Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: [Configuration and Trust Management Discussion]
Date Submitted: [September 21, 2005]
Source: [Rene Struik] Company [Certicom Research]
Address [5520 Explorer Drive, Fourth Floor, Mississauga, ON, L4W 5L1, Canada]
Voice:[905 501-6083], FAX: [905 507-4230],
E-Mail:[rstruik@certicom.com]

Re: [ ]

Abstract: This presentation discusses configuration and trust management issues related to the secure operations of ad-hoc networks.

Purpose: Highlight principles underlying the secure operations of ad-hoc networks, raise awareness for secure, yet flexible system lifecycle management, and introduce flexible device role models.

Configuration and Trust Management Discussion

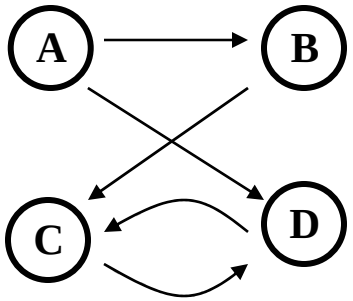
René Struik
Certicom Research

Configuration management (1)

Configuration

Information on which entities are supposed to communicate with which other entities.

Without sub-units:



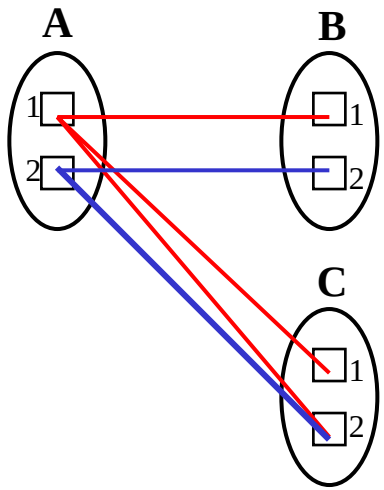
Each device keeps track of its own local neighborhood:

A → B, A → D;

B → C;

C → D; D → C.

With sub-units:



Each device keeps track of its own color scheme:

A1: red → B, C; A2: blue → B, C;

B1: red → A; B2: blue → A;

C1: red → A; C2: red, blue → A.

Configuration management (2)

Configuration manager

Responsible for selecting which entities are supposed to talk with which other entities:

- Definition of groups of devices that are supposed to communicate with each other;
- Communication of group membership to each individual member hereof.

Configuration mechanisms

- via external configuration tool;
- via service discovery process.

Trust requirement

Each device needs to trust its configuration manager(s), in the sense that it does not hook it up with spy-ware or other devices that are supposed to be kept out of the loop.

Note: *Independent verification possible*

One can verify whether a configuration manager has done its job properly, i.e., has set up proper ‘virtual wiring’, without access to keying material or other privileged info (e.g, by querying the device).

Configuration management (3)

Selection of configuration manager

- Each device may choose its own set of favorite configuration managers (*ConfigSet*);
- This list should be adaptable by a device with the proper credentials (*Config-Δ-Set*). Each such device is a member of *ConfigSet*.

Trust guarantee options

- Evidence that info indeed originates from purported configuration manager;
- Inspection of conformance of configuration afterwards ('independent verification').

