

Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications

Authors: M. M. Fouda, Z. Md. Fadlullah, and N. Kato
Proc. International Conference on Computer Engineering and
Systems (ICCES), Cairo, Egypt, 2010

Presenter: Jae-Yeon Won

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

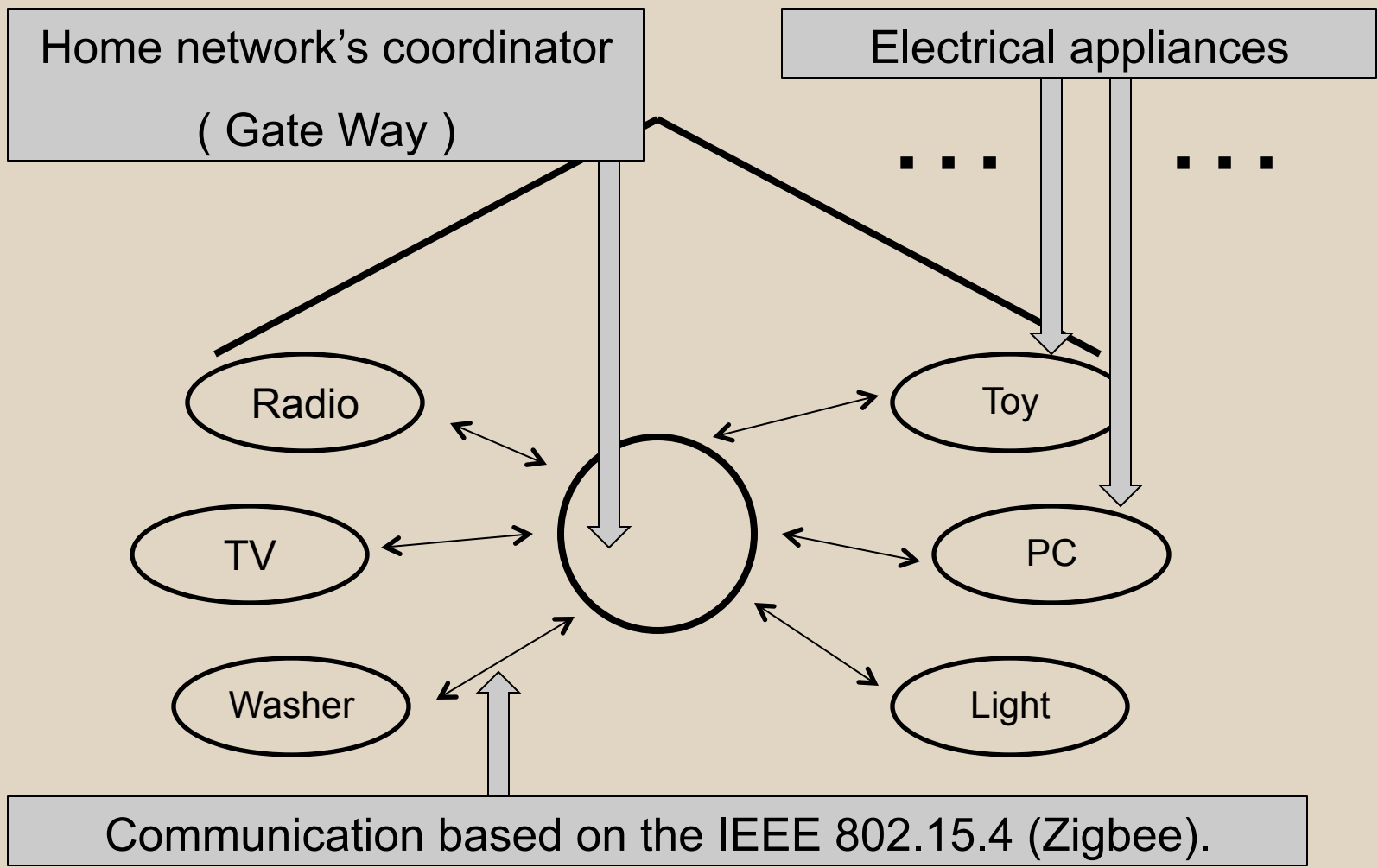
Overview

- Introduction and Motivation
- Backgrounds
- Related Works
- Considered Framework
- Considered Attack model
- Simulation & Results
- Solution
- Personal assessment
- Conclusion & Future Works
- References

Introduction and Motivation

- Smart Grid (SG) : future grid to provide stable and reliable power to the end-user.
- Focus : how to protect the home area network systems from illegal accesses and threats.
- **Home area network ID conflict** can be occurred in the system based on Zigbee.

