A Delay-Aware and Secure Data Forwarding Scheme for Urban Sensing Networks

Di Tang Jian Ren
Dept. of ECE, Michigan State University, East Lansing, MI 48824
Email: {ditony, renjian}@msu.edu

***Abstract*—People-centric urban sensing is envisioned as a novel urban sensing paradigm. Communication delay and security are two important design issues in urban sensing network. To address these two issues concurrently, we propose a novel DElay-Aware secuRe (DEAR) forwarding scheme by combining secret sharing and two-phase message forward. In DEAR scheme, the collected data is first split into pieces. Each piece is being relayed to the application data server through a randomly selected delivery node. The combination of secret sharing scheme and two-phase message forward ensures confidentiality of the collected data and anonymity of the participating users. It also makes it infeasible for the application data server to estimate the source node identity. Moreover, DEAR provides redundancy in message forwarding to achieve high message delivery ratio. This design makes the trade-off between security and communication delay adjustable based on selection of the (k, n) scheme.**

I. Introduction

The recent technological advances enable people-centric urban sensing networks technically and economically feasible to be widely used in civilian applications, such as monitoring the urban environment, traffic conditions and personal health. People centric urban sensing network relies on the human-carried mobile devices equipped with embedded sensors to collect and report the sensing data. The powerful resources equipped in the mobile devices increase their capabilities in computation, sensing, data storage and lifetime. It makes energy consumption less critical than in traditional wireless sensor networks.

Due to mobility of participating users, data sensing and forwarding no longer rely on fixed network topologies. The collected data can be forwarded to an application data server directly through wireless access points or indirectly through multi-hop forwarding. Communication delay becomes one of the key quality of service (QoS) issues of the network.

The method of data collecting and reporting puts the users' privacy at risk. Delivery nodes and wireless access points are both able to identify the data source through direct communication. The uploaded data is collected with spatial-temporal information which may be used to extract or infer sensitive information. As a result, the locations correlated with identities may be used to build the trajectory of the participating users. In addition, side information could also be used to correlate identities to location information even if pseudonyms are used.

This work was supported in part by the NSF under grants CNS-0845812, CNS-1117831, CNS-1217206, and ECCS-1232109.

In this paper, we propose a decentralized data forwarding scheme to preserve trajectory privacy of participating users based on secret sharing and two-phase message forward. The proposed scheme is designed to achieve a trade-off between communication delay and security. DEAR provides redundancy for error tolerance under additional computational overhead, which ensures a high message delivery ratio for data transmission. DEAR makes security and communication delay trade-off adjustable based on selection of the (k, n) scheme.

Our contributions of this paper can be summarized as follows:

1) We propose a novel DElay-Aware secuRe (DEAR) forwarding scheme to preserve trajectory privacy of the participants in urban sensing network.
2) The proposed DEAR makes security and communication delay trade-off adjustable based on selection of the (k, n) scheme.
3) DEAR provides a design trade-off between message delivery ratio and communication/computational overhead.

The rest of this paper is organized as follows. In Section II, the related work is reviewed. The system model is presented in Section III. The proposed scheme is described in Section IV. In Section V, security analysis of the proposed scheme is conducted. Section VI provides performance analysis of the proposed scheme. We conclude in Section VII.

II. Related Work

Participatory sensing was first proposed in [1]. The concept was extended to urban sensing and people-centric sensing in [2]. The key idea of such sensing networks is that it relies on mobile devices for data collecting and forwarding. The networks provide a flexible method to collect valuable environmental information for people in urban area. However, it also raises privacy concerns.

Location privacy for urban sensing networks was first discussed in [3]. It first proposed an algorithm based on data aggregation for anonymous task allocation and data reporting. It blurs the location information in an aggregated data packet. This idea of data aggregation was further studied in [4] and [5]. Spatial cloaking was proposed to achieve location k-anonymity recently. It relies on a trusted third party to construct a cloaking area to obfuscate a mobile user's exact location. In [6] and [7], it has been studied to achieve a trade-off between location accuracy and user privacy. The authors in [8] and [9] proposed dummy location methodology

to prevent adversaries from estimating the reported location information. However, the privacy protection is achieved by sacrificing resolution on either spatial or temporal dimensions.

