Minimum-Latency Data Gathering Scheduling in Multi-Channel Wireless Sensor Networks Using Only Secure Links

Lixin Wang†, Jianhua Yang†, Hanyu Liang‡ and Peng-Jun Wan*

***Abstract*—Many applications of wireless sensor networks (WSNs) are time-critical as well as requiring secure operations, and have serious consequences if the network is compromised. WSNs are often deployed in hostile environments where communication is monitored and the sensor nodes are subject to be compromised or manipulated by adversaries. For such WSNs, it is very important to have secure communications among the sensors. The m-composite key pre-distribution schemes proposed in [3] is one of the most popular mechanisms for communication security of WSNs. With such a security scheme, two nodes within each other's transmission range have a secure link between them if their key rings have at least m keys in common. In this paper, we develop an efficient scheduling algorithm for data gathering on *secure* WSNs. The link between two nearby sensors may not be secure and cannot be used for communication. Such a nature of secure WSNs makes the analysis of any scheduling algorithm for gathering much more challenging than on WSNs that can be modeled as disk graphs. To the best of our knowledge, this is the first paper that develops fast gathering schedules for multihop WSNs where the network topology cannot be modeled as a disk graph.**

I. Introduction

Wireless sensor networks (WSNs) have a wide range of applications for various tasks such as environmental monitoring, real-time traffic monitoring, building safety monitoring, real-time pollution monitoring, and military surveillance, sensing and tracking as well as for emergency disaster relief and distributed measurement of seismic activities. Many such applications of WSNs are time-critical as well as dependent on secure operations of the network. There will be serious consequences if some wireless links are compromised, unreliable, or disrupted due to harsh environments, barriers or shadowing effects among the sensor nodes.

†TSYS School of Computer Science, Columbus State University, GA 31907. Emails: {wang_lixin, yang_jianhua}@columbusstate.edu.

‡School of Computer Science and Engineering, University of New South Wales, New South Wales, Australia. E-mail: hanyuhlv@gmail.com.

*Department of Computer Science, Illinois Institute of Technology, Chicago, Illinois, USA. E-mail: wan@cs.iit.edu.

Usually, WSNs are deployed in hostile environments where data communications are cautiously monitored. The wireless sensor nodes or communication links are subject to be compromised or manipulated by adversaries. On such WSNs, it is very important to secure the data communications among the sensor nodes. Since the sensor nodes have limited resources in terms of computation power, capacity and memory, traditional key management algorithms and security schemes are too complex and very hard to be implemented on WSNs. Many security mechanisms have been proposed to provide secure communications for WSNs [3][4][5][8]. By far, the most popular security mechanism for WSNs is the *m-composite key pre-distribution* mechanism that was proposed in [3]. In the m-composite key pre-distribution scheme, K distinct keys are chosen from a key space at random to form a key pool. A key ring is defined to be a subset of the key pool with t elements. Prior to being deployed, every sensor node uploads a key ring into its memory at random. Two sensor nodes have a secure link between them if and only if they are within each other's transmission range and there are at least m common keys in their key rings. Only secure links can be used for data communication on WSNs with sensitive data. Such WSNs is referred to as *secure WSNs*. Assume that all the sensor nodes have uniform transmission range r. A secure WSN can be modeled as a subgraph of the r-disk graph over all the sensor nodes.

Data gathering is a primitive communication task in which all nodes send their individual messages to a distinguished sink node without data aggregation or combination. Since some essential data of each sensor node often need be sent separately to the sink node on a WSN for security purposes. For example, the data contains sensitive information that can only be known by the sink, or the network traffic are encrypted and the intermediate sensor nodes are unable to decrypt the packets, etc. Therefore, data gathering is a very important and essential operation and widely used on various applications of WSNs for the sink node to collect data separately from all

978-1-7281-5212-7/19/$31.00 ©2019 IEEE
DOI 10.1109/MSN48538.2019.00042

other sensor nodes in the network.

The problem of computing a data gathering schedule with minimum latency in multihop WSNs is referred to as **M**inimum-**L**atency **G**athering **S**chedule (**MLGS**). Under the assumption that all the communication links are secure, **MLGS** in multihop WSNs has been well studied under both the protocol interference model and the physical interference model (see [1][2][13][14][17] and all the references therein).