Background



Background – Cont.

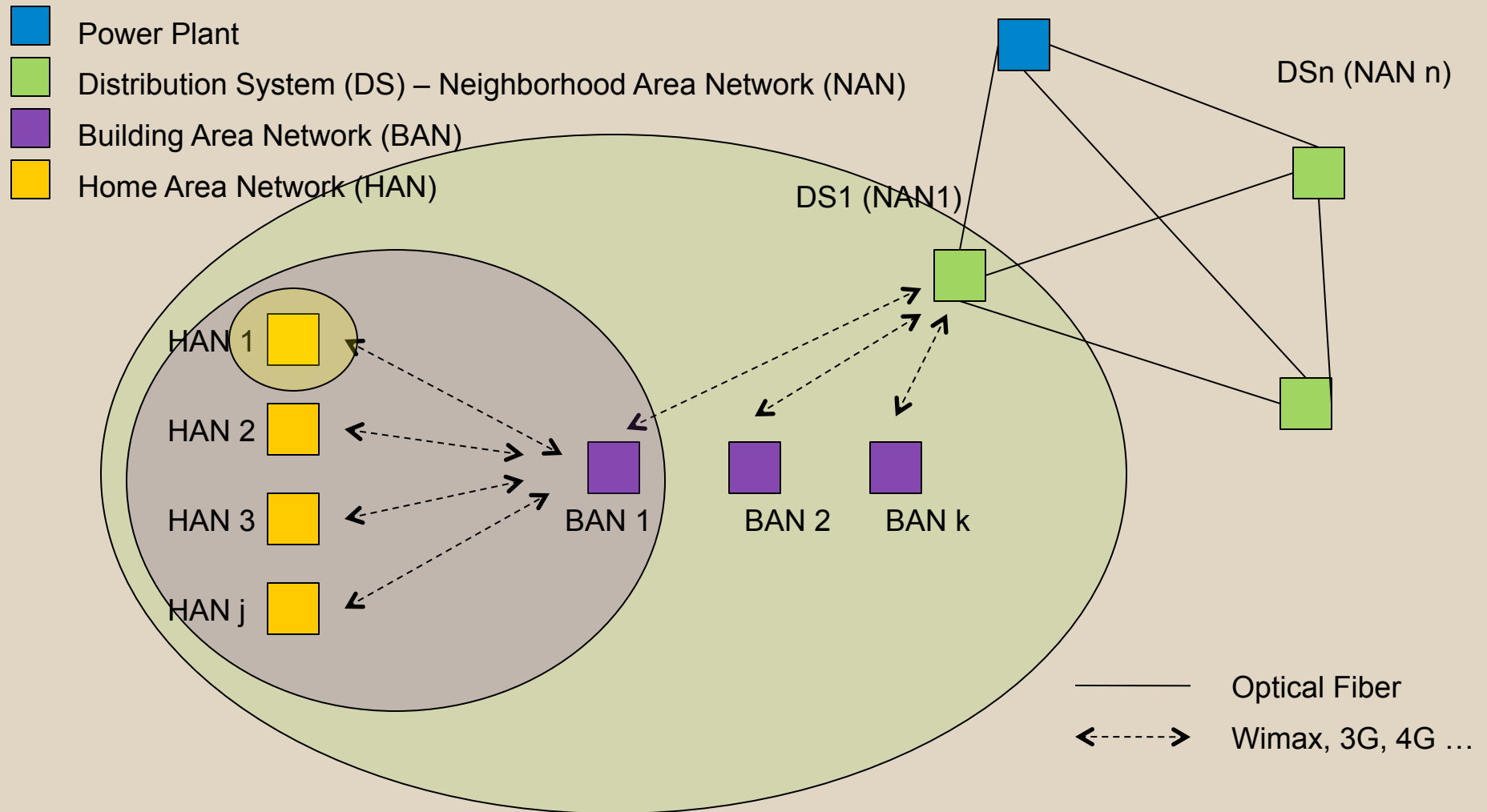
- Zigbee
 - IEEE 802.15.4 specification
 - wireless protocols for cheap and power saving
 - support several security features
 - typical method for Home Area Network (HAN)
- Home Area Network ID(HANID)
 - Identifier to differentiate apartment units
 - One HANID is allocated for one unit.