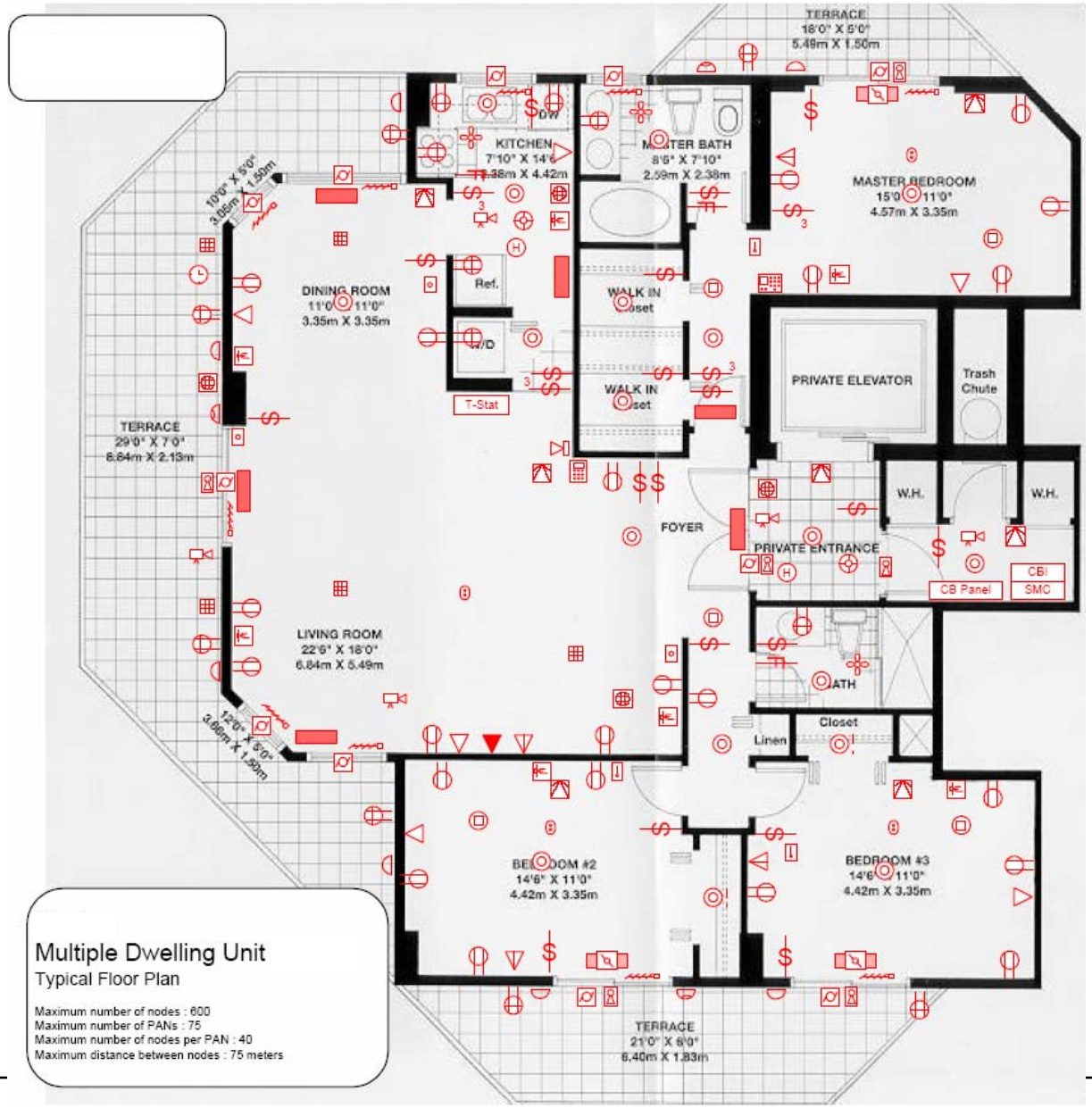
Notes:

- If *Config-Δ-Set* is the empty set, this freezes the current set of configuration managers;
- If *ConfigSet* is the empty set, the configuration is fixed towards the future.

Initial setup via finite state machine (example – resurrecting duckling policy)

- Initial state: the sets *ConfigSet* and, hereby, *Config-Δ-Set* are the empty set;
- Bootstrap mechanism: non-cryptographic introduction of configuration manager to device (thus provoking state change from initial state to other state); *) tricks omitted!
- Return to initial state: via erasure of *ConfigSet* by member with proper credentials.

Example:


TERRACE
16'0" X 5'0"
5.49m X 1.50m
KITCHEN
7'10" X 14'6"
2.38m X 4.42m
MASTER BATH
8'6" X 7'10"
2.59m X 2.38m
MASTER BEDROOM
15'0" X 11'0"
4.57m X 3.35m
DINING ROOM
11'0" X 11'0"
3.35m X 3.35m
Ref.
W/D
T-Stat
WALK IN Closet
WALK IN Closet
PRIVATE ELEVATOR
Trash Chute
TERRACE
29'0" X 7'0"
8.84m X 2.13m
FOYER
W.H.
W.H.
PRIVATE ENTRANCE
CB Panel
CBI
SMC
LIVING ROOM
22'6" X 18'0"
6.84m X 5.49m
BATH
Closet
Linen
BEDROOM #2
14'6" X 11'0"
4.42m X 3.35m
BEDROOM #3
14'6" X 11'0"
4.42m X 3.35m
TERRACE
21'0" X 6'0"
6.40m X 1.83m
Multiple Dwelling Unit
Typical Floor Plan
Maximum number of nodes : 600
Maximum number of PANs : 75
Maximum number of nodes per PAN : 40
Maximum distance between nodes : 75 meters

Configuration management (5)

Assisted configuration (with help of external configuration device)

Step 1 (‘virtual wiring’)
Define the groups of physical devices that are supposed to communicate with each other.

