



Key
Redistribution

Cichoń,
Gołębiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

From Key Predistribution to Key Redistribution

Jacek Cichoń, Zbigniew Gołębiewski,
Mirosław Kutyłowski

Wrocław University of Technology
FRONTS, 7th Framework Programme, contract 215270

ALGOSENSORS 2010, Bordeaux, 5.07.2010



Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Devices

- weak computationally
- no asymmetric cryptography

Communication

- wireless
- no advance knowledge of network architecture
- mobility
- nodes join and leave the network



Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

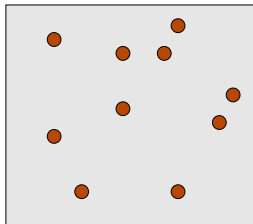
Redistribution

Analysis

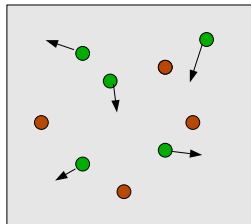
Scenarios

- sensors fields
- mobile artefacts

Sensor field



Mobile artefacts





Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

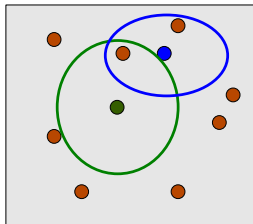
Redistribution

Analysis

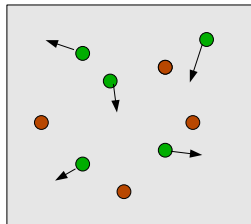
Scenarios

- sensors fields
- mobile artefacts

Sensor field



Mobile artefacts





Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

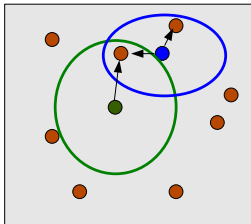
Redistribution

Analysis

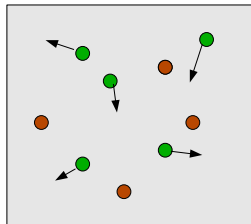
Scenarios

- sensors fields
- mobile artefacts

Sensor field



Mobile artefacts





Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

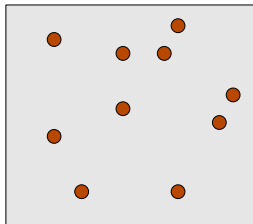
Redistribution

Analysis

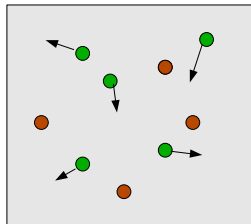
Scenarios

- sensors fields
- mobile artefacts

Sensor field



Mobile artefacts





Ad hoc network of tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

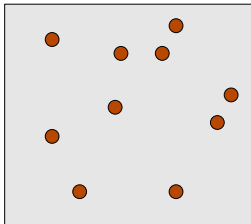
Redistribution

Analysis

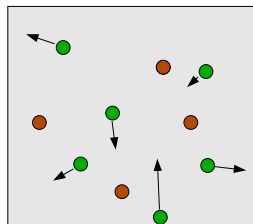
Scenarios

- sensors fields
- mobile artefacts

Sensor field



Mobile artefacts





Data protection

for tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Data

- sensitive measurement information
- safety critical data
- ...



Data protection

for tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Data

- sensitive measurement information
- safety critical data
- ...

Adversary

- capturing data
- impersonation
- intercepting nodes



Data protection

for tiny artefacts

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Data

- sensitive measurement information
- safety critical data
- ...

Adversary

- capturing data
- impersonation
- intercepting nodes

Possibilities:

- eavesdropping communication
- reverse engineering some devices
- cloning devices



Security requirements

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Requirements

- **communication encrypted**
(confidentiality)
- **data integrity**
(data not manipulated when transmitted)
- **authentication of nodes**
(impersonation impossible)



Key predistribution

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

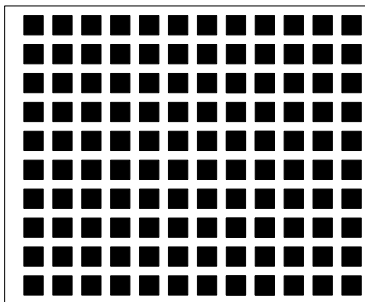
Key
predistribution

Redistribution

Analysis

Pool of keys

- the system provider generates a large pool of n keys
- each device receives a subset of keys of cardinality k





