Delphine Christin, Matthias Hollick, and M. Manulis: *Security and Privacy Objectives for Sensing Applications in Wireless Community Networks.* In: Proceedings of the 19th International Conference on Computer Communications and Networks (ICCCN), pp. 1-6, 2010

Security and Privacy Objectives for Sensing Applications in Wireless Community Networks
(Invited Paper)

Delphine Christin*†, Matthias Hollick†, and Mark Manulis‡
*Authors listed in alphabetical order
†Secure Mobile Networking Lab, Center for Advanced Security Research Darmstadt
Department of Computer Science, TU Darmstadt, Germany
Email: delphine.christin@seemoo.tu-darmstadt.de; matthias.hollick@seemoo.tu-darmstadt.de
‡Cryptographic Protocols Group, Center for Advanced Security Research Darmstadt
Department of Computer Science, TU Darmstadt, Germany
Email: mark@manulis.eu

***Abstract*—Wireless Community Networks (WCN) are formed by the integration of user-operated wireless sensor networks that are internetworked by wireless mesh networks available within urban communities. WCNs enable novel applications for the members of the community. These include different sensing applications, where individuals contribute sensor data for further use within their community at large or with well-defined restrictions to certain users. Sensing application scenarios for WCNs differ from traditional sensor network applications with respect to their security and privacy requirements. In this paper, we define three representative scenarios—personal sensing, designated sensing, and community sensing. These scenarios are then studied with respect to their privacy and security implications. In particular, we identify main research questions and highlight the challenges of using various security and privacy approaches from networking and cryptography to make sensing applications in WCNs security and privacy aware.**

***Keywords*-wireless community networks, wireless mesh networks, wireless sensor networks, sensing applications, security, privacy, anonymity, access control**

I. Introduction

Within the scope of the future Internet, the integration of wireless mesh networks, wireless sensor networks, and mobile communications is expected to form the nucleus of future network infrastructures for urban communities—defined as *Wireless Community Networks (WCN)*. This trend is observable today from the establishment of wireless local area networks as the de-facto default access technology to the Internet in private households. As an extension of these existing networks, WCNs could offer valuable community- and human-centric services and enable novel applications. The protagonists of future community applications are not only residents, but also local authorities including fire-fighters and police as well as institutions of public interests/businesses such as schools, hospitals, pharmacies, post offices, restaurants, and local merchants.

Within the aforementioned networks security and privacy are of utmost importance; however solutions from the area of traditional networks cannot directly be transferred, since WCNs feature fundamentally different assumptions and constraints, which we subsequently identify and discuss. Our contribution is this paper is as follows: (i) we define representative application scenarios within WCNs, (ii) we identify and discuss security and privacy challenges based on these scenarios.

II. Infrastructure of Wireless Community Networks

The WCN infrastructure will have a high degree of heterogeneity as depicted in Figure 1. This heterogeneity manifests itself in different wireless technologies in both WSNs (e.g. ZigBee, 6LoWPAN, Bluetooth, IEEE 802.15.4) as well as WMNs (e.g. IEEE 802.11, IEEE 802.16, or upcoming relay and mesh extensions to existing standards). The *Wireless Mesh Network (WMN)* will serve as a backbone for the communication among the different wireless network devices, possibly operated by the users. In particular, it will allow users to provide and consume content, share information and digital resources, access services offered by other users or their own network in a remote way while being in the urban proximity.

Furthermore, the advances in ambient intelligence and smart home technology facilitate the deployment of sensors supporting our daily activities by measuring the environmental information and triggering appropriate actions. Such sensors can be comprised into a pervasive in-house *Wireless Sensor Network (WSN)* and help, for example, to conserve energy, recognize fire, or trigger alarm in case of house break-ins. Medical sensors can be further deployed to collect and monitor health information about elderly people or patients. These in-house sensor networks will be connected to the wireless mesh network and become accessible from within the community WCN.

Additionally, the advances in mobile computing and the technology progress aiming at improvement of the functionality of mobile devices such as laptops, smart phones, and tablet PCs will introduce the *mobility* factor into the WCN infrastructure. Mobile devices will be used not only for the plain communication among the users of the community such as telephony, exchange of information and data but also enable a variety of collaborative applications.