The main purpose of this paper is to conduct analytic and algorithmic studies for minimizing communication latency of data gathering in *secure* WSNs by utilizing multiple channels under the protocol interference model described below: Each sensor node has a uniform transmission radius (normalized to one), and a uniform interference radius $\rho = 1$. Thus, if both the secure and insecure links are used for communication, the network topology is a unit-disk graph (UDG). The network topology of the *secure* WSN is a subgraph of this UDG. We further assume all the communications proceed in synchronous time-slots and each sensor can transmit at most one packet of a fixed size in each time-slot.

Let λ denote the number of available channels, V the set of all the nodes in the WSN. Denoted by G_u the UDG over V. Two nodes u and v have a *secure* link between them if and only if $(u, v) \in E(G_u)$ and they have at least m common keys in their key rings, where $E(G_u)$ denotes the edge set of G_u. Denoted by $G_{\rm sec}$ the secure WSN over V. Note that two nodes in V may not have a *secure* link between them even if they are very close to each other, and thus they cannot have direct communication on $G_{\rm sec}$. As a result, a node in $G_{\rm sec}$ may have many neighbors that are independent with one another. It is well-known that any node of G_u has at most five independent neighbors in G_u. Moreover, most of the geometric properties that hold on UDGs do not hold on $G_{\rm sec}$ any more. Therefore, these geometric properties of UDGs cannot be used in the analysis for any data gathering scheduling algorithms proposed for $G_{\rm sec}$. Such natures of $G_{\rm sec}$ make the analysis of any scheduling algorithms much more challenging than on the WSNs that can be modeled as a disk graph. As a matter of fact, all the existing scheduling algorithms for **MLGS** based on UDGs are no longer suitable for $G_{\rm sec}$.

In this paper, we address this challenge and develop an efficient approx. algorithm for **MLGS** in *secure* WSNs, referred to as **MLGS-Sec**. To the best of our knowledge, this is the first work that develops fast data gathering schedules for multihop WSNs where the network topology cannot be modeled as a disk graph.

The remaining of this paper is organized as follows. In Section II, we give a literature review for some related work. In Section III, we introduce some preliminaries needed to present the scheduling algorithm for data gathering. In Section IV, we develop an efficient approx. algorithm for MLGS-Sec that produces a fast gathering schedule. Finally, we conclude this paper, discuss some future research directions and present several open problems in this area in Section V.

II. Related Work

When all the links are assumed to be secure, MLGS of multihop WSNs has been well studied under both the protocol interference model and the physical interference model [1][2][13][14][17]. Under the protocol interference model, Bermond et al. [1] proved the NP-hardness of MLGS and proposed an algorithm for MLGS that achieves 4-approx. when the network topology can be modelled as a UDG. Bonifaci et al. [2] developed a greedy algorithm for MLGS and proved it to be 4-approx. in general and 3-approx. when the network topology can be modelled as a UDG. When the interference radius equals the transmission radius, Zhu et al. [17] proposed a heuristic algorithm for MLGS that achieves $(1 + 1/(k + 1))$-approx., where k is a constant integer. By far, the best known approx. algorithm for MLGS was proposed by Wan et al. [14] that focused on how to utilize the multiple channels to speed up four group communications including broadcast, aggregation, gathering, and gossiping. For MLGS, when the sensor nodes have uniform interference radius ρ that is at least the transmission radius, [14] proposed an efficient scheduling algorithm with approx. ratio at most $2\lceil\beta_\rho/\lambda\rceil$, where λ is the number of available channels and β_ρ denote the maximum number of points in a half-disk of radius $\rho + 1$ whose mutual distances are greater than one.

Under the physical interference model, the best known algorithm for MLGS is proposed in Wan et al. [13]. This paper developed short communication schedules for broadcast, data aggregation, data gathering, and gossiping subject to physical interference. Under mild assumptions, all of the communication schedules for those four group communications have constant approx. bounds. For MLGS, [13] proposed an efficient scheduling algorithm with approx. ratio at most a constant $2\beta_\rho$.

III. Preliminaries

In this section, we introduce some preliminaries needed for presenting the data gathering scheduling algorithm to be proposed.