Key predistribution

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

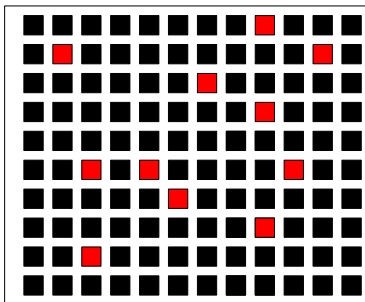
Key
predistribution

Redistribution

Analysis

Pool of keys

- the system provider generates a large pool of n keys
- each device receives a subset of keys of cardinality k



keys of device A



Key predistribution

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

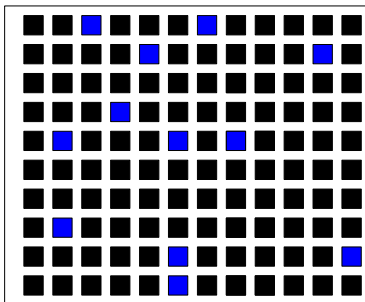
Key
predistribution


Redistribution

Analysis

Pool of keys

- the system provider generates a large pool of n keys
- each device receives a subset of keys of cardinality k



 keys of device B



Key predistribution

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

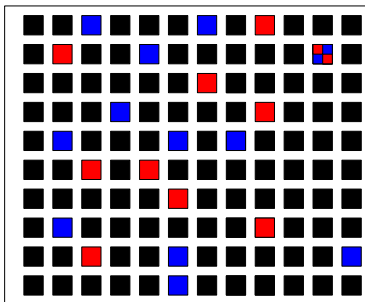
Key
predistribution

Redistribution

Analysis

Pool of keys

- the system provider generates a large pool of n keys
- each device receives a subset of keys of cardinality k



shared keys of devices A and B



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

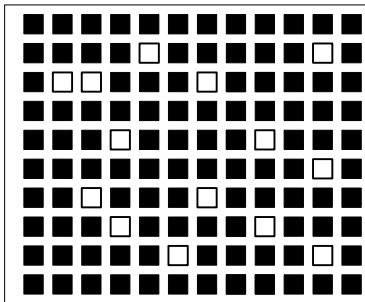
Key
predistribution

Redistribution

Analysis

Capturing keys

- an adversary can reverse engineer some devices
-



keys captured by the adversary



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

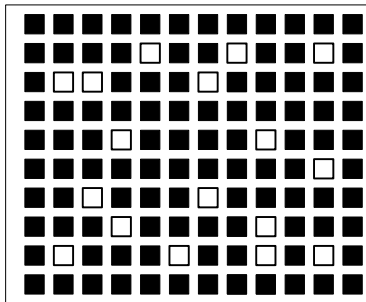
Key
predistribution

Redistribution

Analysis

Capturing keys

- an adversary can reverse engineer some devices
-



keys captured by the adversary



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

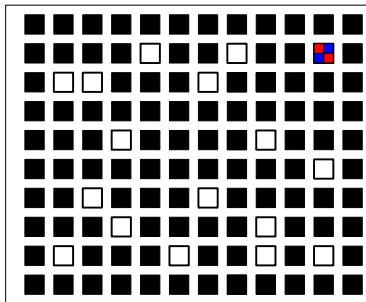
Key
predistribution

Redistribution

Analysis

Capturing keys

- an adversary can reverse engineer some devices
- no more protection with the captured keys



keys captured by the adversary



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Known countermeasures

q-composite at least q shared keys are necessary for establishing a secure link,

- each device has to hold more keys
- therefore collecting keys by the adversary more efficient



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Known countermeasures

q-composite at least q shared keys are necessary for establishing a secure link,

- each device has to hold more keys
- therefore collecting keys by the adversary more efficient

multipath devices A and B establish a session key from keys transported over the links: $A-C_1-B$, $A-C_2-B$, \dots , $A-C_q-B$

- high density of devices necessary



Key predistribution problems

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Known countermeasures

q-composite at least q shared keys are necessary for establishing a secure link,

- each device has to hold more keys
- therefore collecting keys by the adversary more efficient

multipath devices A and B establish a session key from keys transported over the links: $A-C_1-B$, $A-C_2-B$, \dots , $A-C_q-B$

- high density of devices necessary

key levels each key has many versions computed with a hash chain, an adversary holding wrong version cannot decrypt communication

- it increases the cost of attack, but only by 50%



Key redistribution scheme

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

General framework

- **predistribution keys** used only for encryption of temporal keys
- **temporal keys** used for communication between devices
- new temporal keys **broadcasted** periodically, every key from the pool used to encrypt one temporal key



Key redistribution scheme

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

General framework

- **predistribution keys** used only for encryption of temporal keys
- **temporal keys** used for communication between devices
- new temporal keys **broadcasted** periodically, every key from the pool used to encrypt one temporal key

Man trick

each temporal key encrypted **by m randomly chosen predistribution keys**



Key redistribution scheme

how does it work?