Alternatively, data exchange schemes were proposed in [10]. The collected sensor readings are exchanged between participants within direct communication range. The collected data may be exchanged multiple times to prevent adversaries from correlating between identity and the data content. In [11], the collected data is forwarded from friends to friends of the source user until the required number of hops has been reached. However, the identity information of this scheme can be exposed through direct communication. The location information can also be directly exposed to the delivery nodes. There is little flexibility in delivery ratio when the data is being dropped or tampered with.

III. Models and Assumptions

A. System Model

The urban sensing network relies on a set of mobile sensor nodes embedded in mobile devices and carried by volunteer participants for data collection and forwarding. These devices can get wireless Internet access intermittently through wireless access points (APs) in the sensing area. The APs, such as WiFi access points, may be owned and operated by the government, organizations or individuals. They are directly connected to the application data server. In this network, the surrounding environment information is collected by the participating mobile devices and eventually sent to the application data server.

The application data server provides environmental sensing services for data consumers and disseminates the requested tasks to participating mobile users. Mobile devices can join the system at will to participate in data sensing. They are required to report the collected data to the application data server once they accept the tasks. To provide precise service to data consumers, the data is required to be collected with spatial-temporal information. This information may expose details about participating user's location. Due to the characteristics of opportunistic sensing and the physical infrastructure of urban sensing networks, we only deal with sensing data that is delay tolerant.

B. Adversary Model

Our adversary model is similar to [4]. We assume the adversaries can be any parties in the network, including individual sensing nodes, wireless access points, and even the application server. Adversaries may try to disclose the privacy of participants by discovering the identity and location information. They may further recover the trajectory of a participant by correlating a series of reported locations with the participating user's identity. We also consider the side information attack [12]. More specifically, in this paper, the adversaries are assumed to have the following characteristics:

- The adversaries can be any parties in the network, including individual sensing nodes, wireless access points, and even the application data server.
- The adversaries are generally assumed to be honest but curious. However, in this paper, we further assume that some adversaries may drop or tamper with the reported data due to their own interests.
- The adversaries are able to collect side information to observe the appearance of the participants.
- The administrative adversary, such as application data server, can access the spatial-temporal information in the reported data. It may try to correlate this information to the participating user's identity to recover his trajectory.
- The individual adversary, such as the delivery node, can obtain the source pseudonym. To obtain location of the participant, it may try to discover the spatial-temporal information, and link the pseudonyms with the real identity by collecting side information.

IV. Proposed Privacy Protection Scheme

In this section, we present a Shamir's secret sharing based privacy-preserving message forwarding scheme for reported data. It can ensure confidentiality and also provides a verification option for reported data. The scheme includes two phases in message forwarding.

A. Overview of the Proposed Privacy Protection Scheme

To transmit collected data, the source node generates n data pieces based on the secret sharing scheme. The source node then picks a pseudonym and assigns it to each data piece as its identity to conceal the source information. The generated data pieces are then forwarded to n randomly selected neighboring participating users, named as delivery nodes, within the communication range. Each delivery node relays the received data piece to the application data server through nearby AP. Upon receiving k or more data pieces, the application data server is able to reconstruct the original collected data. Additionally, the reconstruction algorithm also enables the recovered data to be verified for integrity.

B. Secret Sharing

Shamir's (k, n) secret sharing scheme can be described as follows: let $a_0, a_1, \cdots, a_{k-1}$ be positive integers from a finite field $\mathbb{Z}_p$, and $a_0 = S$ be the shared secret. Define

$$f(x) = a_0 + a_1 x + \cdots a_{k-1} x^{k-1}$$

and select n points out of $f(x)$. Without loss of generality, let the n points be the pairs $(i, f(i)), i = 1, \cdots, n$. Then given any k pairs, we can find the coefficients of the polynomial using Barycentric Lagrange Interpolation as follows:

Define

$$\begin{aligned} l(x) &= (x-1)(x-2)\cdots(x-k), \\ w_j &= \frac{1}{\prod_{i=0, i\neq j}^{k}(j-i)}, \end{aligned} \tag{1}$$

$$L(x) = l(x)\sum_{j=0}^{k}\frac{w_j}{x-j}f(j). \tag{2}$$

The shared secret is $a_0 = L(0)$.