III. Sensing Applications in Wireless Community Networks

Among the novel applications offered by WCNs there will be various types of *sensing applications* aiming to collect and process information sensed from the environment. For a wide variety of measurements there already exist appropriate sensors and a single node is usually equipped with multiple embedded sensors and capable of handling several data types at once. In particular there exist sensors measuring diverse chemical compounds, occurring vibrations and hall effects, changing light conditions, temperature, humidity, various types of pressure, electromagnetic fields, presence of liquids/water, noise, as well as diverse medical data and detection of movements. In general, sensors can be used in a static way, that is a sensor being responsible for the measurement of data at some particular location, or in a dynamic way, for example, when integrated into some mobile device such as a smart phone.

In the scope of WCNs sensors will surely offer valuable services with regard to the personal and public safety of community members, secure and protect their houses, and may help, in general, to improve the living conditions in the community, while also providing all sorts of assistance to community members in their everyday activities. While taking a global view on the sensing applications allows surely to identify their overall benefits and potentials, it is still desirable to differentiate among the sensing applications based less on the type of data being sensed but more on the ability of users to access this data and use it for their purpose. Especially, in WCNs where the network infrastructure is used by all members of the community, questions related to the privacy of measurements and access to the possibly shared data are of great importance. For example, data collected by an in-house WSN may serve different purposes and it may be desirable that this data is accessible by various community members: e.g. medical data collected from an in-house health monitoring system of a patient is valuable for the medical personnel hospitals/surgerys in the neighborhood, data aiming at house protection (e.g. in case of fire or a house break-in) is valuable for firefighters and police, whereas the general environmental data, e.g. for measuring the pollution is valuable to the community as a whole.

In this paper we put forth three sensing application scenarios for WCNs—personal sensing, designated sensing, and community sensing. We distinguish among them by considering the roles of participants and access policies to the measurements as explained in the following.

By *personal sensing* we understand individual access to the in-house WSN data by the householder. The householder is in general the owner or the administrator of the in-house sensor network. This sensing application is essential for the measurement of some private data that should be accessible only by the owner of the network. In particular, personal sensing may be defined for *any* in-house WSN node. Consider as an example some movement or light recognition sensor being installed in the bath room. It is clearly desirable that the information on whether the bath room is currently occupied is not available to any other member of the community, except for the habitants of that house.

By *designated sensing* we consider applications in which data measured by some in-house WSN nodes becomes accessible only to some designated member(s) of the community. This application addresses, for example, monitoring of the health data of patients and elderly people at home and access to it by certain medical personnel in the neighborhood in order to thwart risks in case of emergency. Another example, are fire alarm or house break-in sensors that could actuate the appropriate operation by firefighters or police forces. Specific in-house WSN nodes can thus be dedicated to serve in the designated sensing applications. Moreover, it is imaginable that some of these nodes are not actually configured or controlled by the house habitants but by network or utility operators or even some other authorities. Addressing privacy aspects in this latter scenario is of paramount importance, since users are not in control of these sensors.

Finally, by *community sensing* we consider applications with public access to some in-house WSN nodes. In general, these applications may serve the improvement of living conditions and public safety of the community. In particular, community sensing may provide environmental information on current weather conditions or pollution at some particular location within the community. Community sensing applications can be also extended by considering the mobility aspect of WCNs towards the so-called *participatory sensing* scenarios [1] where any mobile member of the community may gather and share information useful for other members. In particular, this includes *opportunistic sensing* scenarios, where the mobile device of a member is activated while being in proximity of some certain location.

IV. Security and Privacy Challenges in WCN Sensing

The different sensing applications described above have their own security and privacy challenges. Security challenges are motivated by the integration of sensors into the WCN infrastructure. These include typical problems with