For each $0 \le i \le m - 1$, let b_i be the probability that two sensor nodes have *exactly* i common keys in their key rings. Since the key ring of the second sensor contains i keys that

are also contained in the key ring of the first sensor, and $t-i$ keys from the remaining $K-t$ keys that are not in the key ring of the first sensor, we have

$$b_i = \left(\begin{array}{c} t \\ i \end{array} \right) \left(\begin{array}{c} K-t \\ t-i \end{array} \right) \diagup \left(\begin{array}{c} K \\ t \end{array} \right).$$

Let E denote the event that two nodes have at most $m-1$ common keys in their key rings, E' the event that two nodes have at least m common keys in their key rings. Let q, p be the probability of the events E, E', respectively. Clearly,

$$q = \sum_{i=0}^{i=m-1} b_i, \ and$$
$$p = 1 - q.$$

Appropriate values for the parameters K and t can be chosen so that we can have a desired probability p for two sensor nodes having at least m common keys in their key rings. In order for the secure WSN to be connected, the values for both K and t should appropriately be chosen so that the probability p is large enough. Therefore, it is natural to assume that the values for both K and t can appropriately be chosen so that the percentage of the insecure links among all the links incident to any sensor node is at most γ, where γ is a parameter to be used in this paper.

Given an undirected graph $G = (V, E)$ with $|V| = n$. Let s be a fixed node in V. The subgraph of G induced by a subset $U \subseteq V$ is denoted by $G[U]$. $\delta(G)$ and $\Delta(G)$ respectively represent the minimum and maximum degrees of G. $\alpha(G)$ and $\chi(G)$ respectively represent the independent number and chromatic number of G. The *inductivity* of the graph G is defined as follows:

$$\delta^*(G) = \max_{U \subseteq V} \delta(G[U]).$$

The square of a graph G, denoted by G^2, is the graph over V on which for any $u, v \in V$, (u, v) is an edge on G^2 if and only if u and v are at most two hop away on G. The *depth* of a node v on G *with respect to* s is the graph hop distance from s to v. The *radius of* a graph G *with respect to* s, denoted by $R(G)$, is the maximum graph hop distance from s to all other nodes in V. For each $0 \leq i \leq R(G)$, let L_i denote the set of all the nodes of depth i and is referred to as the i-th layer w.r.t. the graph radius.

A subset U of V is an *independent set* of G if there is no edge between any two nodes in U. If U is an independent set of G but $U \cup \{x\}$ is no longer an independent set for any $x \in V \diagdown U$, then U is called a *maximal independent set* (MIS) of G. Any vertex ordering $v_1, v_2, \cdots, v_n$ of V induces an MIS U in the first-fit manner [14]. A subset $U \subseteq V$ is a *dominating set* of G if every node in $V \diagdown U$ is a neighbor of some node in U. If U is a dominating set of G and the induced subgraph $G[U]$ by U is connected, then U is called a *connected dominating set* (CDS) of G. *A vertex coloring* of G is an assignment of colors to the nodes in V such that adjacent nodes receive different colors. Clearly, computing a vertex coloring of G is equivalent to partitioning the nodes in V into different independent sets of G. Consider a vertex ordering $v_1, v_2, \cdots, v_n$ of V. For each $1 \leq i \leq n$, denote by $N_{\prec}(v_i)$ the set of all preceding neighbors of v_i in this ordering of the nodes in V. That is,

$$N_{\prec}(v_i) = \{v_j : 1 \leq j < i, \ v_j \in N(v_i)\},$$

where $N(v_i)$ denotes the set of all neighbors of the node v_i.

The first-fit coloring algorithm in the ordering $v_1, v_2, \cdots, v_n$ use colors represented by natural numbers $1, 2, 3, \cdots$ [14]. Clearly, this vertex coloring uses at most $1 + max_{1<i\leq n} |N_{\prec}(v_i)|$ colors. The value of $max_{1<i\leq n} |N_{\prec}(v_i)|$ is referred to as the *inductivity* of *the vertex ordering* $v_1, v_2, \cdots, v_n$ [14].

Given a positive integer $d > 0$. A subset U of V is said to be a *distance-d independent set* if and only if the pairwise Euclidean distances of the nodes in U are larger than d. It is easy to see that U is a (maximal) *distance-d independent set* of G if and only if U is a (maximal) *independent set* of G^d. For any $d > 0$, a *distance-d coloring* of the nodes in U is an assignment of colors to the nodes in U such that any pair of nodes with distance at most d are assigned with different colors [14].