C. The Proposed Privacy Protection Scheme

Assume the source node $\mathcal{H}$ holds the collected data d to transmit. It first computes the hash value $H(d)$, where H is a one way hash function. Then, it treats d and $H(d)$ as two independent pieces of secret data. Develop two separate (k, n) secret sharing schemes to share d and $H(d)$ separately. The polynomial computation is operated over finite field $\mathbb{Z}_q$. The procedure is described as follows:

1) $\mathcal{H}$ chooses a prime $q > \max(d, n)$.
2) $\mathcal{H}$ constructs two coefficient sets, $\mathcal{A}$ and $\mathcal{B}$. Each set contains k randomly selected coefficients, $\mathcal{A} = \{a_0, ..., a_{k-1}\}$ and $\mathcal{B} = \{b_0, ..., b_{k-1}\}$ from $\mathbb{Z}_q$ such that $a_0 = d$ and $b_0 = H(d)$.
3) $\mathcal{H}$ generates two random polynomials over $\mathbb{Z}_q$ as follows:

$$f_a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \quad (3)$$

$$f_b(y) = b_0 + b_1 x + \cdots + b_{k-1} x^{k-1} \quad (4)$$

4) $\mathcal{H}$ computes n components $f_a(i), f_b(i)$ from d and $H(d)$, respectively, $i = 1, \cdots, n$.
5) The i^{th} data piece for d and $H(d)$ is $(i, f_a(i), f_b(i))$, where $i = 1, \cdots, n$.

The generated n data pieces are distributed to n randomly selected delivery nodes before being relayed to the application data server. Since the delivery nodes are not completely trusted, the reconstructed data has to be verified for integrity assurance. The reconstruction algorithm follows Shamir's secret sharing scheme using Barycentric Lagrange Interpolation. It is described in the following steps:

1) Suppose the server has received at least k shared secret pieces out of the n data pieces. Each piece is denoted as $(i, f_a(i), f_b(i))$ for data $(d, H(d))$.
2) Reconstruct the data d and $H(d)$ by using Barycentric Lagrange Interpolation. Since some of the received data components may have been tampered with, the reconstructed data could be different from the original data. So we denote the reconstructed data as d' and D, respectively.
3) The recovered data is then verified by comparing whether $H(d') = D$. If the equality holds, then it shows the reconstructed pair secret data pieces are both valid. Otherwise, the data set used to construct d' and D contains at least one corrupted data piece.

The proposed data distribution scheme includes two phases in message forwarding. It can be summarized as Algorithm 1.

Algorithm 1 Data Distribution

1: Choose a prime $q > \max(d, n)$.
2: Construct two random coefficient sets $\mathcal{A}$ and $\mathcal{B}$ from $\mathbb{Z}_q$.
3: Based on $\mathcal{A}$ and $\mathcal{B}$, construct two polynomials over $\mathbb{Z}_q$ $f_a(x) = \sum_{i=0}^{k-1} a_i x^i$, and $f_b(y) = \sum_{i=0}^{k-1} b_i y^i$ to share d and $H(d)$ as two secret values, respectively.
4: Compute n data pieces $d_i = (i, f_a(i), f_b(i)), i = 1, \cdots, n$.
5: **for** each $i \in [1, n]$ **do**
6: Send d_i to a randomly selected neighbor node A_i.
7: The neighbor node A_i forwards it to the wireless access point.
8: **end for**
9: The server recovers and verifies the collected data based on the data reconstruction algorithm.

V. Security Analysis

The users in urban sensing network can contribute valuable information by collecting and forwarding the sensed data to the application server. However, the reported data with its spatial-temporal information may expose the privacy information of the participating user. Adversaries may first reveal the spatial-temporal information contained in the received data. Furthermore, they may correlate the exposed spatial-temporal information with the identity to disclose the privacy of participating users. The aforementioned attacks may be repeated by the adversaries to obtain the trajectory information.

