

Distinct difference configurations and Wireless Sensor Networks

Simon R. Blackburn

Joint work with:

Tuvi Etzion, Keith M. Martin, Maura B. Paterson

Royal Holloway, University of London

12th May 2009



- 1 WSN Key predistribution
- 2 Distinct difference configurations
- 3 Constructions
- 4 Bounds
- 5 Related models

Wireless Sensor Networks

A **Wireless Sensor Network** consists of:

- A large number of devices (nodes);
- Each node has low computational power;
- A node can sense something;
- A node can communicate wirelessly with its neighbours.

Wireless Sensor Networks

A **Wireless Sensor Network** consists of:

- A large number of devices (nodes);
- Each node has low computational power;
- A node can sense something;
- A node can communicate wirelessly with its neighbours.

Recommended for applications in military, disaster recovery, and scientific monitoring situations.

The main question

Question

How do nodes form a secure connected network?

The main question

Question

How do nodes form a secure connected network?

- The answer depends on the application.

The main question

Question

How do nodes form a secure connected network?

- The answer depends on the application.
- If we don't know how our nodes will be distributed: use Eschenauer–Gligor.

The main question

Question

How do nodes form a secure connected network?

- The answer depends on the application.
- If we don't know how our nodes will be distributed: use Eschenauer–Gligor.
- What happens if we know how our sensors will be arranged?

Our model

We assume:

- There is a node at all positions $(x, y) \in \mathbb{Z}^2$.
- A pair of nodes can communicate when they are within **distance d** .
- Nodes cannot use public key cryptography.
- Nodes can be preloaded with **m secret keys**.

Our model

We assume:

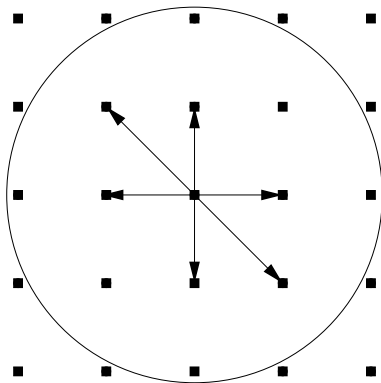
- There is a node at all positions $(x, y) \in \mathbb{Z}^2$.
- A pair of nodes can communicate when they are within **distance d** .
- Nodes cannot use public key cryptography.
- Nodes can be preloaded with **m secret keys**.

Issues we are interested in:

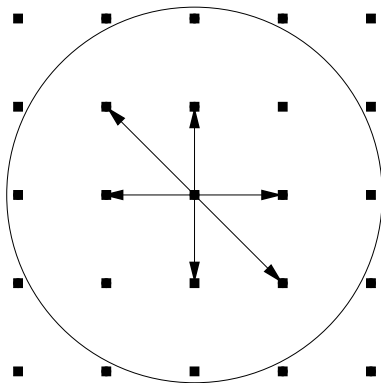
- Maximize the number of nodes that can communicate securely.
- Minimize the number of keys per node.
- Use lots of keys in case nodes are compromised.



Our model



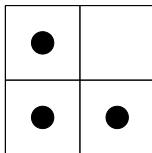
Our model



We want at most one key shared by any pair of nodes.

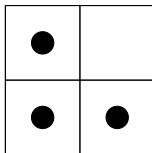
Distinct Difference Configurations

An example with 3 dots (**we will use this later**):



Distinct Difference Configurations

An example with 3 dots (*we will use this later*):



Important property

Any two shifts of a distinct difference configuration have at most one dot in common.

Distinct Difference Configurations

Definition

A **distinct difference configuration with m dots** is a set $\{v_1, v_2, \dots, v_m\} \subseteq \mathbb{Z}^2$ such that the differences $v_i - v_j$ for $i \neq j$ are all distinct.

We abbreviate the above to $DD(m)$.

Distinct Difference Configurations

Definition

A **distinct difference configuration with m dots** is a set $\{v_1, v_2, \dots, v_m\} \subseteq \mathbb{Z}^2$ such that the differences $v_i - v_j$ for $i \neq j$ are all distinct.

We abbreviate the above to $DD(m)$.

So $\{(0, 0), (1, 0), (0, 1)\}$ is a $DD(3)$ with differences given by:

	(0, 0)	(1, 0)	(0, 1)
(0, 0)		(1, 0)	(0, 1)
(1, 0)	(-1, 0)		(-1, 1)
(0, 1)	(0, -1)	(1, -1)	

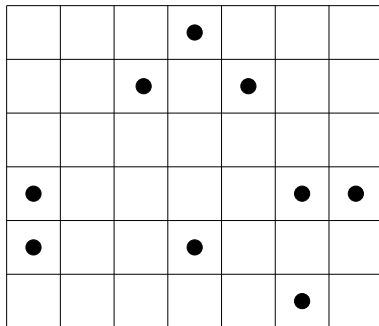
Distinct Difference Configurations

The following is a DD(9):

			●			
		●		●		
●					●	●
●			●			
					●	

Distinct Difference Configurations

The following is a DD(9):



All pairs of dots are at distance at most 7. This is the largest such example.