Next, we introduce a simple lemma from [6] that partitions a half disk of radius two into 14 small subregions, each of which is of diameter at most one. This lemma is proved in [6].

Lemma 1. *Any half disk with radius equal to two can be partitioned into* 14 *small subregions, each of which has diameter at most one (see Fig. 1 in [6]).*

The next lemma gives an upper bound on the number of independent nodes in $G_{\rm sec}$ that can be contained in any of the 14 small subregions shown in Fig. **??**.

Lemma 2. *Let S denote any of the 14 small subregions described in Lemma 1 with diameter at most one. For any independent set I of the secure WSN $G_{\rm sec}$, we have $|S \cap I| \leq \gamma\Delta(G_u) + 1$, where G_u is the unit-dsik graph over V.*

Proof: If $S \cap I = \varnothing$, the lemma is clearly true. Next we assume that $|S \cap I| \geq 1$. Pick a node $u \in S \cap I$. For any $v \in S \cap (I \diagdown \{u\})$, we have $\|uv\| \leq 1$ since both u and v

belong to S and the diameter of S is at most S. Thus, there is an edge between u and v in the unit disk graph G_u. Since $u, v \in I$, they are independent in the secure network G_{se}. Thus, the link (u, v) on the unit disk graph G_u is not secure. Based on our assumption described above, the total number of insecure links incident to u is at most $\gamma\Delta(G_u)$, where γ is an upper bound on the percentage of the insecure links among all the links incident to any sensor node in V. Thus, $S \cap (I \setminus \{u\})$ contains at most $\gamma\Delta(G_u)$ nodes in I. Therefore, $|S \cap I| \leq \gamma\Delta(G_u) + 1$.

This completes the proof of the lemma. ■

For any independent set I of a secure network $G_{\rm sec}$, the following lemma gives an upper bound for the inductivity of the induced subgraph $G^2_{\rm sec}[I]$ of the square graph $G^2_{\rm sec}$ induced by I.

Lemma 3. *For any independent set I of a secure network $G_{\rm sec}$, we have*

$$\delta^*(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 11.$$

Proof: First we prove that $\delta(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 11$. Let $v \in I$ be the bottom-most node in the deployment region of the network. It is sufficient to prove that the degree of v in the square graph $G^2_{\rm sec}[I]$ induced by I is at most $14\gamma\Delta(G_u) + 11$. Since $v \in I$ is the bottom-most node, all neighbors of v in $G^2_{\rm sec}[I]$ is contained in the top half-disk centered at v with radius two. By Lemma 1, the top half-disk centered at v with radius two can be partitioned into 14 small subregions as shown in Fig. **??**. Let S denote any of these 14 small subregions. We have two cases:

Case 1. S is one of the three 60^o-sectors in the inner disk of radius one with labels 1, 2 or 3. In this case, $S \cap (I \setminus \{v\})$ contains at most $\gamma\Delta(G_u)$ nodes in I since $v \in S \cap I$.

Case 2. S is one of the small subregions in the two annuli with labels $4, 5, \cdots$, or 14. In this case, we $|S \cap I| \leq \gamma\Delta(G_u) + 1$ by Lemma 2. Thus, the independent set I contains at most

$$11(\gamma\Delta(G_u) + 1) + 3\gamma\Delta(G_u) = 14\gamma\Delta(G_u) + 11$$

nodes in the top half-disk centered at v with radius two.

Therefore, the degree of v in $G^2_{\rm sec}[I]$ is at most $14\gamma\Delta(G_u) + 11$. Hence, $\delta(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 11$.

Next, we prove that $\delta^*(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 11$.

Note that I is an independent set of the secure network $G_{\rm sec}$. For any subset U of I, U itself is an independent set of $G_{\rm sec}$. The subgraph of $G^2_{\rm sec}[I]$ induced by U is $G^2_{\rm sec}[U]$. Therefore, $\delta(G^2_{\rm sec}[U]) \leq 14\gamma\Delta(G_u) + 11$. Since U is an arbitrary subset of I, we have $\delta^*(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 11$.