Key
Redistribution

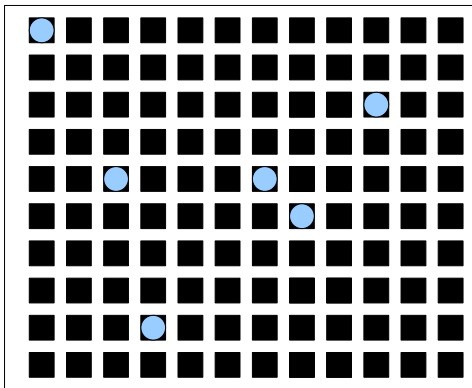
Cichoń,
Golebiewski,
Kutyłowski



Model

Key
predistribution

Redistribution

Analysis



 predistribution keys used to encrypt temporal key 



Key redistribution scheme

how does it work?

Key
Redistribution

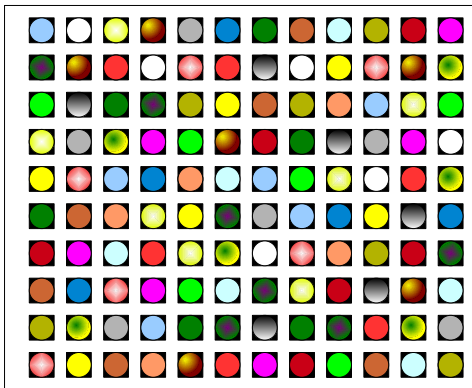
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



an assignment of all temporal keys to predistribution keys



Key redistribution scheme

how does it work?

Key
Redistribution

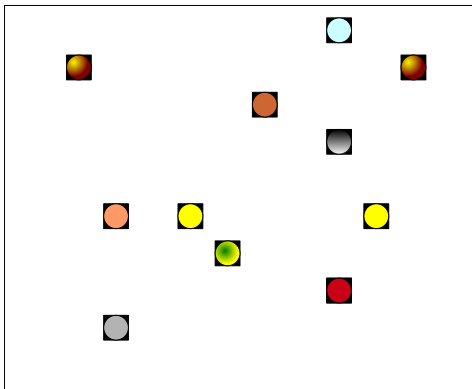
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



Temporal keys received by device A



Key redistribution scheme

how does it work?

Key
Redistribution

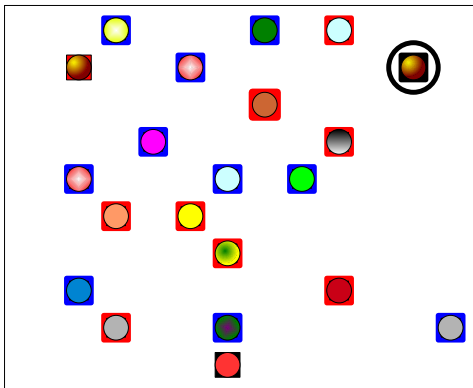
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



Temporal keys received by devices A and B



Key redistribution scheme

how does it work?

Key
Redistribution

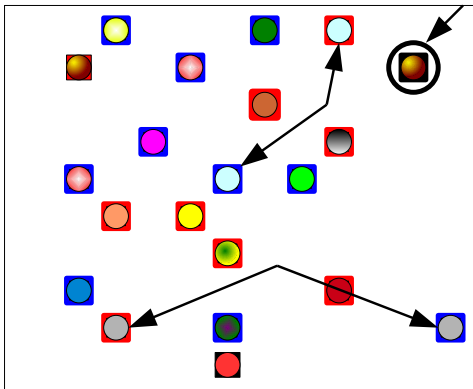
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



Temporal keys received by devices A and B



Key redistribution scheme

how does it work?

Key
Redistribution

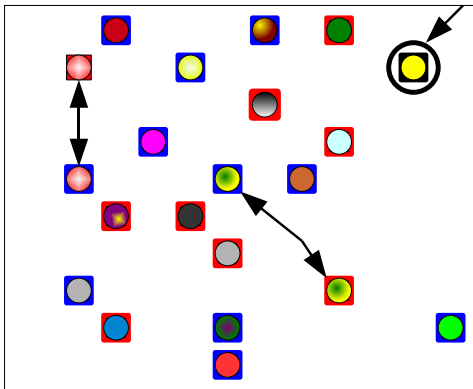
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



Temporal keys received by devices A and B for another session



Key redistribution scheme

how does it work?