Distinct Difference Configurations

Definition

A **distinct difference configuration with m dots of diameter d** is a $DD(m)$ such that $|v_i - v_j| \leq d$ for all i, j .

So any pair of dots is at distance d or less.

Distinct Difference Configurations

Definition

A **distinct difference configuration with m dots of diameter d** is a $DD(m)$ such that $|v_i - v_j| \leq d$ for all i, j .

So any pair of dots is at distance d or less.

- We abbreviate the above to $DD(m, d)$.
- Our running example is a $DD(3, \sqrt{2})$.

How are the configurations used?

- Shift the configuration over the entire grid.
- For each shift $s \in \mathbb{Z}^2$, generate a key k_s .
- Give k_s to nodes under the dots of the shift: in other words at positions $s + v_i$, $i = 1, 2, \dots, m$.

How are the configurations used?

- Shift the configuration over the entire grid.
- For each shift $s \in \mathbb{Z}^2$, generate a key k_s .
- Give k_s to nodes under the dots of the shift: in other words at positions $s + v_i$, $i = 1, 2, \dots, m$.

In our DD(3) example:

- A node X at position (x, y) gets 3 keys: $k_{(x,y)}$, $k_{(x-1,y)}$, $k_{(x,y-1)}$;
- Each key is shared with 2 other nodes;
- X shares a key with 6 nodes, at positions:
 $(x+1, y)$, $(x, y+1)$, $(x-1, y)$, $(x-1, y+1)$, $(x, y-1)$, $(x+1, y-1)$.
- All shared keys are with nodes within distance $\sqrt{2}$ or less.

Performance

In general, when a $DD(m, d)$ is used:

- A node receives m keys.
- Each key is shared with $m - 1$ other nodes;
- A node shares a key with $m(m - 1)$ nodes;
- These $m(m - 1)$ nodes are at distance at most d .

Performance

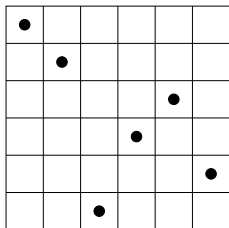
In general, when a $DD(m, d)$ is used:

- A node receives m keys.
- Each key is shared with $m - 1$ other nodes;
- A node shares a key with $m(m - 1)$ nodes;
- These $m(m - 1)$ nodes are at distance at most d .

Main combinatorial question

When d is fixed, how big can m be?

Some constructions



Definition

An $n \times n$ **Costas array** is a $DD(n)$ contained in $\{0, 1, \dots, n-1\}^2$ with no pair of dots parallel with the x -axis, and no pair of points parallel with the y -axis.

Costas arrays

There exist several constructions of Costas arrays.

For example let p be a prime. Let α be a primitive root mod p .

Construction

Let $n = p - 2$. Put a dot in position (i, j) when $\alpha^{i+1} + \alpha^{j+1} = 1$. Then the dots form an $n \times n$ Costas array.

Costas arrays

There exist several constructions of Costas arrays.

For example let p be a prime. Let α be a primitive root mod p .

Construction

Let $n = p - 2$. Put a dot in position (i, j) when $\alpha^{i+1} + \alpha^{j+1} = 1$. Then the dots form an $n \times n$ Costas array.

So when m is large, there exists a $DD(m)$ contained in an $n \times n$ square with $n \approx m$.

A lower bound on m

Costas arrays give:

Theorem

There exists a $DD(m, d)$ with $m = \frac{1}{\sqrt{2}}d - o(d) \approx 0.70711d$.

Proof: Place an $n \times n$ square in a circle of diameter d . □

A lower bound on m

Costas arrays give:

Theorem

There exists a $\text{DD}(m, d)$ with $m = \frac{1}{\sqrt{2}}d - o(d) \approx 0.70711d$.

Proof: Place an $n \times n$ square in a circle of diameter d . □

In fact we have an explicit construction such that:

Theorem

There exists a $\text{DD}(m, d)$ with $m \approx 0.80795d$.

A corresponding upper bound

Theorem

A $DD(m, d)$ must satisfy $m \leq (\sqrt{\pi}/2)d - o(d) \approx 0.88623d$.

A corresponding upper bound

Theorem

A $DD(m, d)$ must satisfy $m \leq (\sqrt{\pi}/2)d - o(d) \approx 0.88623d$.

Sketch proof:

The convex hull of the $DD(m, d)$ has area at most $(\pi/4)d^2$.

Cover the convex hull with small circles of radius $\ell \approx d^{2/3}$ whose centers lie in \mathbb{Z}^2 .

There are w small circles where $w \approx (\pi/4)d^2$.