This completes the proof of the lemma. ■

The following corollary can be easily verified by using Lemma 3 above:

Corollary 4. *Any independent set I of a secure network $G_{\rm sec}$ can be partitioned into at most $(14\gamma\Delta(G_u) + 12)$* distance-2 *independent sets of $G_{\rm sec}$. That is, a* distance-2 coloring *of the nodes in I uses at most $(14\gamma\Delta(G_u) + 12)$ colors.*

Proof: By Lemma 3, we have

$$\chi(G^2_{\rm sec}[I]) \leq 1 + \delta^*(G^2_{\rm sec}[I]) \leq 14\gamma\Delta(G_u) + 12. \quad (1)$$

Thus, the square graph $G^2_{\rm sec}[I]$ induced by I is $(14\gamma\Delta(G_u) + 12)$-colorable.

Given a proper *distance-2* coloring of the graph $G^2_{\rm sec}[I]$ that uses at most $14\gamma\Delta(G_u) + 12$ colors. For each $1 \leq i \leq 14\gamma\Delta(G_u)+12$, let U_i be the subset of nodes in I that receive the i-th color in this *distance-2* coloring of $G^2_{\rm sec}[I]$. Since U_i is an independent set of the square graph $G^2_{\rm sec}[I]$ induced by I, the graph hop-distance on the secure network $G_{\rm sec}$ between any pair of nodes in U_i is greater than 2. Therefore, I can be partitioned into at most $(14\gamma\Delta(G_u) + 12)$ *distance*-2 independent sets of $G_{\rm sec}$.

This completes the proof of the corollary. ■

IV. A Fast Gathering Scheduling for Secure WSNs

In this section, we adopt the data gathering scheduling algorithm we developed in our prior work [14]. Let s denote the sink node of data gathering.

We first we introduce a spanning tree T of $G_{\rm sec}$ rooted at s constructed from the CDS presented in our prior work [14]. This rooted spanning tree is referred to as a dominating tree in [14] and will be used for routing in data gathering.

The data gathering scheduling algorithm presented in [14] employed a multi-labelling algorithm to assign multiple labels to each edge in T. This multi-labelling algorithm works as follows:

Consider a vertex ordering $v_1, v_2, \cdots, v_{n-1}$ of $V \setminus \{s\}$ in the descending order of their depths in T (ties can be broken arbitrarily) with $n = |V|$. Thus, v_1 belongs to the bottom-most layer of T (see Fig. 3 in [14]). For convenience, let $s = v_n$. For $1 \leq i \leq n-1$, we assign the j-th edge in the tree path from the root node s to the sensor node v_i with the label $2(i-1) + j$, where $1 \leq j \leq M$ with M being the length of the tree path from s to v_i. Therefore, when $i = 1$, the edges of the path from s to v_1 in T are labelled respectively as $1, 2, 3, \cdots$. An example of multi-labels that are assigned to each edge of the tree T is given in [14] (see Fig. 3 in [14]). From the figure, we can see that the number of descendents of the sensor node v_i in T (including v_i itself) is the same as

the number of the integer labels assigned to an edge between the node v_i and its parent node equals. Furthermore, if v_i is a dominator (black node) in T, all labels assigned to the edge between v_i and its parent node are even numbers. But if v_i is connector (white node) in T, all labels assigned to the edge between v_i and its parent node are odd numbers. Also, for any two adjacent layers in the dominating tree T, all edges across these two adjacent layers are assigned with different label values, one layer having odd labels and the other layer having even labels. The number $2n-3$ is the largest label assigned to the edges in T. An argument of this claim was given in [14] (see Section 6 of [14] for details).

Let $\overrightarrow{T}$ denote the *inward arborescence with respect to* s generated from T. For each $1 \leq k \leq 2n-3$, let

$$E_k = \{the\ set\ of\ the\ edges\ in\ the\ tree\ T\ that\ received\ a\ label\ k\},\ and$$
$$A_k = \{the\ set\ of\ the\ links\ in\ the\ inward\ s\text{-}arborescence\ \overrightarrow{T}\ that\ received\ a\ label\ k\}.$$

We claim that for every $1 \leq k \leq 2n-3$, all the links in A_k are disjoint. This claim is verified as follows: If the label k is an odd number, all the receiving endpoints of links in A_k are dominators. If the label k is an even number, all the transmitting endpoints of links in A_k are dominators. Furthermore, for each $1 \leq k \leq 2n-3$, every dominator (black node) is incident to at most one link in A_k. Therefore, all the links in A_k are disjoint for every $1 \leq k \leq 2n-3$.

