of the *smart community*. A smart community is a multihop network of smart homes that are interconnected through radio frequency following wireless communication standards such as WiFi (IEEE 802.11) and the third generation (3G) of mobile telephony. It can be viewed as a cyber-physical system, in which homes are virtually multifunction sensors with individual needs, continuously monitoring the community environment from various aspects; and, when necessary, automatic or human-controlled physical feedback is input to improve community safety, home security, healthcare quality, and emergency response abilities. As elaborated later in this article, the realization of a smart community requires sophisticated supporting techniques, and there are many associated technical challenges to be tackled. With ever advancing wireless communication and ubiquitous sensing technologies, we envision a proliferation of smart communities in the future.

THE SMART COMMUNITY ARCHITECTURE

A smart community is a virtual environment composed of networked smart homes located in a local geographic region. It is formed upon the agreement of participating homeowners, with respect to local geographic, terrain, and zoning features. For example, enclave homes should participate in the community of surrounding homes rather than become a separate one; isolated (e.g., by major streets) homes should not belong to the same community. Architecturally, a smart community consists of three domains: the home domain, community domain, and service domain, as shown in Fig. 1.

HOME DOMAIN

In this domain, a home network is formed by a number of home automation systems (e.g., healthcare systems and security systems) for continuous real-time monitoring of residents, the home environment, and the nearby community environment (e.g., the street segments beside a house). These systems report their surveillance results to a *home gateway* inside the home in a single-hop or multihop way. The connection may be realized by powerline communication technologies such as HomePlug (www.homeplug.org), wireless communication technologies like Bluetooth, phone line communication technologies such as HomePNA (www.homepna.org), or other technologies such as Ethernet that require dedicated wiring. The gateway is the home's communication interface with the outside world.

0163-6804/11/$25.00 © 2011 IEEE

It is able to intelligently process and manage gathered surveillance data, provide efficient paths for forwarding them to other homes or the remote *community center* in the community domain via wireless networks, and/or enable immediate contact with the call center in the service domain for response.

Community Domain

The core of the smart community architecture is the community domain, where a connected community network is formed by home gateways (representing their hosting homes) for cooperative and distributed monitoring of the community environment and information dissemination among individual homes. A reliable tamper-proof wireless device, called a community center, is placed in the network for data storage and processing. It is guarded by advanced sensor technologies and protected by defensive layers; unauthorized access will trigger alarms, notifying community residences and authorities. Home gateways and the community center are connected wirelessly using WiFi links in a multihop manner. In case of communication failure, 3G cellular networks can be used for bridging individual homes and the community center. Data stored on the community center can be personal, sensitive, and confidential. For home privacy, they are selectively accessible, only to authorized parties as needed; remote access may not be permitted, subject to the community residents' collective decision.

Service Domain

The key component of this domain is a *call center*, which is a communication and computation device hosted by a trusted party like the local police department. It receives service calls from the community domain by being connected to individual homes (the corresponding home gateways) and dispatches them to proper authorities or service providers, through a reliable communication channel such as the public telephone system or television cable system. It is connected to the community center as well, and thus able to provide value-added data gathering services for a variety of smart community applications related to municipal affairs, such as election and voting or utility management, such as accounting and billing. It is possible that the service domain is shared by multiple communities that are close to each other.

Secure and Robust Community Networking

In the smart community architecture, the home domain emphasizes intra-home networking, which deals with how to interconnect smart appliances, home automation systems, security systems, and other applications in a smart home environment. This problem has been extensively studied in the literature [1]. Here we focus on the new inter-home (community) networking issue in the community domain, raised by the smart community concept. To simplify the presentation, we use the terms *node*, *home gateway*, and *smart home* (or *home*) interchangeably.

Notice that the community network is a classic wireless ad hoc network. We have considered WiFi technologies at the medium access control (MAC) layer. TCP [2] is a natural choice at the transport layer since it provides reliable congestion control and has become the de facto standard in most applications. According to [3], plain WiFi protocols do not work well with TCP in wireless ad hoc networks due to the hidden terminal and exposed terminal problems. Effort has been made to improve the protocol performance [4], and bandwidth management is further suggested to ensure satisfactory quality of service [5]. While considerable research has covered the issues at the MAC and transport layers, we study the network-layer routing problem (i.e., selecting multihop paths for sending network traffic between homes).