Based on the two-phase design, our security analysis includes two scenarios. First, the delivery node may collect side information to correlate the obtained pseudonym or the received data piece with the real identity. However, it will not be able to obtain the spatial-temporal information. Second, the application data server could obtain the spatial-temporal information. However, it will not be able to reveal the source identity information. We also demonstrate that the proposed DEAR is able to verify the reconstructed data and defend the reported data against tampering attacks.

We will introduce identity information leakage and location information leakage to measure security of the proposed scheme.

Definition 1 (Identity Information leakage)**.** *The identity information leakage is defined as the probability that the adversary is able to derive the source node identity of a given data.*

Definition 2 (Location Information leakage)**.** *The location information leakage is defined as the probability that the adversary is able to derive the spatial-temporal information of a given data.*

A. Identity Information Leakage

The adversaries may obtain identity information when they directly communicate with participating users. Direct communication can also help the delivery node to infer that the source node is located in his communication range. By collecting identities of the participating users appearing in this range, the delivery node may be able to derive the real identity of the message.

To deal with this issue, in this paper, the source node uses dynamic pseudonyms [13] when it forwards messages to the delivery nodes. As a result, it becomes infeasible for the delivery node to correlate the received data with the real identity. However, as aforementioned, the delivery nodes can collect side information, such as identities, to narrow the scope of estimation on the real identity of reported data.

Suppose l is the number of collected identities, which equals to the population in the communication range of the delivery node. The identity information leakage for each message should be $\frac{1}{l}$. Assume ρ is the population density in the network and Δ is the communication range of the sensor node. Then,

TABLE I
THE AVERAGE COMMUNICATION DELAY AND LOCATION INFORMATION LEAKAGE FOR DIFFERENT (k, n)

$Delay(s)/P_k(\%)$	$k=10$	$k=15$	$k=20$	$k=25$	$k=30$
$n=10$	416.991/0.0017	-	-	-	-
$n=15$	220.831/0.89	$455.47/6.97\times10^{-6}$	-	-	-
$n=20$	174.79/9.24	$252.89/1.67\times10^{-2}$	$484.47/2.87\times10^{-8}$	-	-
$n=25$	148.95/30.42	203.88/0.56	$276.17/2.27\times10^{-4}$	$506.36/1.18\times10^{-10}$	-
$n=30$	132.281/56.83	176.22/4.3	$225.761/1.94\times10^{-2}$	$295.25/2.44\times10^{-6}$	$523.38/4.86\times10^{-13}$

the average l can be computed as $l=\pi\Delta^2\rho$. In a typical urban area of Manhattan, parameter ρ is 2.74×10^5 persons/km^2. As a result, the identity information leakage can be very small.

In the worst case, the side information helps the delivery node to correlate one single pseudonym to the real identity. However, since the pseudonym changes for each reported data, which makes it infeasible to correlate the pseudonyms used for other reported data with the real identity. As a result, the delivery node is unable to correlate them and build the trajectory.

Furthermore, the administrative adversaries are isolated from the source node by the two-phase forwarding method. Therefore, the administrative adversaries, such as the data server and the APs, are not able to obtain the real identity.

B. Location Information Leakage

The spatial-temporal information can be revealed by discovering the content of the reported data. Since the application data server is able to access the content of the reported data, it makes the malicious delivery node the only party interested in obtaining the spatial-temporal information. Based on secret sharing scheme, the malicious delivery node needs to collect k or more data pieces to reveal this information. In each data distribution, the source node randomly selects one neighboring node as the delivery node. It means the malicious node needs to be selected as the delivery node k or more times to discover the spatial-temporal information. Suppose ρ is the population density in the network and Δ is the communication range of sensor nodes. The probability P_s for a node to be selected as the delivery node can be computed as $\frac{1}{\pi\Delta^2\rho}$. Assume that the malicious node is a candidate delivery node for relaying each data piece, the location information leakage P_k can be computed by the following equation:

$$P_k=\sum_{i=k}^{n}\binom{n}{i}P_s^i(1-P_s)^{n-i}. \tag{5}$$

Numerical results of the location leakage is shown in Table I. In this table, we compared location leakage for various k, n that vary from 10 to 30. From the numerical results we can see that when delay increases, the location information leakage will decrease. In particular, for a properly selected (k, n), the location leakage is close to 0.