Next, we present the data gathering scheduling algorithm for the secure WSN $G_{\rm sec}$. The data gathering schedule are respectively partitioned in $2n-3$ rounds. For each $1 \leq k \leq 2n-3$, the k-th round is dedicated to schedule the links in the set A_k. The data gathering scheduling starts with the link set A_{2n-3}, and then followed by the link set A_{2n-2}. Finally, the links in the set A_1 will be scheduled. The link sets are sequentially scheduled in the following order:

$$A_{2n-3},\ A_{2n-2},\ \cdots,\ A_2,\ A_1.$$

For each $1 \leq k \leq 2n-3$, let I_k denote the set of the dominator endpoints of the links in A_k. The round for the links in A_k is scheduled as follows:

- First we compute a *distance-2 coloring* of the independent set I_k of the dominator endpoints in the first-fit manner as described in Section III;
- Then each link in A_k whose dominator endpoint assigned with the i-th color by the above distance-2 coloring is scheduled to transmit in the $\lceil i/\lambda \rceil$-th time-slot of the k-th round at channel i if $i \leq \lambda$, or $i \bmod \lambda$ if $i > \lambda$. The available channels are respectively represented by positive integers $1, 2, \cdots, \lambda$.

The following theorem gives the total latency and approx. ratio of the data gathering schedule produced by the algorithm described above.

Theorem 5. *The total latency of the data gathering schedule produced by above scheduling algorithm is at most* $\lceil (14\gamma\Delta(G_u)+12)/\lambda \rceil (2n-3)$. *The approx. ratio of the data gathering schedule produced by this algorithm is at most* $2\lceil (14\gamma\Delta(G_u)+12)/\lambda \rceil$.

Proof: By Corollary 4, a *distance-2 coloring* of the nodes in I_k uses at most $(14\gamma\Delta(G_u)+12)$ colors. Totally, there are $2n-3$ rounds for the data gathering operation to be completed. Therefore, the total latency of the data gathering schedule produced by the scheduling algorithm described above is at most $\lceil (14\gamma\Delta(G_u)+12)/\lambda \rceil (2n-3)$, where λ is the total number of channels available on the network.

Next, we prove that $n-1$ is a lower bound for the minimum data gathering latency, i.e. the minimum number of time-slots is required for a complete data gathering operation. For data gathering, $n-1$ nodes (other than the sink node s) must send their packets separately to the sink node s. Thus, $n-1$ packets must be transmitted/forwarded to the sink node separately. Note that the sink node can only receive one packet in each time-slot. Therefore, at least $n-1$ time-slots are required for the data gathering operation to be completed. Thus, $n-1$ is a lower bound for the minimum data gathering latency.

Hence, the approx. ratio of the data gathering schedule produced by the algorithm described above is at most $2\lceil (14\gamma\Delta(G_u)+12)/\lambda \rceil$. ■

Note that if the maximum degree $\Delta(G_u)$ is bounded, then our data gathering scheduling algorithm proposed in this paper achieves constant approx.

V. Conclusion and Future Work

In this paper, we proposed an efficient approx. algorithm for MLGS-Sec on *secure* WSNs. On such a secure WSN, two sensor nodes that are very close to each other may not have a secure link between them. As a result, they cannot have direct communications on the secure WSN. Such a nature of secure WSNs makes it much more challenging for the analysis of data gathering scheduling algorithms than on WSNs that can be modeled as disk graphs. To the best of our knowledge, this is the first paper that develops fast data gathering schedules for *secure* WSNs. This is also the first work that proposed efficient scheduling algorithms for data gathering on multihop WSNs

where the network topology cannot be modeled as a disk graph. When the maximum degree of the unit-disk graph over all the sensor nodes is bounded, the data gathering schedule produced by the scheduling algorithm presented in this paper for *secure* WSNs achieves constant approx.

For future research directions in this area, we present the following open problems for data gathering scheduling on WSNs: Under the protocol interference model, when the sensor nodes have uniform interference radius ρ greater than or equal to the transmission radius, [14] proposed an efficient scheduling algorithm for data gathering, with approx. ratio at most $2\lceil\beta_\rho/\lambda\rceil$, where λ is the number of available channels for the network and β_ρ denote the maximum number of points in a half-disk of radius $\rho+1$ whose mutual distances are greater than one. We believe that the approx. ratio of this algorithm can be improved. For *secure* WSNs discussed in this paper, whether there exist constant-approx. algorithms to produce fast data gathering schedules is still open on such networks when the maximum degree of the unit-disk graph over all the sensor nodes can be arbitrarily large.