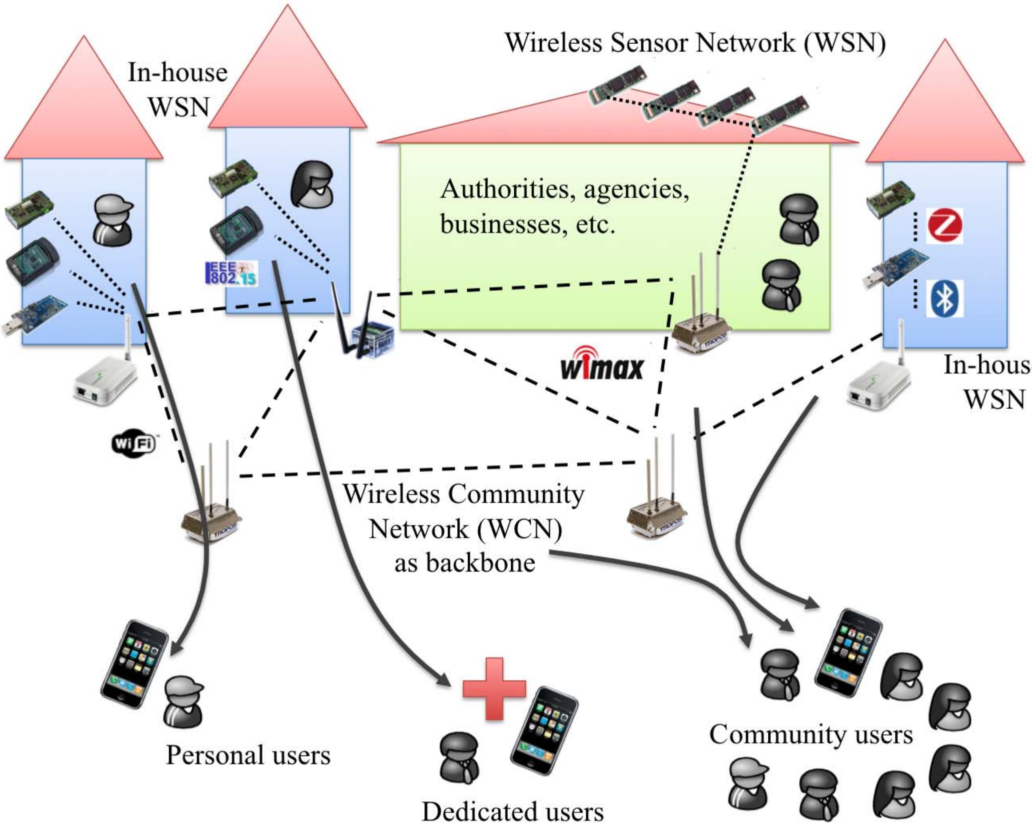
Wireless Sensor Network (WSN)
In-house WSN
Authorities, agencies, businesses, etc.
IEEE 802.15
wimax
Wi Fi
In-house WSN
Wireless Community Network (WCN) as backbone
Personal users
Dedicated users
Community users

Figure 1. WCN infrastructure and application scenarios in WCNs

securing the WCN communication and in particular the access control to the measured data. Privacy challenges are motivated by the availability of sensors in houses of community members or in their mobile devices. As such measurements being sensed may shed light on private activities of community members or reveal their personal information. In the following we identify several security and privacy challenges for sensing applications in WCNs.

A. Security and Privacy Models

In order to protect security and privacy in WCN sensing applications it is necessary to understand the exact risks and threats for each of the application types. Hence, specification of appropriate security and privacy models for WCN sensing applications is of utmost importance for the design and comparison of future protection mechanisms. On the one hand, these models should consider the capabilities of the adversary, which may differ depending on the application. In general, adversarial threats should be addressed along the different components of the WCN infrastructure and thus include threats with respect to the underlying WMN as well as integrated WSNs and mobile networks. These models should also consider that WCN is a heterogeneous infrastructure that is administrated in a distributed way. For example, different integrated WSNs may have their own owners and also different parts of the WMN backbone may not have any centralized control. In addition to the networks, the adversary model should consider different roles of community members and distinguish among possible attacks from the outside of the WCN network and also from the inside, i.e. by other members of the community.

B. Mechanisms for Privacy-Preserving Personal and Designated Sensing

In personal and designated sensing applications access to the measurements should be based on appropriate privacy-preserving access control mechanisms. The access here should be restricted either to the owner of the sensor network or to some particular community member, designated by the owner. Hence, the actual design of suitable privacy-preserving access control mechanisms to WSNs constitutes the main challenge for these applications.