Related Works

- Hamlyn et al. [2]
 - a utility computer network security management and authentication in SG
 - Focus : securing host area

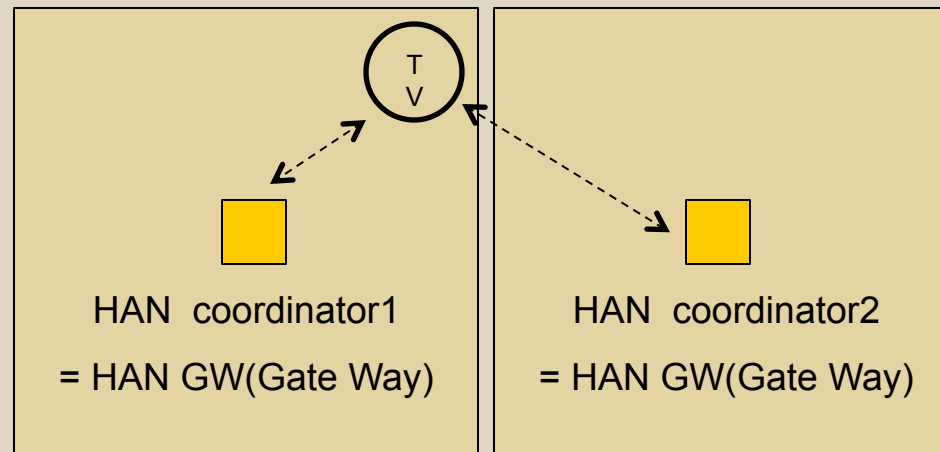
- Metke et al. [3]
 - strict security requirements
 - Focus : by the utility provider

Considered Framework



Considered Attack Model

- The electrical appliances of a given HAN know their HANID.
- **A HANID conflict** may be occurred if there exists more than one HAN coordinator have same HANIDs.



➔ It can detect this conflict by receiving conflict notification messages. [4]

Considered Attack Model – Cont.

- Procedure
 - The HANID conflict may be occurred. (same HANIDs)
 - It can detect this conflict.
 - Conflict notification message is sent to the HAN coordinator.
 - If it is detected, it performs the conflict resolution procedure. (Related to channel scans, coordinator realignment procedure and choosing a new HANID)
 - It takes about **3 seconds** to resolve it. ← **TARGET**
 - Assumption : The attacker can produce **the conflict notification messages.**

Considered Attack Model – Cont.

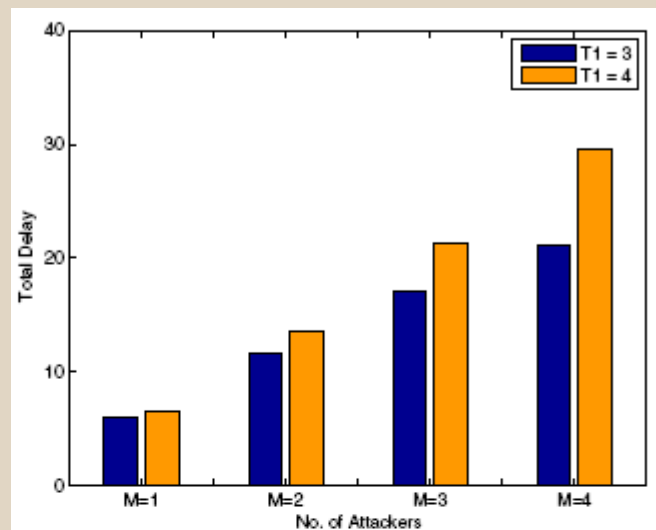
- Problem
 - Time duration for the conflict resolution procedure.
 - While it resolves, other legitimate devices are deprived of the utility service as they are detached from the HAN coordinator.