Acknowledgement*: This work of Dr. Peng-Jun Wan was supported in part by the National Science Foundation of USA under grant CNS-1526638.*

REFERENCES

[1] J.-C. Bermond, J. Galtier, R. Klasing, N. Morales, and S. Perennes, Hardness and approx. of gathering in static radio networks. *Proceedings FAWN06* (2006).

[2] V. Bonifaci, P. Korteweg, A. Marchetti-Spaccamela, and L. Stougie, An approx. Algorithm for the Wireless Gathering Problem. *Proceedings of SWAT* (2006), pp. 328-338.

[3] Chan, H., Perrig, A., and Song, D.: Random key predistribution schemes for sensor networks, in Proceedings of the 2003 *IEEE Symposium on Security and Privacy*, May 11-14 2003, pp. 197–213.

[4] Du, W., Deng, J., Han, Y. S., and Varshney, P. K.: A pairwise key predistribution scheme for wireless sensor networks. In Proceedings of the 10th *ACM Conference on Computer and Communications Security* (CCS '03), 2003.

[5] Eschenauer, L. and Gligor, V. D.: A key-management scheme for distributed sensor networks, in Proceedings of the 9th *ACM Conference on Computer and Communications Security*, November 18-22 2002, pp. 41–47.

[6] Huang, C.-H., Wan, P.-J., Jia, X., Du, H., and Shang, W.: Minimum Latency Broadcast Scheduling in Wireless Ad Hoc Networks, *IEEE INFOCOM* 2007.

[7] Huang, S.C.-H., Wan, P.-J., Vu, C. T., Li, Y., and Yao, F.: Nearly Constant approx. for Data Aggregation Scheduling in Wireless Sensor Networks, *IEEE INFOCOM* 2007.

[8] Liu, D. and Ning, P. Establishing pairwise keys in distributed sensor networks. In Proceedings of the 10th *ACM Conference on Computer and Communications Security* (CCS '03), 2003.

[9] Mao, G. and Anderson, B.: Connectivity of large wireless networks under a general connection model. *Information Theory, IEEE Transactions on,* Vol. 59.3: 1761-1772 (2013).

[10] Pietro, R. D., Mancini, L., Mei, A., Panconesi, A., and Radhakrishnan, J.: Connectivity properties of secure wireless sensor networks, in Proceedings of the 2004 *ACM Workshop on Security of Ad Hoc and Sensor Networks* (SASN '04), October 25 2004.

[11] Wan, P.-J., Huang, C.-H., Wang, L., Wan, Z.-Y., and Jia, X.: Minimum-Latency Aggregation Scheduling in Multihop Wireless Networks, *ACM MOBIHOC* 2009.

[12] Wan, P.-J., Wang, Z., Du, H., Huang, S. C.-H., and Wan, Z.: First-Fit Scheduling for Beaconing in Multihop Wireless Networks, *IEEE INFOCOM* 2010.

[13] Wan, P.-J., Wang, L., and Frieder, O.: Fast Group Communication in Multihop Wireless Networks Subject to Physical Interference, *IEEE MASS* 2009.

[14] P.-J. Wan, Z. Wang, Z. Wan, S. C.-H. Huang, and H. Liu: Minimum-Latency Schedulings for Group Communications in Multi-channel Multihop Wireless Networks, *WASA* 2009.

[15] Wan, P.-J., Wang, L., and Yao, F.: Two-Phased approx. Algorithms for Minimum CDS in Wireless Ad Hoc Networks, *IEEE ICDCS 2008*, pp. 337-344.

[16] Yi, C.W., Wan, P.J., Lin, K.W. and Huang, C.H., 2006, November. WSN18-5: asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with unreliable nodes and links. In *IEEE Globecom* 2006 (pp. 1-5). *IEEE.*

[17] X. Zhu, B. Tang, and H. Gupta: Delay efficient data gathering in sensor networks, *International Conference on Mobile Ad-Hoc and Sensor Networks,* 2005 Dec 13 (pp. 380-389). Springer, Berlin, Heidelberg.