PROCESS CONTROL SYSTEM FORUM (PCSF)
2007 Annual Meeting
March 5-8, 2007
Atlanta, GA

Industrial Plants Un-Wired!

William J. Miller
Maximum Control Technologies
a MILLER WJ & ASSOCIATES Company
http://www.mact-usa.com

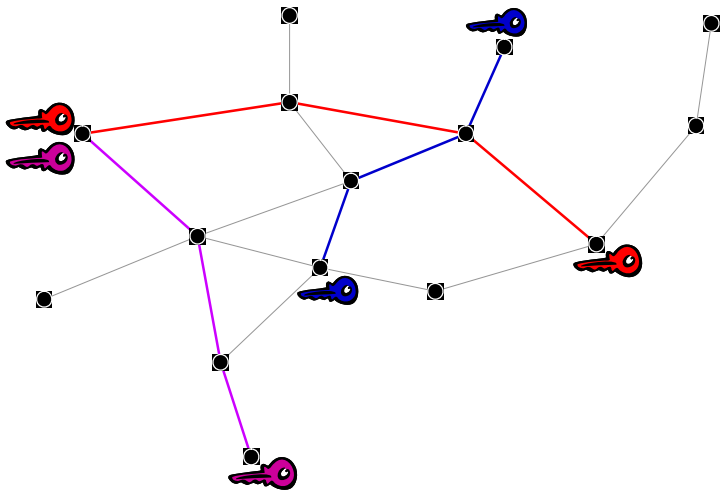
Collaborating to Advance Control System Security

"Challenges for using wireless in industrial plants"

- **ISA SP100 End-User Survey, April 10, 2006**
  - *Security* was the #1 reason identified as a specific barrier to adoption of wireless by 68.6% of the respondents
  - *Performance/Reliability* was the #2 and #3 reason with 40.8% and 24.7% respectively
  - The *lack of confidence* in current technology was found in 49.3% of the respondents

"What is a wireless mesh network?"

- **Mesh networks are an autonomous self-organizing system of wireless nodes connected by nodes that are not in direct range communicate via intermediary nodes.**
- **Routing is challenging, with a highly dynamic topology and bandwidth constraints.**
- **Security is "critical" due to the accessibility of the shared wireless medium and the co-operative nature of mesh nodes.**



- *Examples of a wireless mesh networks that protect industrial plants*

Wireless Applications

- **Cement Plant**
  - VoIP (Voice-over-IP)
    - Emergency Phone System
  - Power Monitoring (OPC)
  - Asset Management (HART)
  - Remote Maintenance
  -

Wireless Applications

- **SCADA - Water Treatment and Distribution System**
  - Control Center Access
  - Video Surveillance
  - Augment of Frame Relay Network used for monitoring and control
  - Remote Maintenance capabilities
  - Asset Management

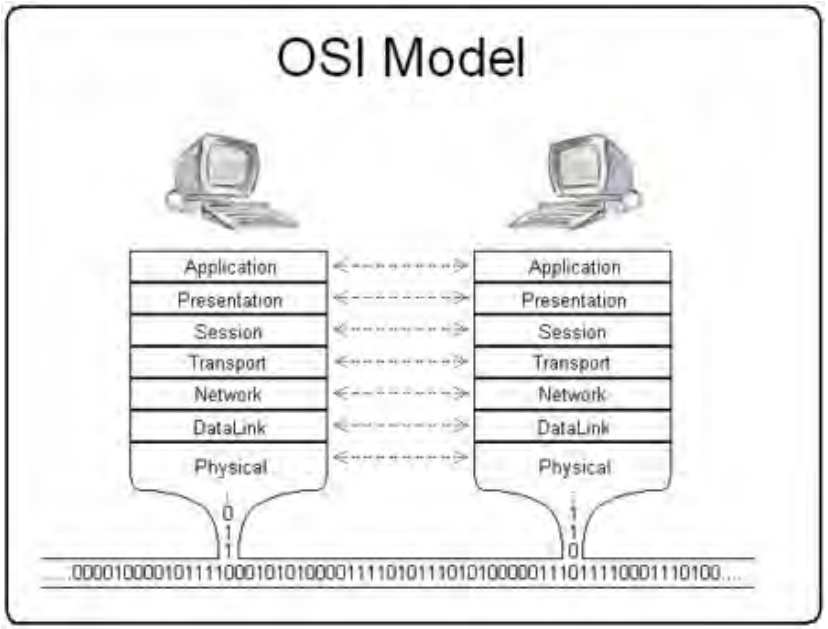
"Achieving high speed wireless mesh mobility for use in industrial plants"