→ Critical : Time duration

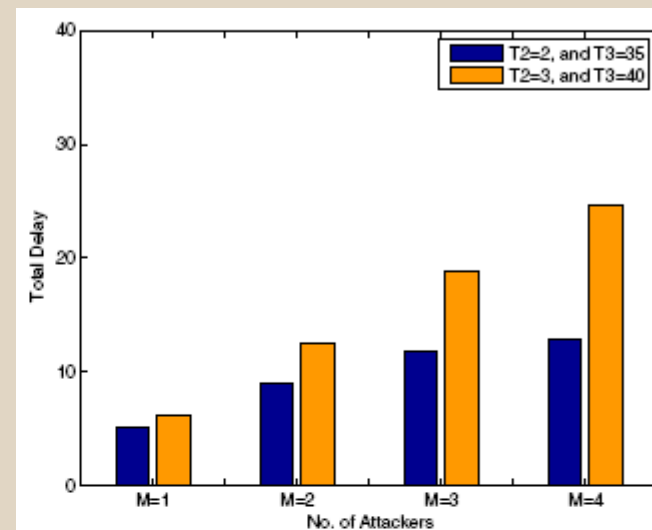
Simulation & Results

- Parameters

- T1 : the maximum number of conflicts for an attacker
- T2 : the maximum number of HANID conflicts
- T3 : a duration time for an attacker
- M : the number of attackers



From Reference[1]

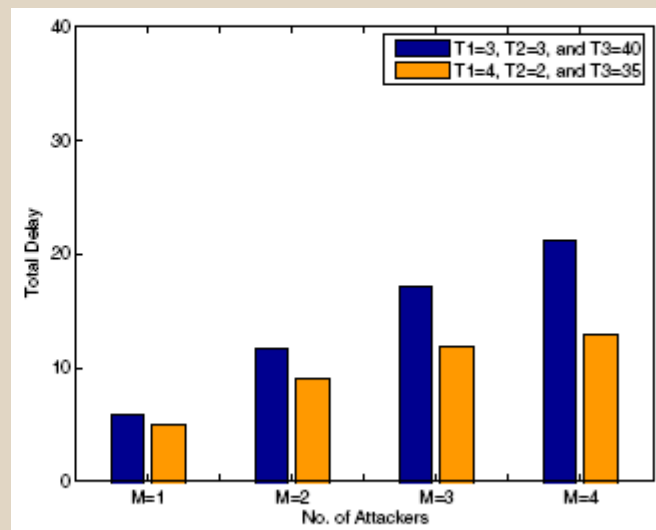


From Reference[1]

→ Simulation was done for 100 seconds.

Simulation & Results – Cont.

- Parameters
 - T1 : the maximum number of conflicts for an attacker
 - T2 : the maximum number of HANID conflicts
 - T3 : a duration time for an attacker
 - M : the number of attackers



→ Quite long for the end-user



From Reference[1]