Although network security and cryptography offer traditional authentication mechanisms for securing access control to a network or some data such as digital signatures or encryption, these mechanisms may not be directly applicable to the sensing applications since they do not respect the privacy of the authenticating parties. Hence, the arising research question is how to establish confidential communication across the heterogeneous multihop network built from the integration of WMNs and WSNs, possibly under consideration of a mobile device as one of the end-points of the communication. This includes the design of appropriate privacy-preserving remote access control mechanisms by which a mobile user can access the measurements of his in-house WSN. For example, the classical use of VPNs is not privacy-preserving as it discloses the identities of communicating parties to the intermediate network components, this in addition to the increased overhead resulting from the management of the VPN infrastructure and its limited use on mobile devices. Hence, design of appropriate privacy-preserving mechanisms for secure WCN communications will require novel cryptographic protocols and network security approaches.

In particular, novel encryption methods such as attribute-based [2], [3], [4] or predicate-based encryption [5] that have been designed with privacy-preserving access control to encrypted data in mind, may give suitable interactive solutions for privacy and security in the personal and designated sensing applications. One of the challenges here is to adapt these techniques to the heterogeneity of the WCN infrastructure and to deal with multiple authorities [6] for the management of cryptographic keys. Since most of these methods require costly cryptographic computations it will thus be necessary to adapt them to the lightweight requirements of WSNs. A possible solution to this problem is to design efficient security protocols that utilize the resources of the mesh nodes to aid resource-constrained sensor nodes, i.e. to introduce the asymmetry into the security-relevant computations performed by sensor nodes. Another challenge results from the co-existence of personal and designated sensing applications. In fact, it is worth to investigate how privacy of measurements performed by some in-house WSN nodes can be guaranteed while allowing controlled partial access from the WCN to some other nodes. Obviously, appropriate mechanisms will require some fine-grained form of access control.

C. Mechanisms for Privacy-Preserving Community Sensing

Controlled access to the sensed data in a privacy-preserving way is crucial for within personal and designated sensing applications. The privacy problem behind the community sensing applications is slightly different: These applications assume that the measurements become public and thus no access control in its traditional sense is necessary. The actual privacy problem is that although the sensed information is of value for the community as a whole, it might be still desirable to anonymize it and make it untraceable to a particular household or user. Note also the significant privacy problem in participatory community sensing applications in which not only the identity of the mobile user or his device but also the entire location should remain private, or, for certain applications, a trade-off between location privacy and sensing accuracy exists.

Hence, we are mostly concerned with the anonymization of the sensed environmental data that should become public. Several solutions are worth of being explored. In particular, one may try to approach this problem through the use of appropriate in-network processing techniques such as secure aggregation of data [7], [8], [9], [10]. While schemes like [8], [9] guarantee authenticity and integrity of aggregated measurements, some approaches such as [10] support additional confidentiality of aggregated data through the use of homomorphic encryption techniques. Nevertheless, existing schemes are not privacy-preserving since the aggregation process reveals identities of participating nodes. Hence, design of privacy-preserving aggregation schemes could give rise to suitable solutions for community sensing applications.

Another approach it to harness the characteristics of wireless multihop networks, such as spatial diversity by using directional antennae and multipath routing [11], [12], or temporal diversity by using the delay-tolerant networking approaches to protect eavesdropping on data. Depending on the adversary model it may become hard for the adversary to breach the privacy of the measured data.

Anonymization in community sensing applications could also utilize the mechanism of differential privacy [13], [14]. This approach is frequently applied for maintaining privacy of users in database applications. In essence, it aims at minimizing the risks for privacy of user who join some statistical database. By considering all in-house WSN nodes that participate in a community sensing application as a distributed database, the techniques of differential privacy may give interesting solutions for maintaining privacy of users and their households in these applications. Potential challenge here is to cope with the distributed nature of the WSN database comprised of nodes under different administrative control. This may require design of additional overlay networks which will be responsible for collecting the measurements and providing them to the community in a privacy-preserving way.

V. Related Work

The security and privacy challenge of participatory sensing has recently been raised [15], and first approaches towards privacy-aware participatory sensing have been proposed [16], [17], [18]. Ref. [16] focuses on location privacy in systems with centralized data collection infrastructure, which cannot directly be applied in the situated and localized operation necessary in WCNs. Ref. [17] focuses on temporal and spatial privacy of mobile users and builds on the well-known principles of *k*-anonymity and *l*-diversity; it similarly focusses on centralized processing of the collected data. Ref. [18] proposes mechanisms to utilize the direct interactions between participants/sensors to establish mutual trust relationships between participants and allow for establishing decentralized privacy solutions. Consequently, existing mechanisms from the area of participatory sensing cannot be directly applied, since community sensing extends the classical participatory sensing concept by assuming situated, direct, and proximity-based exchange of information using WCNs as well as by including additional sensing capabilities (stationary sensors in homes).