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Summary

- devices A and B may share a temporal key K'_i because:
 - K'_i was broadcasted as $E_{K_u}(K'_i)$ and A knows K_u
 - K'_i was broadcasted as $E_{K_v}(K'_i)$ and B knows K_v
- while A does not know K_v and B does not know K_u .



Key redistribution scheme

how does it work?

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Summary

- devices A and B may share a temporal key K'_i because:
 - K'_i was broadcasted as $E_{K_U}(K'_i)$ and A knows K_U
 - K'_i was broadcasted as $E_{K_V}(K'_i)$ and B knows K_Vwhile A does not know K_V and B does not know K_U .
- after broadcasting new temporal keys K_U and K_V does not help to share a key, since this time they encrypt different keys, say

$$E_{K_U}(K''_r), \quad E_{K_V}(K''_z)$$



Key redistribution scheme properties

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

while A talking with B :

- after redistribution of temporal keys they share different keys
- an adversary impersonating B has to hold appropriate predistribution keys possessed by B

It does not suffice to hold some key of B in order to impersonate B or eavesdrop the whole communication of B . Now it is necessary to hold all or most keys of B !



Analytic results

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Method used

combinatorial classes ...

Results

exact values for the expected number of shared:

- predistribution keys
- temporal keys



Analytic results

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Expected number of shared temporal keys χ

Suppose that each predistribution key is broadcasted m times, and each device holds $k = \Theta(\sqrt{n})$ out of n predistribution keys. Then

$$E(\tilde{\chi}) = \frac{m}{n}k^2 + O\left(\frac{1}{\sqrt{n}}\right).$$

Precise values for any n, m, k are given in the paper

Corollary

so for $m = 2$ devices A and B should have 2 shared temporal keys!

From a random pair of predistribution keys!



Analytic results

Key
Redistribution

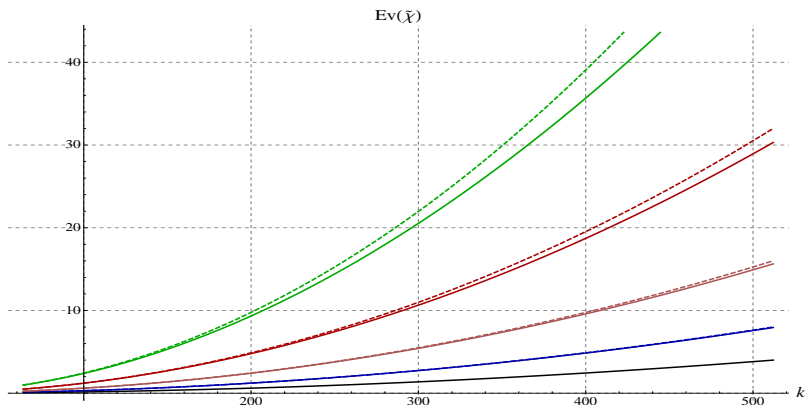
Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis



Rysunek: The expected number of temporal keys shared by A and B for $n = 2^{16}$, $2^6 \leq k \leq 2^9$ and $m = 1$ (black plot), $m = 2$ (blue plot), $m = 4$ (pink plot), $m = 8$ (red plot), $m = 16$ (green plot) (dashed plots present approximations from the previous slide).



Attack cost

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Let n be the pool size, k number of keys for each device, $m =$ number of copies of each temporal key.

Let $T_{A,B}$ be a set of temporal keys shared by the devices A and B . Let Ad denote the set of the temporal keys held by an adversary.

Then

1 If $|Ad| = \sqrt{n}$, then $\Pr[T_{A,B} \subseteq Ad] \leq \left(\frac{m}{\sqrt{n}}\right)^m$.

2 If $|Ad| < \frac{n}{m^{2^{1/m}}} \approx \frac{n}{m} \left(1 - \frac{\ln 2}{m}\right)$, then $\Pr[T_{A,B} \subseteq Ad] < \frac{1}{2}$.



Conclusions

Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

surprising advance that make predistribution effective and
reliable without a substantial cost



Key
Redistribution

Cichoń,
Golebiewski,
Kutyłowski

Model

Key
predistribution

Redistribution

Analysis

Thanks for your attention!

Contact data

- 1 `Mirosław.Kutyłowski@pwr.wroc.pl`
- 2 `http://kutyłowski.im.pwr.wroc.pl`
- 3 `+48 71 3202109, fax: +48 71 320 2105`