Step 2 (device identification)
Determine the IEEE MAC address of each device to be configured.

Step 3 (bootstrap mechanism)
Imprint each device with the IEEE MAC address of the configuration device.

Step 4 (configuration step)
Send each device the configuration information corresponding to the groups it belongs to

Step 5 (verification step)
Verify the conformance of the device configurations via one of the trust guarantee options (i.e., via independent inspection or via data origin authentication).

Configuration management (6)

Manual configuration (without help of external configuration device)

Same as assisted configuration with help of external configuration device!!!
(simply, take one of the network devices to be the configuration device)

Note 1: The main difference between assisted and manual configuration is with the configuration step (Step 4):

Assisted configuration relies on an external configuration device with, usually, a far more powerful user interface (useful for conveying detailed configuration information) than would be possible with a network-internal device.

Note 2: Another difference might be with *form factors* of the configuration device. An external configuration tool may be tailored towards ease of use, whereas a network device might have limitations (e.g., dimensions, weight) that may limit ease-of-use or prevent it altogether (e.g., try lifting a compressor or a heat pump!).

Configuration management (7)

Assisted configuration (with help of configuration device) – cont'd (ii)

Flexibility:

- *Parallelization.* The role of the configuration manager can be performed by multiple configuration managers in parallel, without requiring much coordination:

  Each configuration manager only needs to implement the assisted configuration of those devices allocated to him.

- *Configuration freeze*. The configuration setting can be locked by the configuration manager by setting the set *ConfigSet* to the empty set (if he has the proper credentials).

- *Limitation of liability*. Control can be handed over to, e.g., the network owner by setting the set *ConfigSet* to represent this network owner only (if he has the proper credentials). The configuration manager now does not carry responsibility/liability for leakage of security material (only for hooking up the correct devices, which can be checked).

Configuration management (8)

Assisted configuration (with help of configuration device) – cont'd (iii)

Security:

- *Unsecured configuration (no crypto aboard).*
  Verification of proper configuration (Step 5) needs to be realized using independent (manual) inspection of the a postiori configuration settings of each device.

- *Secured configuration (public-key based techniques).*
  If a device shares a root key with its configuration manager, the configuration info (sent in Step 4) can be secured using the data key derived after executing the public-key key establishment protocol between those two devices.

- *Secured configuration (symmetric-key based techniques).*
  If a device shares a master key with its configuration manager, the configuration info (sent in Step 4) can be secured using the data key derived after executing the symmetric-key key establishment protocol between those two devices.

Configuration management (9)

Assisted configuration (with help of configuration device) – cont'd (iv)

Security:

- *Unsecured configuration (no crypto aboard).*
  No cryptographic mechanism for secure network operation available.

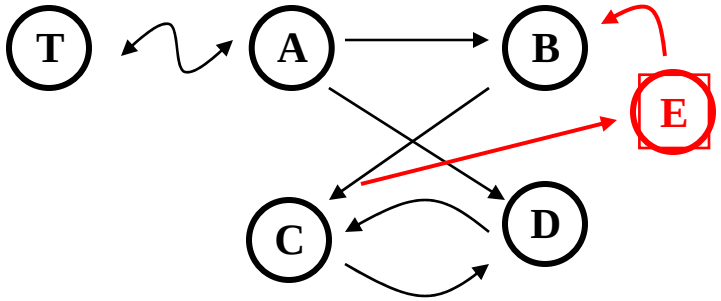
- *Secured configuration (public-key based techniques).*
  If a device shares a root key with each 'security manager' of each group in its configuration setting, then it may obtain all group keys automatically, without any further intervention (and, thereby, all keying material for secure network operation).

- *Secured configuration (symmetric-key based techniques).*
  If a device shares a master key with each 'security manager' of each group in its configuration setting, then it may obtain all group keys automatically, without any further intervention (and, thereby, all keying material for secure operation).

Configuration management (10)

Assisted configuration (with help of configuration device) – cont'd (v)

Example A: Public-key based techniques.