C. Data Integrity and Availability

In order to prevent the adversaries from tampering with the reported data, DEAR provides verification procedures for the received data. First, the proposed scheme can prevent up to $k-1$ malicious nodes from recovering the data based on the secret sharing design. If at least one of these k components has been tampered with, then we should have $H(d')\neq D$ and we can detect that the data set used to recover the secret d contains at least one corrupted data piece.

In summary, the proposed two-phase forwarding scheme can prevent the server from estimating the identity of the participating user. It can also thwart the delivery nodes from obtaining the location information. Therefore, the trajectory privacy of participating users can be protected by the proposed two-phase forwarding scheme. Additionally, the scheme can also verify the received data and defend against tampering attacks.

VI. PERFORMANCE ANALYSIS

In urban sensing networks, the quality of service may be measured by communication delay and delivery ratio. In this section, we analyze the communication delay and error rate of the proposed scheme. Numerical results of the expected communication delay and error rate are also presented in this section.

A. Overhead of the Proposed Scheme

The proposed scheme includes two phases for data forwarding. For communication delay, the first phase of the forwarding scheme is introduced for the source node to distribute the data pieces when encountering the delivery nodes. The second phase is introduced for the delivery nodes to relay the data pieces to the application data server.

The delay for each data piece distribution can be analyzed by using the pedestrian content distribution process, which can be modeled as Poisson Process [14]. Let λ be the arrival rate, then the time duration γ_i for the i^{th} data piece distribution follows the Γ distribution. The probability distribution function of γ_i is given by

$$f_{\gamma_i}(t)=\lambda e^{-\lambda t}\cdot\frac{(\lambda t)^{(n-1)}}{(n-1)!}. \tag{6}$$

In the second phase, the delay is the time duration from the time that the delivery node receives a data piece until it travels to the next AP. Suppose the delivery node receives the data piece at time $\hat{t}$. Let T be the time duration that the delivery node travels from one AP to the next AP. Then, the time $\hat{t}$ should be uniformly distributed in the range of T. We denote the delay in the second forwarding phase as t_i for each data piece d_i. The total communication delay T_d can be computed by

$$T_d=\min_{1\to k}\{\gamma_i+t_i\,|i=1,\cdots,n\}, \tag{7}$$

where $\min_{1\to k}$ is the delay time for the application data server to receive the first k data components.

TABLE II
THE ERROR RATE FOR THE REPORTED DATA. n=30

$P_E(\%)$	$k=5$	$k=10$	$k=15$	$k=20$	$k=25$
$p_e=1\%$	2.64×10^{-46}	1.31×10^{-33}	1.27×10^{-22}	4.59×10^{-13}	4.83×10^{-5}
$p_e=2\%$	1.70×10^{-38}	2.52×10^{-27}	7.31×10^{-18}	7.87×10^{-10}	2.51×10^{-3}
$p_e=3\%$	6.20×10^{-34}	1.15×10^{-23}	4.19×10^{-15}	5.70×10^{-8}	2.33×10^{-2}
$p_e=4\%$	1.05×10^{-30}	4.43×10^{-21}	3.65×10^{-13}	1.13×10^{-6}	1.06×10^{-1}
$p_e=5\%$	3.35×10^{-28}	4.39×10^{-19}	1.13×10^{-11}	1.10×10^{-5}	3.28×10^{-1}

B. Numerical Results of Communication Delay

In the simulations, we assume the time duration T is uniformly distributed in the range of $[100s, 300s]$. The arrival rate for the data distribution is 10 s/packet. Table I shows the proposed scheme can minimize the location leakage by increasing the communication delay. As a result, based on selection of the (k, n) secret sharing scheme, the security and the communication delay can both be adjusted to satisfy various demands of the participants.

C. Delivery Ratio

Due to the nature of wireless communications, the message may be dropped or received incorrectly. However, the proposed scheme provides redundancy to minimize the error rate for the reported data. The underlying secret sharing ensures that the reported data is correctly recovered by receiving at least k or more correct data pieces. The extra $n-k$ data pieces are considered redundant messages that may be used for data recovery under erroneous scenarios. Let p_e be the error rate or packet loss rate that a single data piece is received incorrectly or dropped. Then the overall error rate P_E for the reported data can be computed by the following equation:

$$P_E = \sum_{i=n-k+1}^{n} \binom{n}{i} p_e^i (1-p_e)^{n-i}. \tag{8}$$

In Table II, we computed the error rate P_E for various number of message redundant levels. It can be seen that the error rate P_E decreases significantly by increasing the redundancy level. This table also shows that DEAR can increase the delivery ratio of the reported data.