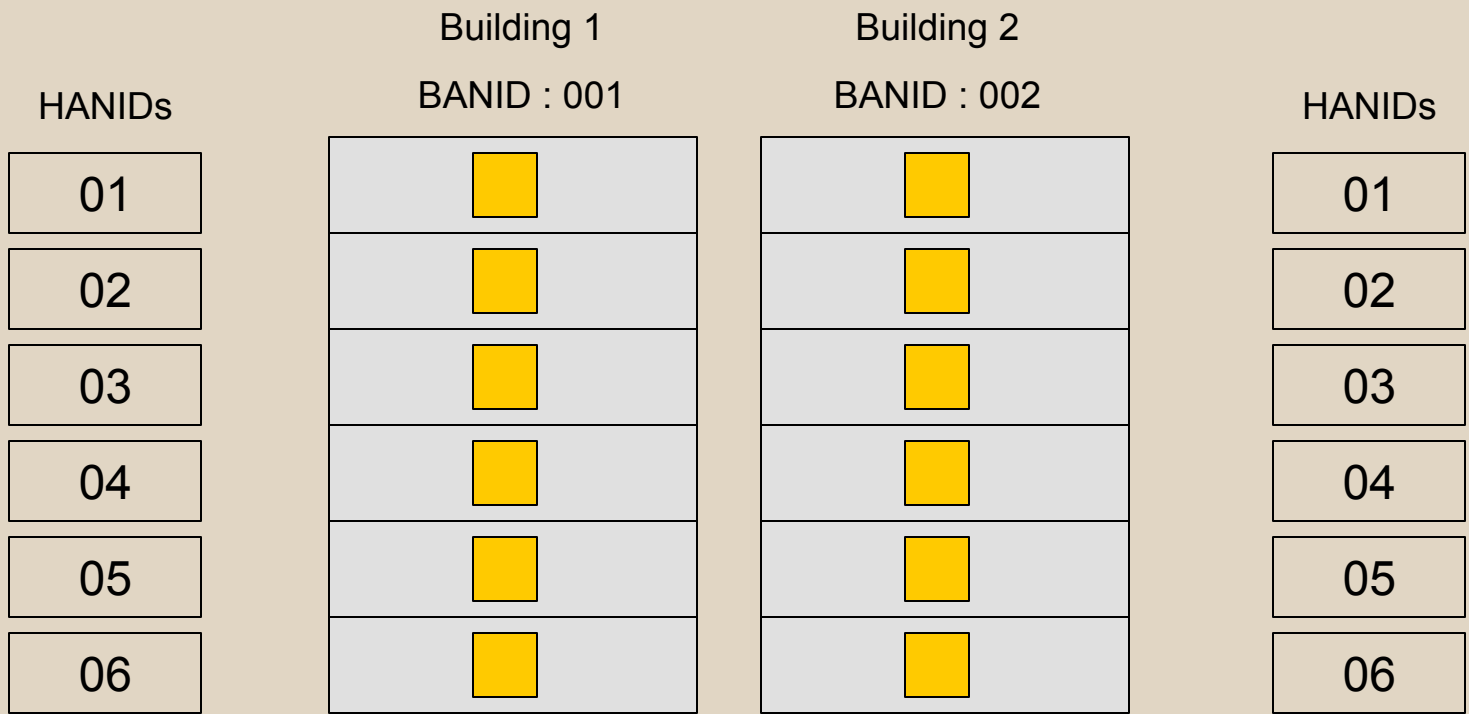
Solution


- Root cause
 - They can have same HANIDs.
- Solution
 - should always have different HANIDs
 - For example, the HANID can be constructed with HANID and BANID. (or unique information)


Solution – Cont.

Current – Conflict phase

-  Building Area Network (BAN) Coordinator
-  Home Area Network (HAN) Coordinator