Although there are significant research efforts on distributed wireless ad hoc routing [6] in large-scale or mobility-rich networks, we notice the limited scale and static nature of the community network. In such a network, it is feasible and realistic to pre-load each home gateway with a global view of the network topology. Routing can thus be performed at the source in a centralized and straightforward way. Nevertheless, it is not trivial to ensure secure and robust data communication, due to the openness and unreliable nature of the wireless communication media.

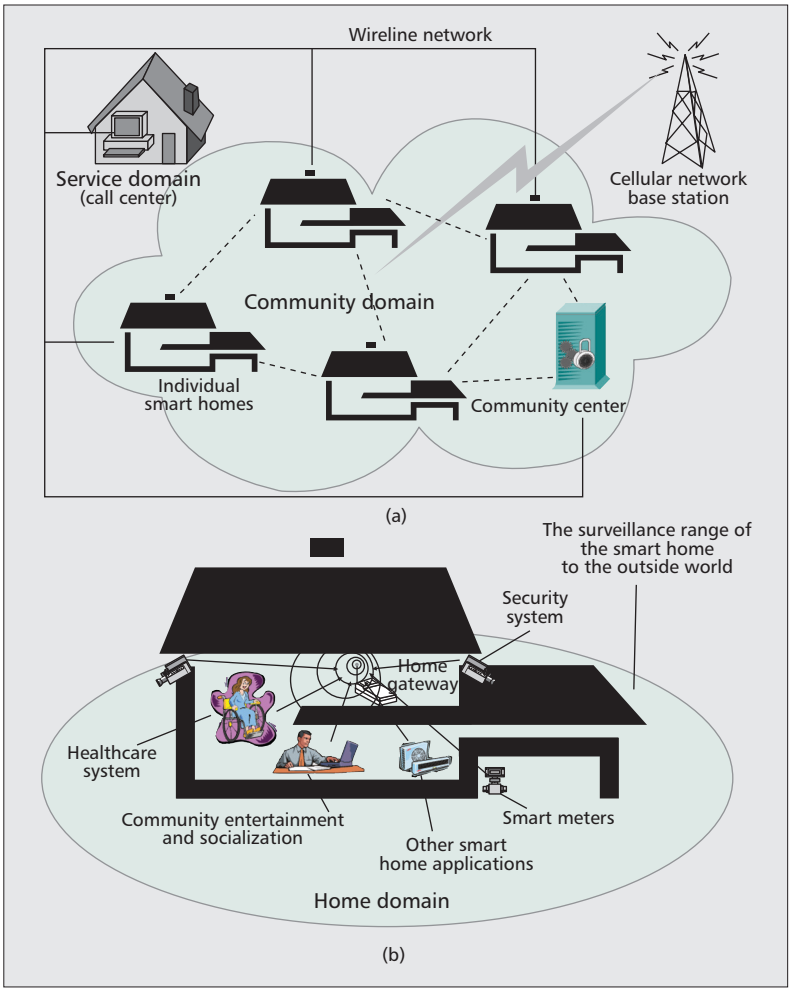

Figure 1. *The smart community architecture: a) community and service domains; b) home domain.*

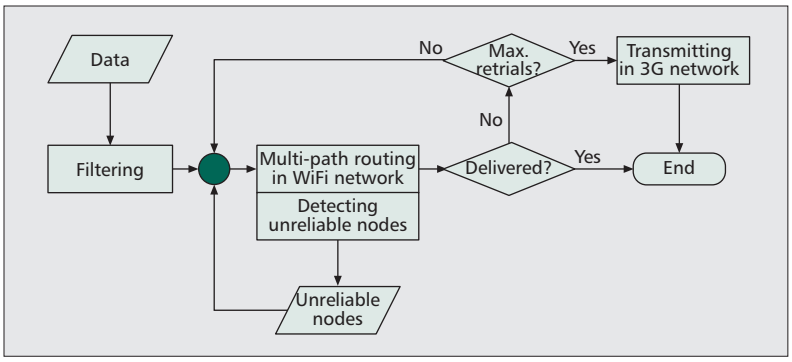

Figure 2. *The flow chart of smart community communication.*

Security and Reliability Requirements

There are five basic security requirements: data confidentiality, integrity, authenticity, non-repudiation, and access control. The network traffic in a smart community must be protected to meet the first four requirements. The last requirement may be satisfied optionally according to the traffic type. Community network traffic may be classified as private or public. The content of both types of traffic is protected from being read by people outside of the community. Private traffic, such as personal health information, is originated for the benefit of individual homes. Its content should not be disclosed to other community residents. Public traffic, such as safety warnings, is for the collective benefit of the entire community. It is thus open to all community members.