$CASet = \{\text{Root Key}_1, \text{Root Key}_2, \text{Root Key}_3\}$

	A	B	C	D	E
ConfSet	T	T	T	T	
KeyEstabl	k_{AT}	k_{BT}	k_{CT}	k_{DT}	
Binding	E_A	E_B	E_C	E_D	
ConfSet					T
KeyEstabl					k_{ET}
Binding			$\hat{E}_C$		E_E

$E_A = \{A \rightarrow B, A \rightarrow D\}$;

$E_B = \{B \rightarrow C\}$; $E_D = \{D \rightarrow C\}$;

$E_C = \{C \rightarrow D\}$; $\hat{E}_C = \{C \rightarrow D, C \rightarrow E\}$;

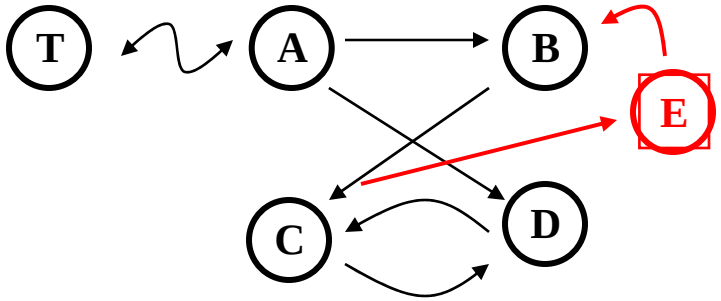
$E_E = \{E \rightarrow B\}$.

Added bonus: all other secure trust relationships automatic!

Configuration management (11)

Assisted configuration (with help of configuration device) – cont'd (vi)

Example B: Symmetric-key based techniques.



	A	B	C	D	E
ConfSet	$T;K_{AT}$	$T;K_{BT}$	$T;K_{CT}$	$T;K_{DT}$	
KeyEstabl	k_{AT}	k_{BT}	k_{CT}	k_{DT}	
Binding	E_A	E_B	E_C	E_D	
ConfSet					$T;K_{ET}$
KeyEstabl					k_{ET}
Binding			$\hat{E}_C$		E_E

E_A={A → B, A → D};

E_B={B → C}; E_D={D → C};

E_C={C → D}; $\hat{E}_C$={C → D, C → E};

E_E={E → B}.

Disadvantage: all other secure trust relationships require involvement of some trusted party T'! (Here, T'=T if configuration manager and trust manager coincide.)

Operational description – Set-theoretic definition of roles

Informational elements (provided by device itself)

(1) *Global device Id.*
Each device has own *static* global device Id (IEEE MAC address).

(2) *Public key (in public-key scenario).*
Each device has its own public/private key pair (P_A, S_A).
{The public key P_A need not to be stored on the device itself.}

(3) *Access control list (ACL) (if desired).*
Each device has own set of devices it may wish to establish a secure peer-to-peer link key with.

(4) *TrustSet (in dynamic-trust scenario).*
Each device has own set of devices it trusts to assume the role of security manager.

(5) *CA-Set (in dynamic-trusted party scenario).*
Each device has own set of devices it trusts to assume the role of trusted third party.

(6) *ConfigSet (in dynamic configuration manager scenario).*
Each device has own set of devices it trusts to assume role of configuration manager.

(7) *ACL-Δ-Set (in dynamic-trust scenario).*
Each device has own set of devices it trusts to change the *ACLSet.*

(8) *Trust-Δ-Set (in dynamic-trust scenario).*
Each device has own set of devices it trusts to change the *TrustSet.*

(9) *CA-Δ-Set (in dynamic trusted party scenario).*
Each device has own set of devices it trusts to change the *CA-Set.*

(10)*Config-Δ-Set (in dynamic configuration manager scenario).*
Each device has own set of devices it trusts to change the *ConfigSet.*

Initial set-up – Boot-strap mechanism

	A	B
Pre:	A: x	B: y
Post:	B: y	A: x

(Here, x and y are authentic or secret keying material (or status information)

Exchange of info:

- secret info via wire: resurrecting duckling security policy [Stajano, Anderson (1999)]
- authentic info via limited channel [Smetters et al (2002)]
- 2-way authentic channel, 1-way secret and authentic channel, 2-way secret channel [Henk-Jan Hoekman (2004)]
- Proximity-based authentication [Chaum and Brands (1994), Struik (2004)]

  Basic building block: (1) [A $\rightarrow$ B: x
  (2) A $\leftarrow$ B: $x \oplus y$]