For within wireless mesh networks (WMNs), which form the backbone in WCNs, several security solutions exist [19], [20], [21], including secure remote access for community WMNs [22]. However, these works focus on the basic security guarantees for authenticated and confidential communication, yet without considering the additional privacy guarantees arising in WCNs. In the Internet, solutions for anonymous communication and traffic pattern concealment have been proposed such as layered encryption mechanisms (onion routing) [23], [24], [25], which is used to hide traffic patterns. These mechanisms can provide user anonymity in an end-to-end connection as long as no collusion of routers along the underlying path does occur. Their application to WMNs directly is difficult, since WMNs have typically a limited number of mesh nodes and more importantly the shortest transmission path is usually chosen by underlying routing algorithms, thus restricting the ability of mesh nodes to forward traffic along pre-specified routes. Another approach for traffic privacy is to generate a continuously random data stream at the link layer (traffic padding) [26]. Although this makes the traffic pattern recognition more difficult, it has negative impact on the consumed network bandwidth [27]. Multipath routing, originally proposed for load-balancing, can be used to increase traffic privacy by forwarding packets over distinct (possibly random) paths [11], [12].

The aggregation of data in WSNs has also attracted a lot of attention in the recent years: Earlier solutions [28], [29] did not consider adversarial attacks; some approaches offer only limited tolerance to node corruptions [30], [7] or can deal only with limited set of functions [8]. The approach in [9], although being generic and optimally secure against node corruptions, offers basic authenticity of measurements, yet without considering privacy for the nodes. Similarly, the concealed data aggregation techniques [31], [10] provide confidentiality of measurements but no privacy guarantees for the nodes, and are thus not directly applicable to community sensing applications in WCNs.

VI. Conclusion

Wireless Community Networks will shape the landscape of future Internet and enable novel applications for the members of urban communities aiming at the improvement of their safety and living conditions. This improvement will be partly due to the deployment of various sensing applications in WCNs, in which all sorts of environmental data will be sensed by the stationary or mobile sensors and provided to the members of the community either publicly or controllable. In this paper we identified three representative sensing applications (personal sensing, designated sensing, and community sensing) for which different security and privacy guarantees arise. Our work is a first step towards understanding the relevant problems and finding solutions behind WCN sensing applications. We discussed the main research challenges and highlighted techniques from networking, cryptography, and information security, that may give rise to suitable security and privacy solutions for WCN sensing applications.

Acknowledgment

This work was supported by the Center of Advanced Security Research Darmstadt - CASED (www.cased.de).

References

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, “Participatory Sensing,” in *Proceedings of World Sensor Web Workshop (WSW), ACM Sensys 2006, Boulder, CO, USA*, 2006, pp. 1–5.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” in *13th ACM Conference on Computer and Communications Security (CCS 2006)*. ACM, 2006, pp. 89–98.

[3] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures,” in *14th ACM Conference on Computer and Communications Security (CCS 2007)*. ACM, 2007, pp. 195–203.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” in *IEEE Symposium on Security and Privacy (S&P 2007)*. IEEE CS, 2007, pp. 321–334.

[5] J. Katz, A. Sahai, and B. Waters, “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products,” in *EUROCRYPT 2008*, ser. LNCS, vol. 4965. Springer, 2008, pp. 146–162.

[6] M. Chase, “Multi-Authority Attribute Based Encryption,” in *Theory of Cryptography Conference (TCC 2007)*, ser. LNCS, vol. 4392. Springer, 2007, pp. 515–534.

[7] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks,” in *ACM Conference on Embedded Networked Sensor Systems (SenSys 2003)*. ACM, 2003, pp. 255–265.

[8] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," in *13th ACM Computer and Communications Security Conference (CCS 2006)*. ACM, 2006, pp. 278–287.

[9] M. Manulis and J. Schwenk, "Security Model and Framework for Information Aggregation in Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 2, p. Article 13, 2009.