Some basic security mechanisms may be sufficient for securing data communication in the community network. For example, asymmetric keys can be assigned to each home gateway by the service provider that offers smart community services. They are used for authentication and negotiating symmetric session keys for data communication, and they can be updated on a periodic basis. Since each home gateway is normally a powerful device like a wireless access point, cryptography may be applied as needed during data communication so as to meet the above mentioned security requirements. When representing its members, a home appears to have social needs. If an adversary observer finds that a home often communicates with a particular home, it may correctly guess the source home's communication purpose with a high probability based on the public information of the social role of the destination home, even if the communication content is hidden by cryptography.

To handle this home privacy concern, the source home may deliberately include some trustworthy homes in the data communication path as relay nodes. As suggested in [7], these trusted nodes can employ a re-encryption algorithm to re-randomize the received cipher text. Such an algorithm does not affect the decryption capability of the destination, but disables the observer from linking the input and output data streams by simply comparing data packets. Furthermore , they can cut off the relation between the input and output data streams by a mix technique. If n input packets are randomly mapped to n output ones, the probability of an adversary's correctly guessing the link relation between source and destination is only $1/n$.

In case there is no trustworthy home in the community, the source home may apply classic layered encryption technique to establish an anonymous route to the destination. The idea is to assign a session key to every hop along the route and encrypt each data packet in layers, using theses keys in accordance with the order of the hops in the route. Intermediate nodes are informed by the source about the session keys of their incidental hops through a route establishment phase. They peel off one encryption layer from a received data packet and retransmit the packet to all the nodes in its communication range including the next hop. The destination removes the last encryption layer and obtains the original data packet. In this way, home privacy can be preserved since no intermediate node is aware of the source, the destination, or even other intermediate nodes.

A home gateway is considered *unreliable* if it either fails to forward messages or transmits incorrect messages. Having unreliable gateways in the community network may increase communication delay and cause bandwidth waste, data loss, and communication failure. The reasons for a home gateway to appear unreliable are multifold: error-prone wireless media, software faults and hardware defects. Network attacks also contribute to home gateway unreliability. An adversary may occupy the wireless channel by overwhelming frequencies of illegitimate traffic so that legitimate traffic is jammed. It may compromise several home gateways, access all keying materials stored on them, and then control them to disseminate bogus data to the community and/or the service center, degrading the fidelity of the propagated information and leading to erratic upper-level decisions. Reliable communication is expected in the presence of unreliable home gateways.

Security and Reliability Improvement Techniques

The flow chart of home-to-community-center data communication is shown in Fig. 2. The blocks of filtering and unreliable node detection, and the use of 3G networks are the main techniques for improving security and reliability. Below we introduce the most recent solution techniques. A review of other possible solutions can be found in [8, 9].

Filtering False Network Traffic — It is impossible to detect within the community false private data due to their intrinsic non-public nature. Detection is possible only after a response is triggered as the response normally involves human intervention and/or cross-verification by authorized parties. Henceforth, we focus on how to filter false public data. Public data concern the interests of the community. They are fused and processed at the community center. By checking data consistency, the community center is able to detect false public data and remove them from consideration.

More specifically, according to data type and other associated attributes such as location and

time, the community center asks the entire community for relevant data (if they are not locally available yet), and computes the distance between the data to be verified and the centroid of the replies received. The target data is false if the distance is beyond a threshold value, which is normally given as a system input. This centralized technique, however, allows false data to be propagated in the community, wasting precious bandwidth of en route nodes; it additionally puts all the verification burden on the community center, thus making it vulnerable to denial of service (DoS) attacks. Early detection and filtering is highly desired.

Lu *et al.* [8] recently proposed a cooperative authentication scheme to prevent false data from propagating in the network. In this scheme, source node S informs its k-hop neighborhood N_S^k about the data X to be propagated and the complete routing path P to be used. Each node in N_S^k uses an elliptic curve cryptography (ECC)-based non-interactive keypair establishment method to compute shared keys with all nodes in P. It generates message authentication codes (MACs) for these en route nodes using these keys if it agrees on X, or randomly otherwise. S collects MACs from N_S^k and transmits them together with X along P. Each node in P generates the shared keys with N_S^k similarly and verifies the received MACs intended for it. It decides whether to retransmit according to the verification result and a locally selected vote threshold L.