- *Maximizing Routing Performance and Design Factors for Optimal Route Selection*
  - ***Layer 2 (L2) Multi-layer Switching***
  - ***New Metric (Time vs. Hop)***
  - ***New Proactive Routing Protocol***
  - ***Advanced Encryption***
  - ***Key Management (Public vs. Private)***
  - ***Summary***

- *How can optimal routing performance be achieved to provide converged services for industrial wireless networks?*

Maximizing Routing Performance: Layer 2 (L2) Switching

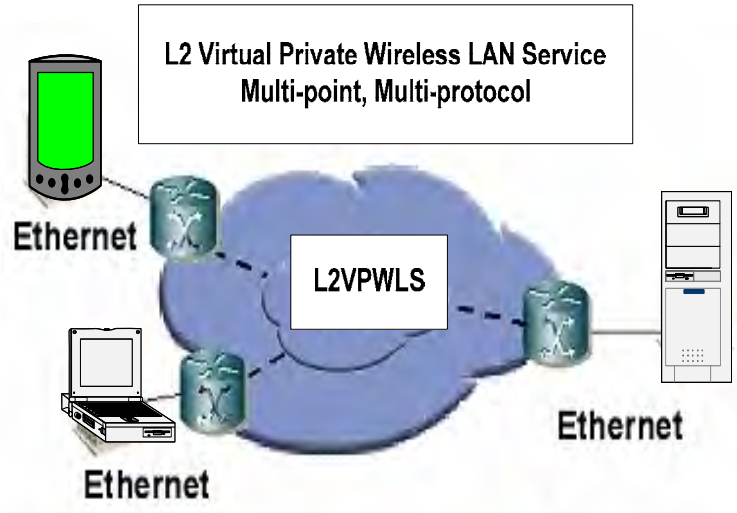
- ***L2*** **forwards traffic based on physical network addresses and are manufacturer hardware specific.**
- ***L2*** **switching is fast - looks only at low-level addressing only; does not process packet contents**
- **L2 does not read very deeply into the packet header, the device can operate very efficiently at very low cost and provide exponentially greater throughput then traditional routers.**
- ***L2 provides routing of packets between any Ethernet device.***



PROCESS CONTROL SYSTEMS FORUM

Maximizing Routing Performance: Multi-layer Switching

- ***Multi-layer switching*** **introduces capabilities based on L3 information that increase the network reliability, stability, and efficiency.**
- **Support for advanced features such as VLANS, UDP Broadcast, Forwarding, IP Multicast, QOS, Multiple Spanning Tree Groups, and Bridging**



- *What are the Design Factors to enhance Performance of industrial wireless networks?*

Design Factors to enhance Performance for industrial wireless networks

- **Traditional Approach:**
  - Minimum Hop Metric (MHM)
- ***New* Approach:**
  - Medium Time Metric (MTM)
- **Existing Mesh Routing Protocols**
- ***New* Proactive Routing Protocol**
  - Pulse Protocol
- **Advanced Encryption**
- **Key Management**
  - Public vs. Broadcast

- *Traditional Approach:*
  Minimum Hop Metric (MHM)