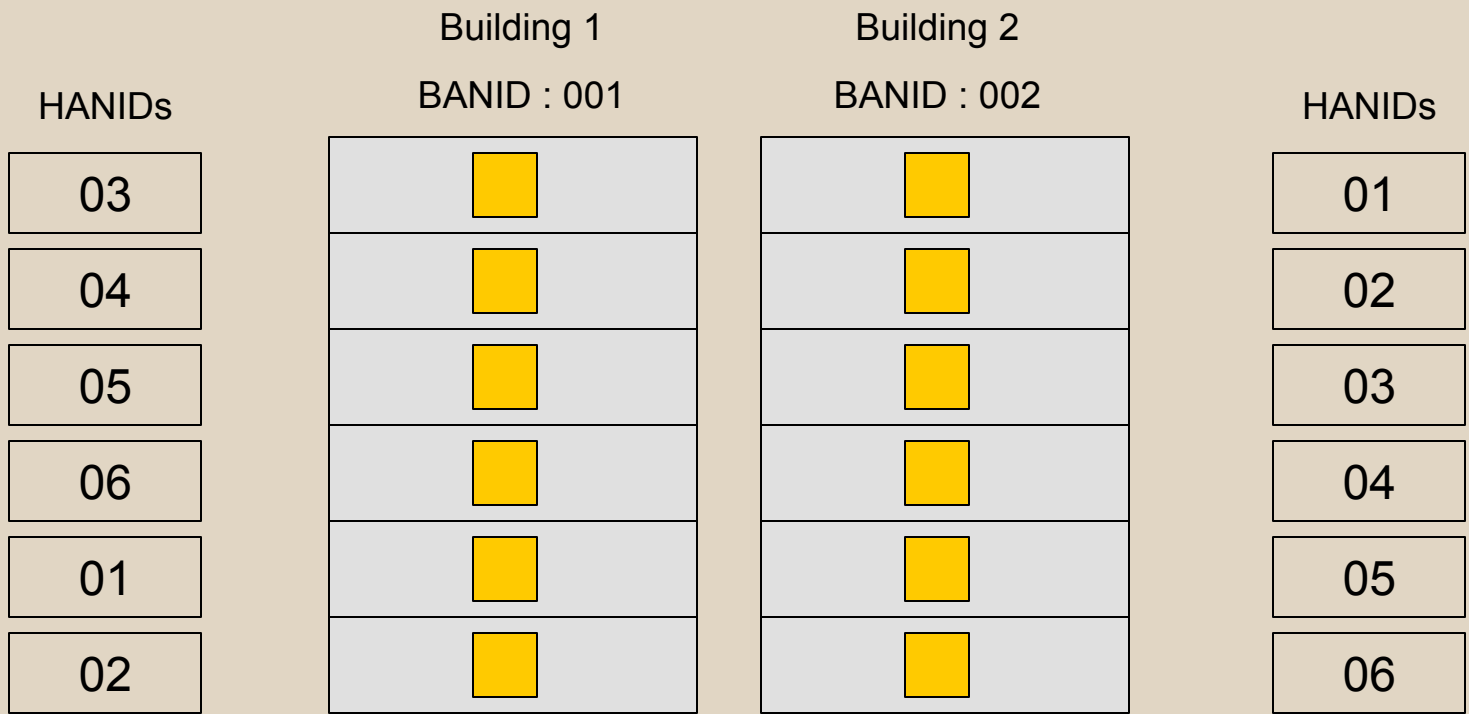
 BAN 001 coordinator


 BAN 002 coordinator


Solution – Cont.

Current – Resolve phase

-  Building Area Network (BAN) Coordinator
-  Home Area Network (HAN) Coordinator