D. Computational Complexity

Computation complexity is determined by computational overhead in recovery of the secret data by using Barycentric Lagrange Interpolation, which is $\mathcal{O}(n)$ for reconstruction of the collected data. If the delivery node only drops the packet without tampering, the algorithm only needs to be implemented once to recover the collected data. However, if the application data server receives modified or corrupted data pieces, it needs to implement the Barycentric Lagrange Interpolation algorithm at most $\binom{n}{k}$ times in the worst case to recover the correct data if the number of tampered components is less than $n-k$. Fortunately, the parameters (k, n) with relative small values are able to decrease the location leakage close to 0, as shown in Table I. Therefore, it enables the application data server to reconstruct the original data in a short time interval. In particular, for $n=25$ and $k=20$, the computer with 2.0GHz processor needs at most approximately 0.053 seconds to reconstruct the original collected data.

VII. CONCLUSION

In this paper, we present a DElay-awaRE (DEAR) secure forwarding scheme for people-centric urban sensing networks. The scheme can preserve the trajectory privacy of the participating users in urban sensing networks. DEAR has the flexibility to provide a trade-off between user privacy and communication delay. Theoretical analysis shows that the proposed scheme can prevent adversaries from correlating identity information with location information of a given reported data. The simulation results show that DEAR can minimize information leakage under the given communication delay constraints. The results also demonstrate that DEAR can achieve a high delivery ratio for the reported data.

REFERENCES

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," in *the 1st Workshop on World-Sensor-Web*, Oct 2006, pp. 1–5.

[2] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing," in *Proceedings of the 2nd Annual International Workshop on Wireless Internet*, 2006, pp. 18–31.

[3] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: Opportunistic and privacy-preserving context collection," *Pervasive Computing*, vol. 5013, pp. 280–297, 2008.

[4] K. L. Huang, S. Kanhere, and W. Hu, "Towards privacy-sensitive participatory sensing," in *Pervasive Computing and Communications, IEEE International Conference on*, March 2009, pp. 1–6.

[5] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "Prisense: Privacy-preserving data aggregation in people-centric urban sensing systems," in *Proceedings of IEEE INFOCOM 2010*, March 2010, pp. 758–766.

[6] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based service," in *Proceeding of IEEE INFOCOM 2008*, March 2008, pp. 547–555.

[7] K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in *Proceeding of INFOCOM 2012*, March 2012, pp. 2399–2407.

[8] S. Gao, J. Ma, W. Shi, and G. Zhan, "Towards location and trajectory privacy protection in participatory sensing," in *Mobile Computing, Applications and Services*, 2011, pp. 381–386.

[9] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *9th Int. Symp. Privacy Enhancing Technologies (PETS10)*, 2005, pp. 88–97.

[10] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, and S. Kanhere, "Privacy-preserving collaborative path hiding for participatory sensing applications," in *Mobile Adhoc and Sensor Systems (MASS), IEEE 8th International Conference on*, Oct 2011, pp. 341–350.

[11] L. Hu and C. Shahabi, "Privacy assurance in mobile sensing networks: Go beyond trusted servers," in *Pervasive Computing and Communications Workshops, 8th IEEE International Conference on*, March 2010, pp. 613–619.

[12] C. Ma, D. Yau, N. Yip, and N. Rao, "Privacy vulnerability of published anonymous mobility traces," *Networking, IEEE/ACM Transactions on*, vol. 21, no. 3, pp. 720–733, June 2013.

[13] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proceeding of IEEE SECON 2009*, June 2009, pp. 1–9.

[14] V. Vukadinovic, O. R. Helgason, and G. Karlsson, "An analytical model for pedestrian content distribution in a grid of streets," *Mathematical and Computer Modelling*, vol. 57(11-12), pp. 2933–2944, June 2013.