Avoiding Unreliable Home Gateways — It is important to identify unreliable home gateways so that they can be avoided in routing and quickly reconfigured/repaired by the homeowners. As data integrity is achieved by cryptographic techniques, this actually boils down to the classic packet drop attack (black/gray hole) detection problem. A recently proposed side channel monitoring (SCM) technique [9] can be adopted to handle this problem at minimal cost.

SCM is a localized scheme with no requirement for any additional trusted device (thus no additional monetary investment). The principle is to select a subset of neighbors for each node along a routing path as observers to monitor its message forwarding behavior and report observed misbehavior to the source. The backward route is a directional primary communication channel to the source; observer nodes constitute a side channel, also toward the source. The two channels are both used for misbehavior reporting. Due to collusion among attackers and topological disconnectivity of the two channels, misbehavior reports may possibly not be delivered successfully, leading to detection failure. It has been shown that SCM has a high detection rate.

After a node detects an unreliable home gateway, it reports this to the community center. Each node intends to use the most reliable home gateways and avoid using frequently detected unreliable ones. Since detection is not guaranteed, to further mitigate unreliable home gateways and increase data delivery probability, multipath routing may be engaged. The community center gathers the misbehavior reports about each home gateway. When the number of reports is beyond a certain threshold, it notifies the corresponding homeowners by other means such as an automatic telephone call. The homeowner is responsible for investigating and fixing the problem quickly and reporting the repair to the community center, which then informs the entire community so that those home gateways can be reused for routing.

When unreliable gateways appear massively, the network can be partitioned, and multipath routing may fail. To ensure the functionality of the smart community in this extreme situation, a source may switch from using the WiFi-based community network to using the relatively reliable and ubiquitously available 3G cellular network for data communication. Because the 3G network is normally not a free resource, it is the home owners' decision whether to use it or not and in which situations to use it. Besides, the switch is not made immediately, but after a few retrials of using the community network.

Smart Community Applications

The smart community platform can support many applications. We elaborate on two major applications, Neighborhood Watch and Pervasive Healthcare, which improve community safety, home security, healthcare quality, and emergency response abilities. We also briefly introduce several value-added services, including smart metering for utility management, and social networking for convenience and entertainment.

Neighborhood Watch

Neighborhood Watch is a traditional program in North America. Similar systems exist in Europe. They are usually implemented as a function of a community association, involving a group of residents devoted to crime and vandalism prevention within a neighborhood. When suspicious activities occur, members contact authorities rather than intervene. Due to unavailability, tiredness, distraction, and limited perception, human-dominated neighborhood watches are inconsistent and of limited effectiveness. The smart community environment provides a perfect platform to implement unattended and pervasive always-on neighborhood watches, saving human resources and increasing effectiveness and efficiency.

Individual homes are equipped with surveillance cameras. These cameras continuously monitor the surroundings of their corresponding homes, including not only the homes' yards but also nearby road/street segments. As such, homes can be abstracted as computationally capable sensors with limited sensing range, and the community network is therefore a wireless sensor network covering the geographic region of the community. Homes cooperatively and distributedly detect suspicious events, and decide whether a detected event is a safety threat; when necessary, they inform other community members within the event interference range and/or contact the call center. Meanwhile, they report the event to the community center, where all the event reports are gathered and analyzed. The

Neighborhood Watch is a traditional program in North America. Similar systems exist in Europe. They are usually implemented as a function of a community association, involving a group of residents devoted to crime and vandalism prevention within a neighborhood.

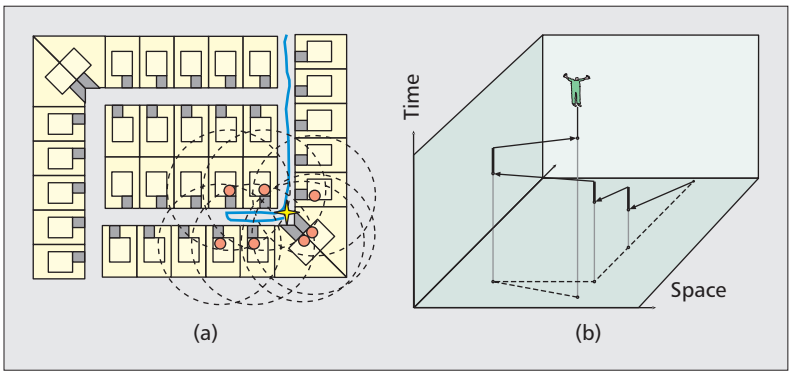

Figure 3. *Suspicious event detection in neighborhood watch: a) a cluster of smart homes, marked by small dots and surrounded by circles indicating their surveillance range, are tracking a suspicious event, represented by a star; b) the event movement trace identified by the community surveillance network is a multi-stage curve of space-time points. The contour line on the space plane in (b) corresponds to the physical path of the event, which is the blue line in (a).*