[10] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 5, no. 3, pp. 1–36, 2009.

[11] J. J. Garcia-Luna-Aceves and M. Mosko, "Multipath Routing in Wireless Mesh Networks," in *1st IEEE Workshop on Wireless Mesh Networks (WiMesh 2005)*, 2005.

[12] D. S. Nandiraju, N. Nandiraju, and D. P. Agrawal, "Adaptive State-Based Multi-Radio Multi-Channel Multi-Path Routing in Wireless Mesh Networks," *Pervasive and Mobile Computing*, vol. 5, no. 1, pp. 93–109, 2009.

[13] C. Dwork, "Differential Privacy," in *33rd International Colloquium on Automata, Languages and Programming (ICALP 2006)*, ser. LNCS, vol. 2. Springer, 2006, pp. 1–12.

[14] ——, "Differential Privacy: A Survey of Results," in *5th International Conference on Theory and Applications of Models of Computation (TAMC 2008)*, ser. LNCS, vol. 4978. Springer, 2008, pp. 1–19.

[15] K. Shilton, "Four billion little brothers?" *Communications of the ACM*, vol. 52, no. 11, pp. 48–53, 2009.

[16] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: Privacy-Aware People-Centric Sensing," in *Proceedings of of the 6th international conference on Mobile Systems, Applications, and Services (MobiSys 2008), Breckenridge, CO, USA*. ACM, 2008, pp. 211–224.

[17] K. Huang, S. S. Kanhere, and W. Hu, "Preserving Privacy in Participatory Sensing Systems," *Computer Communications*, 2010, accepted for publication, to appear.

[18] D. Christin, "Impenetrable Obscurity vs. Informed Decisions: Privacy Solutions for Participatory Sensing," in *IEEE International Conference on Pervasive Computing and Communications (PerCom2010) - PhD Forum*. IEEE, 2010, pp. 1–2.

[19] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[20] B. Wu, J. Chen, J. Wu, and M. Cardei, *Wireless Network Security*. Springer, 2007, ch. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks, iSBN: 978-0-387-28040-0.

[21] P. S. Mogre, K. Graffi, M. Hollick, and R. Steinmetz, "AntSec, WatchAnt and AntRep: Innovative Security Mechanisms for Wireless Mesh Networks," in *IEEE LCN 2007*. IEEE CS, October 2007, pp. 539–547.

[22] M. Manulis, "Securing Remote Access Inside Wireless Mesh Networks," in *10th International Workshop on Information Security Applications (WISA 2009)*, ser. LNCS, vol. 5932. Springer-Verlag, 2009, pp. 324–338.

[23] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous Connections and Onion Routing," in *IEEE Symposium on Security and Privacy (IEEE S&P 1997)*. IEEE CS, 1997, pp. 44–54.

[24] M. J. Freedman and R. Morris, "Tarzan: A Peer-to-Peer Anonymizing Network Layer," in *ACM Conference on Computer and Communications Security (CCS 2002)*. ACM, 2002, pp. 193–206.

[25] X. Wu and N. Li, "Achieving Privacy in Mesh Networks," in *4th ACM Workshop on Security of Ad hoc and Sensor Networks (SASN 2006)*. ACM, 2006, pp. 13–22.

[26] P. Venkitasubramaniam and L. Tong, "Anonymous Networking with Minimum Latency in Multihop Networks," in *IEEE Symposium on Security and Privacy (S&P 2008)*. IEEE CS, 2008, pp. 18–32.

[27] H. Pucha, S. M. Das, and Y. C. Hu, "The Performance Impact of Traffic Patterns on Routing Protocols in Mobile Ad Hoc Networks," *Computer Networks*, vol. 51, no. 12, pp. 3595–3616, 2007.

[28] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks," in *ACM MOBICOM 1999*. ACM, 1999, pp. 263–270.

[29] S. Madden, M. J. Franklin, J. M. Hellerstein, and W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," in *ACM SIGOPS OSDI*. ACM, 2002, pp. 131–146.

[30] L. Hu and D. Evans, "Secure Aggregation for Wireless Network," in *Symposium on Applications and the Internet Workshops (SAINT 2003)*. IEEE CS, 2003, pp. 384–394.

[31] D. Westhoff, J. Girao, and M. Acharya, "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1417–1431, 2006.