Each circle contains a points in \mathbb{Z}^2 , where $a \approx \pi\ell^2$.

Write m_i for the number of points of the $DD(m, d)$ in the i th small circle; the mean of the m_i is $\mu = am/w$. Then

$$w\mu^2 \approx w(\mu^2 - \mu) \leq \sum_{i=1}^w m_i(m_i - 1) \leq a(a - 1) \leq a^2.$$

A new distance measure

A $\overline{DD}(m, d)$ is a $DD(m)$ in which every pair of dots are at **Manhattan distance** at most d .

Our running example is a $\overline{DD}(3, 2)$.

A new distance measure

A $\overline{\text{DD}}(m, d)$ is a $\text{DD}(m)$ in which every pair of dots are at **Manhattan distance** at most d .

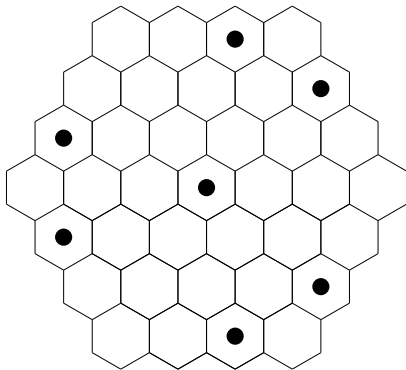
Our running example is a $\overline{\text{DD}}(3, 2)$.

Theorem

There exists a $\overline{\text{DD}}(m, d)$ with $m = (1/\sqrt{2})d - o(d)$. Moreover, in any $\overline{\text{DD}}(m, d)$ we have that $\overline{\text{DD}}(m, d) \leq (1/\sqrt{2})d + o(d)$.

A new grid

A $DD^*(m)$ is a set of vectors **in the hexagonal grid** whose differences are all distinct.



The hexagonal grid

If all pairs of dots are within Euclidean distance d , we have a $DD^*(m, d)$.

Theorem

There exists a $DD^(m, d)$ with $m = 0.86819d - o(d)$. In any $DD^*(m, d)$ we have that $\overline{DD}(m, d) \leq 0.95231d + o(d)$.*

The hexagonal grid

If all pairs of dots are within Euclidean distance d , we have a $DD^*(m, d)$.

Theorem

There exists a $DD^(m, d)$ with $m = 0.86819d - o(d)$. In any $DD^*(m, d)$ we have that $\overline{DD}(m, d) \leq 0.95231d + o(d)$.*

Open Problem

Close this gap.

Hexagonal distance

If we replace Euclidean distance by **hexagonal distance** we call the resulting object a $\overline{DD}^*(m, d)$.

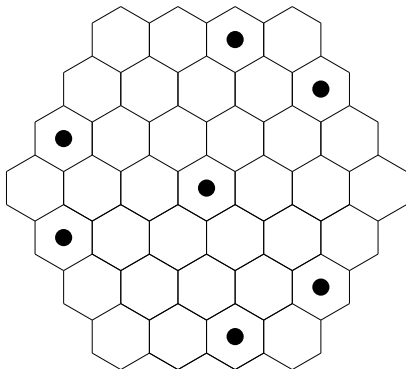
Theorem

There exists a $\overline{DD}^(m, d)$ with $m = 0.79444d - o(d)$. In any $\overline{DD}^*(m, d)$ we have that $\overline{DD}(m, d) \leq 0.86603d + o(d)$.*

Honeycomb arrays

Definition (Golomb and Taylor 1984)

A **honeycomb array of radius r** is a $DD^*(2r + 1)$ contained in a hexagonal sphere of radius r , with the property that there is exactly one dot in every 'row', where 'rows' go in three directions.



Honeycomb arrays

Honeycomb arrays are known to exist for $r = 0, 1, 3, 4, 7, 10, 13$ and 22 .

Theorem (Anastasia Panoui, 2009)

This list is complete for $r \leq 13$.

Honeycomb arrays

Honeycomb arrays are known to exist for $r = 0, 1, 3, 4, 7, 10, 13$ and 22 .

Theorem (Anastasia Panoui, 2009)

This list is complete for $r \leq 13$.

A Honeycomb array is a $\overline{DD}^*(m, d)$ where $m = 2r + 1$ and $d = 2r$.
But we know that $m \leq 0.86603d + o(d)$.

So there are only finitely many honeycomb arrays!

Theorem

Honeycomb arrays of radius r do not exist when $r \geq 644$.

Some links

This talk will appear soon on my homepage:

<http://www.ma.rhul.ac.uk/sblackburn>

Our preprint 'Two-dimensional patterns with distinct differences – Constructions, Bounds and Maximal Anticodes' is available at:

<http://arxiv.org/abs/0811.3832>

The following preprint explores other combinatorial properties motivated by our key predistribution scheme:

<http://arxiv.org/abs/0811.3896>