community center determines the correlation of received event reports (data) by statistical approaches. If, together, they indicate a community-wide threat, it sends alarms to all the homes in the community as well as contact the call center. The call center dispatches received service calls to appropriate authorities so that proper actions or feedback can be taken/provided. We would like to indicate that the monitoring objects of neighborhood watches are events happening in the public space. Other events take place on private property and are taken care of by individual home security systems.

Events such as fires and earthquakes may be simple and static (or slowly varying), and can be identified directly from sensor readings. Events may also be complex and mobile, such as a school bus going through the community in the morning or an unknown car wandering around the community at midnight. These mobile events have spatial and temporal properties. While detecting suspicious static events may be easy, detecting suspicious mobile events requires sophisticated detection techniques. In order to decide whether a mobile event is suspicious and make the decision in real time, we need to track the event. Consider an event, also called a target, as a dynamic system whose state describes the location (possibly as well as velocity) of the target and evolves over time. Tracking can be formulated as obtaining an estimate of target state from a (state) measurement history. Depending on the number of targets, there are single-target tracking and multitarget tracking. Generally speaking, target tracking, whether single or multi, can be performed by sequential Bayesian filtering [10]. The more targets to track, the more complex the state space and observation space, and therefore the more computational power is needed. Multitarget tracking is relatively difficult due to unknown association between the observations and the targets in the presence of noise, clutter, and potentially missed detections [11]. But it is practically desirable because there are usually different targets (e.g., people and vehicles) at the same time in a community environment.

Teng *et al.* [12] presented a cluster-based single-target tracking algorithm using variational filtering — an implementation of Bayesian filtering — for sensor networks. The network is clustered, and clusters are activated in turn so that at any measurement time there is only one cluster of sensors (i.e., individual homes) responsible for sensing and tracking. The head of an active cluster collects sensory data from its cluster members, predicts the mobility of the target by variational filtering, and activates the most appropriate cluster for subsequent tracking. In order to generate enough information for tracking the target, at least three cluster members need to detect the target and report their observations. Cluster activation is based on predicated target position and tendency. If the predicated position is within the current cluster, no efforts will be made; otherwise, the current cluster head will activate, and pass all necessary tracking data to an adjacent cluster to take over the tracking process while deactivating its own cluster. Activation is in favor of a cluster to which the predicted target position is the closest and the target is moving. As a result, clusters along the target's movement trace are activated in sequence, and the target is captured all the time. Figure 3 illustrates suspicious event detection by this algorithm in the Neighborhood Watch scenario. This tracking method requires only local computation within the currently active cluster, and is thus efficient in terms of communication and computation. The cluster-based framework of this algorithm may be extended to support efficient multitarget tracking.

Pervasive Healthcare

Healthcare applications developed in a smart community decrease the community residents' dependence on special caregivers and reduces their healthcare expenses through more efficient use of community healthcare resources and earlier detection of life-threatening emergency situations. To make an accurate and quick emergency response, the applications rely on continuous monitoring of the environmental conditions and the body status of community residents provided by wireless body sensors deployed around the human body. The smart community environment then provides a seamless wireless connection from every location within the community at which the residents reside to nearby healthcare givers living in the same community and remote healthcare institutes.

In a smart community environment, elders and people with cognitive/physical disabilities receive healthcare services any time for any event, and little children and babies are cared for in a more secure way while their parents are not nearby. When an emergency occurs, being detected/reported by body sensors, home surveillance systems, or an onlooking passerby, the emergency information and other relevant data such as body sensor readings and personal health information (PHI) are instantly sent through the community network to nearby healthcare workers who are able to offer the most proper first aid, and service calls are

made in the meantime to healthcare institutes whose professionals will immediately come to the scene and provide advanced emergency measures.