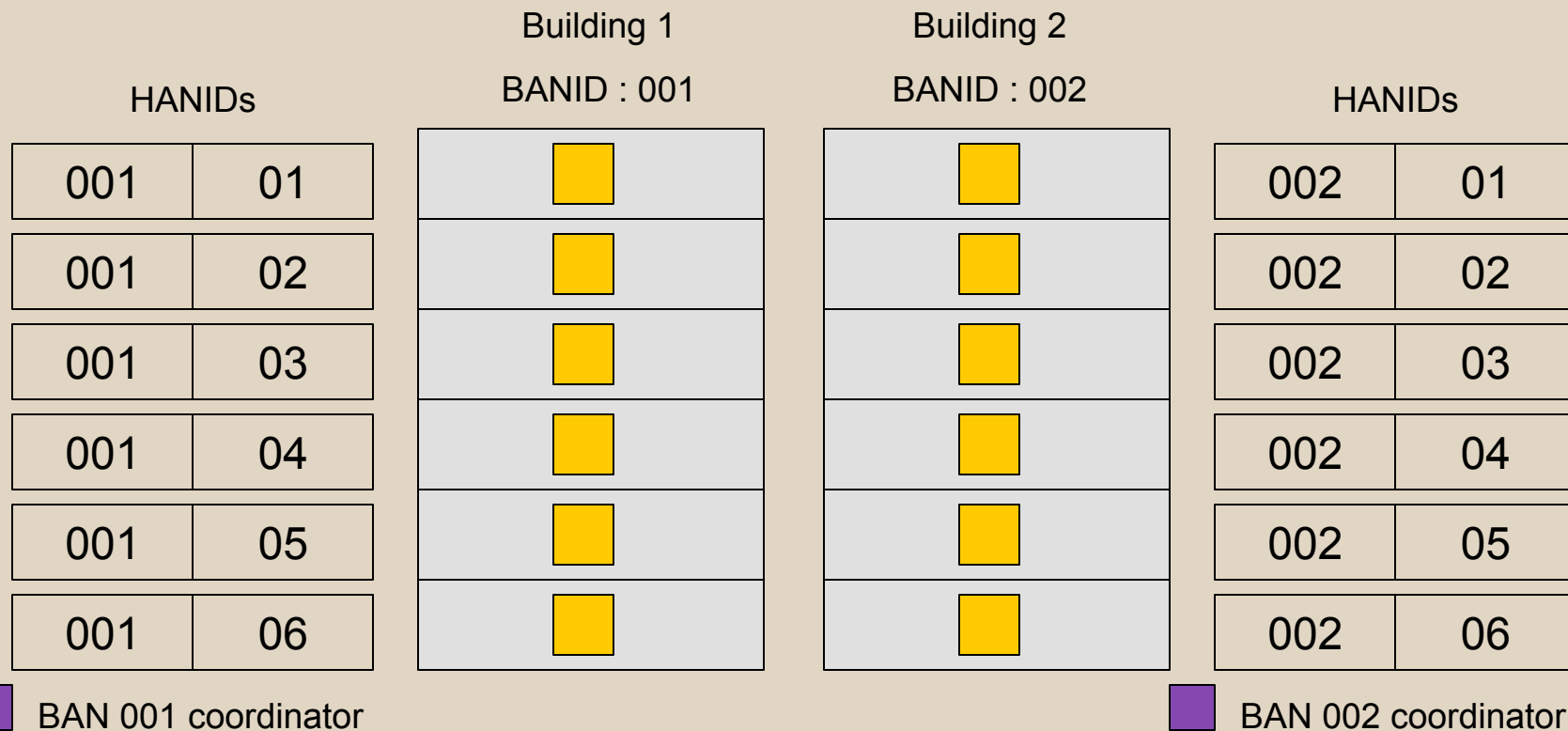
 BAN 001 coordinator

 BAN 002 coordinator

Solution – Cont.

Proposed

-  Building Area Network (BAN) Coordinator
-  Home Area Network (HAN) Coordinator



Personal Assessment

- Pros
 - Enlighten the possible problem during it resolves the another problem.
 - Proposed the fundamental architecture to prevent it in the first place.
- Cons
 - Not considered the bandwidth and power to communicate with large data between the HANGW and electrical appliances.
 - There is no additional information for complexity to communicate among the HAN, BAN and NAN system.

Conclusion & Future work

- Conclusion
 - Introduced an appropriate architecture to facilitate Smart Grid communication.
 - Investigated Home Area Network ID conflict attacks.
 - Studied the effect of the attack on SG communications in various attack scenarios through computer-simulation.
 - Focused on preventing the attack from taking place
- Future works
 - Some researches about bandwidth and power

References

- [1] Mostafa M. Fouda, Zubair Md. Fadlullah, and Nei Kato, “Assessing Attack Threat Against Zigbee-based Home Area Network for Smart Grid Communications”, Proc. International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, pp. 245-250, November/December 2010.
- [2] A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, “Network Security Management and Authentication of Actions for Smart Grids Operations,” Proc. IEEE Electrical Power Conference, Montreal, Que, Canada, Oct. 2007.
- [3] A. R. Metke and R. L. Ekl. “Smart Grid Security Technology,” Proc. IEEE PES on Innovative Smart Grid Technologies (ISGT’ 10). Washington D.C., USA, Jan.2010
- [4] S. C. Ergen, “ZigBee/IEEE 802.15.4 Summary,” Internal Report to Advanced Technology Lab of National Semiconductor, 2004.

Thank you !