In healthcare applications, residents' PHI is transmitted in the community network, exposed to unauthorized collection, disclosure, or other inappropriate use, and constituting privacy threats to those residents. One privacy concern is about the sensitive and confidential nature of PHI. Another concern is, if an observer knows that a resident often sends his/her PHI to a particular healthcare worker, then based on the medical treatment domain of the healthcare worker, the observer can correctly guess that resident's disease with a high probability. These concerns can be resolved by cryptography, packet re-encryption, and mix techniques, as discussed previously.

The healthcare applications also need fine-grained access control for privacy-sensitive data. The access control must be user-centric. That is, residents must be able to select the access policy for their own personal information and apply distinct access policies in different situations. For example, in a normal situation they may only send their data to the remote trusted authority; whereas in a life-threatening scenario they may want to disseminate the data quickly while exposing as little personal information as possible to the public. This trade-off between safety, privacy, and access control in different contextual cases is shown in Fig. 4. Recent research efforts [13] have been devoted to attribute-based encryption (ABE) schemes for fine-grained access control without a lengthy user authorization process. Such schemes associate cipher text with an access tree, where each leaf node represents an attribute (or access role), and each non-leaf node represents a threshold value. If we treat each attribute as a binary variable (either 0 or 1), the access tree can be semantically transformed to a Boolean function, which can be used for controlling access to patient data.

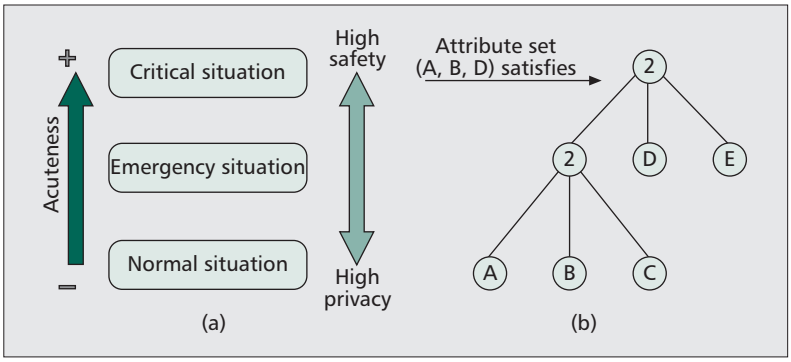

Figure 4. *Access control in pervasive healthcare: a) trade-off of safety, privacy, and access control; b) an access tree consisting of two threshold gates both valued by 2, and five attributes, A, B, C, D, and E. An attribute set (A, B, D) satisfies the access tree.*

Value-Added Services

Utility Management — The smart community environment can facilitate measurement of utility consumption of individual homes. Traditional automated meters have to be read individually by metering personnel from utility companies. In smart community, each home is equipped with smart meters that report their readings to the home gateway, which in turn forward the data to the community center through the community network in a secure and privacy-preserving way. Here privacy preservation is important because the utility usage information may reveal household actives. The community center maintains an account storing detailed utility usage information for each household. It periodically transmits the data to the call center, which then forwards them to the utility companies for computerized billing. Because no direct human intervention is involved in the utility management process, operational cost is reduced at the utility company side. At the consumer side, home privacy and security is improved since no metering personnel enter their houses.

Social Networking — The smart community environment also provides a social network platform. It is convenient and cost-free for residents to utilize the community network to interact with other people in the local region. Because of the geographic proximity, this kind of social network would be more useful than Internet-based ones in many cases. For instance, babysitting is an important community activity, which refers to the practice of temporarily caring for a child on behalf of the child's parents. With the social network platform established in a smart community, parents may easily find a convenient and trustworthy babysitter nearby. Online gaming is a popular leisure activity, which has had an exponential increase in recent years. The advanced community technologies in the smart community make the development and creation of low-cost online gaming possible. It is expected that residents can conveniently play online games with their peers in the same community and do not rely on the public gaming service and the Internet. As a result, there is no or very little associated monetary cost.

Research Challenges

As the smart community belongs to the broad field of wireless communications and networking, it inherits a variety of fundamental problems such as transmission control [2], media access control [3, 4], bandwidth allocation [5], and routing [6]. These problems have been investigated extensively in literature. Given the limited space here, we address only the key issues related to the previously introduced community networking techniques and novel applications.

Networking Challenges

Cooperative Authentication — Previously, when introducing security and reliability improvement techniques for community networking, we presented a cooperative authentication scheme for filtering false data traffic in community network [8]. It is a voting scheme within a k-hop neighborhood, governed by a vote threshold L. Normally, only nodes within an event's interference range are able to sense the event and thus be eligible to vote for each other's surveillance data about the event. Let T be the

Grounded on wireless communications and networking technologies, smart community networks the smart homes in a local community environment and enables a variety of useful and promising services such as neighborhood watch and pervasive healthcare.

number of such eligible voters in a k-hop neighborhood. In a smart community, homes are sparsely located (when houses are separated by a reasonable distance, e.g., a few meters, home-used WiFi signal can cover only a few homes in vicinity); thus, T is usually small unless k is set to be large. Voting results may not reflect the truth if T is small or $T < L$. In order to increase voting effectiveness, both k and L should be dynamically and adaptively selected according to the event range, rather than blindly defined beforehand. Before the voting process, certain collaboration is then needed among sensors for estimating the event range according to their measurements and properly determining the values of these two key parameters. The source node should not make the selection, and the associated communication cost should not offset the savings gained from traffic filtering. The challenge is how to ensure such collaboration under these requirements.

Detecting Unreliable Nodes — We also suggested adopting SCM [9] for detecting unreliable nodes (home gateways) in the community network and eventually avoiding using them during data communication. This scheme relies on neighboring nodes passively listening to each other's retransmission and does not provide detection guarantee. To improve its performance, acknowledgment packets can be used between successive intermediate nodes, and/or between source and destination to verify packet receipt. It is necessary to apply cryptographic techniques on both data packets and acknowledgment packets in order to enable trustworthy and effective verification. It is a challenging open research problem to find lightweight localized unreliable-node detection techniques without using extra hardware and with detection guarantee. Solutions should increase community network reliability, decrease the frequency of using paid 3G cellular networks, and reduce associated monetary expense.

Application Challenges

Target Tracking and Intrusion Detection — For Neighborhood Watch, existing target tracking algorithms including [12] are not designed for smart community environments, where the movement of a target is restricted within community streets/roads. This constraint actually simplifies the problem. It may be exploited to design new efficient data association algorithms and tracking algorithms. With collected event data by the tracking algorithm used, we need to classify the event as either normal or suspicious. This classification involves two challenging tasks: one is to define suspicious mobility patterns; the other is to compare a detected event mobility pattern with the defined malicious patterns and try to find a match. The first task has to be fulfilled offline in advance, before event data collection. It requires analysis and study (through data mining approaches) of historical data from communities where crime and vandalism have occurred, with support from the fields of humanology, sociology, psychology, and criminology. The defined patterns need to be represented and organized in a proper and efficient way for computerized usage. The second task is an analog of network intrusion detection. It has to be done quickly and carefully. Simple direct comparison is not sufficient since a match is not necessarily exact and may be contextual. Some intrusion detection techniques [14] may be borrowed to help resolve this problem. An intelligent context-aware matching algorithm is eventually desired to avoid or minimize both false positives and false negatives.

ABE with Hidden Access Policies — For Pervasive Healthcare, fine-grained access control [13] is applied so as to satisfy community members contextual customized privacy needs. As access control becomes fine-grained, the access policy may contain quite a bit privacy-sensitive information. Improper design and disclosure of the policy would enable partial information of the communicating parties to attackers, and thus violating user privacy. Consider a patient who wishes to share personal information for emergency use with healthcare givers who live in his/her community and satisfy a certain access policy. This policy, however, can possibly reveal confidential information such as diseases, symptoms, or other attributes of the patient. In this case, the patient will seek qualified healthcare givers by transmitting a message, encrypted with the ABE scheme and hiding the access policy in the cipher text, within the community network. Without knowing the policy, a receiver is not able to identify itself as a qualified candidate unless it tries every possibility. The brute-force approach is time- and computation- consuming, and obviously not a practical solution. Finding efficient ABE schemes based on hidden access policies can be a future research direction for delivering pervasive healthcare in smart community environments.

Conclusions

In this article, we have introduced the smart community as a new application of the Internet of Things. Grounded in wireless communications and networking technologies, a smart community networks the smart homes in a local community environment, and enables a variety of useful and promising services such as neighborhood watch and pervasive healthcare. It opens a new research direction with many unique challenging issues.

References

[1] S. Dixit and R. Prasad, *Technologies for Home Networking*, Wiley, 2008.
[2] Y. Tian, K. Xu, and N. Ansari, "TCP in Wireless Environments: Problems and Solutions," *IEEE Commun. Mag.*, vol. 43, no. 3, pp. S27–S32, Mar. 2005.
[3] T. Saadawi and S. Xu, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Commun. Mag.*, vol. 36, no. 6, June 2001, pp. 130–37.
[4] H. Shan, W. Zhuang, and Z. Wang, "Distributed Cooperative MAC for Multihop Wireless Networks," *IEEE Commun. Mag.*, vol. 47, no. 2, Feb. 2009, pp. 126–33.
[5] X. Su, S. Chan, and J. H. Manton, "Bandwidth Allocation in Wireless Ad Hoc Networks: Challenges and Prospects," *IEEE Commun. Mag.*, vol. 48, no. 1, Jan. 2010, pp. 80–85.

[6] I. Stojmenovic, A. Nayak, and J. Kuruvila, "Design Guidelines for Routing Protocols in Ad Hoc and Sensor Networks wth A Realistic Physical Layer," *IEEE Commun. Mag.*, vol. 43, no. 3, Mar. 2005, pp. 101–06.
[7] X. Lin *et al.*, "SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems," *IEEE JSAC*, vol. 27, no. 4, 2009, pp. 365–78.
[8] R. Lu *et al.*, "BECAN: A Bandwidth- Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks," *IEEE Trans. Parallel and Distrib. Sys.*, to appear, 2011.
[9] X. Li *et al.*, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks," *Proc. IEEE ICC '11*, 2011.
[10] J. Liu, M. Chu, and J. E. Reich, "Multitarget Tracking in Distributed Sensor Networks," *IEEE Sig. Proc. Mag.*, vol. 24, no. 3, 2007, pp. 36–46.
[11] G.W. Pulford and B.F. La Scala, "Multihypothesis Viterbi Data Association: Algorithm Development and Assessment," *IEEE Trans. Aerospace and Elect. Sys.*, vol. 46, no. 2, 2010, pp. 583–609.
[12] J. Teng, H. Snoussi, and C. Richard, "Decentralized Variational Filtering for Target Tracking in Binary Sensor Networks," *IEEE Trans. Mobile Computing*, vol. 9, no. 10, 2010, pp. 1465–77.
[13] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," *IEEE Wireless Commun.*, vol. 17, no. 1, Feb. 2010, pp. 51–58.
[14] T. Chen *et al.*, "Recent Developments in Network Intrusion Detection," *IEEE Network*, vol. 23, no. 1, Jan./Feb. 2009, pp. 4–5.

Biographies

Xu Li (xu.li@inria.fr) received a Ph.D. (2008) degree from Carleton University, Canada, an M.Sc. (2005) degree from the University of Ottawa, Canada, and a B.Sc. (1998) degree from Jilin University, China, all in computer science. Prior to joining INRIA, France, as a research scientist, he held post-doctoral fellow positions at the University of Waterloo, INRIA/CNRS, and the University of Ottawa. His current research focuses on topology control, data communications, mobility management, and network security in wireless ad hoc, sensor, and robot networks.

Rongxing Lu [S'09, M'11] (rxlu@bbcr.uwaterloo.ca) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xiaohui Liang [S'10] (x27liang@bbcr.uwaterloo.ca) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo. He is currently a research assistant with the BBCR Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and e-healthcare systems.

Jiming Chen [M'08, SM'11] (jmchen@iipc.zju.edu.cn) received his B.Sc. (2000) and Ph.D (2005) degrees from Zhejiang University, China, both in control science and engineering. He held visiting researcher positions at INRIA, France, National University of Singapore, and the University of Waterloo. He is currently a full professor with the Department of Control Science and Engineering, and the coordinator of the Networked Sensing and Control group in the State Key Laboratory of Industrial Control Technology, Zhejiang University. His research focuses on estimation, target tracking, control, and optimization in sensor and actuator networks.

Xiaodong Lin [S'07, M'09] (xiaodong.lin@uoit.ca) received a Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, China, in 1998 and a Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. (1990) degrees from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He served as an Area Editor for *IEEE Transactions on Wireless Communications* and Editor-in-Chief for *Peer-to-Peer Networks and Applications*. He is a Fellow of the Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.

The brute-force approach is time- and computation-consuming and obviously not a practical solution. Finding efficient ABE schemes based on hidden access policies can be a future research direction for delivering pervasive healthcare in smart community environments.