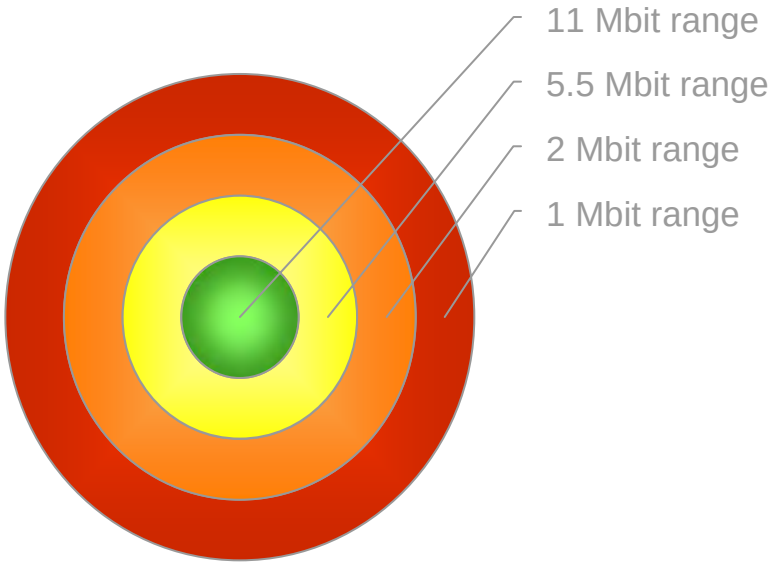
Traditional Approach: Minimum Hop Metric (MHM)

- **Direct routing strategy**
- ***Not designed for multi-rate networks***
- **Usually the minimum hop path is used by a small number of long slow hops**
- **These slow transmissions occupy the medium for a long time, blocking adjacent senders**
- **Selecting nodes on the fringe of the communication range results in reduced *reliability***

- *New Approach:*
  Medium Time Metric (MTM)

New Approach: Medium Time Metric (MTM)

- **Assigns a weight to each link proportional to the amount of medium time consumed by transmitting a packet on the link**
- **Enables the protocol to discover the path with optimal transmission time**
- ***Designed for multi-rate networks***



- *What are channel conditions for Mesh Protocols?*

What are channel conditions for Mesh Protocols?

- **Channel Conditions (i.e. Urban, Industrial)**
  - Multi-path fading
  - Rapidly changing channel conditions
- **On-demand Protocols (AODV, DSR)**
  - No knowledge of channel conditions
  - Channel is continuously changing
- **Link State Protocols (OLSR, TBRPF)**
  - Continuous flooding from every node in the network

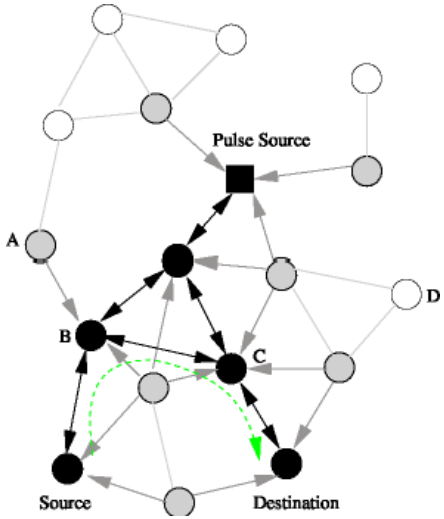
- *New Proactive Routing Protocol designed for Mobility*
  - ***(Pulse Protocol)***

New Proactive Routing Protocol
Pulse Protocol (Designed for Mobility)

- **Utilizes L2 multi-layer switching and achieves high delivery ratios under a wide range of network densities, mobility, and traffic loads.**
- **Periodic pulse flood initiated by the pulse source creates**
  - "*Proactively*" updated spanning tree
  - All broken routes are repaired simultaneously within one pulse using one flood
- **It utilizes MTM to adapt to the environment under high multi-path conditions and choosing an optimal path**
- **Tracks and selects reliable routes between *trusted* nodes**
- **Provides scalability to high levels of mobility**

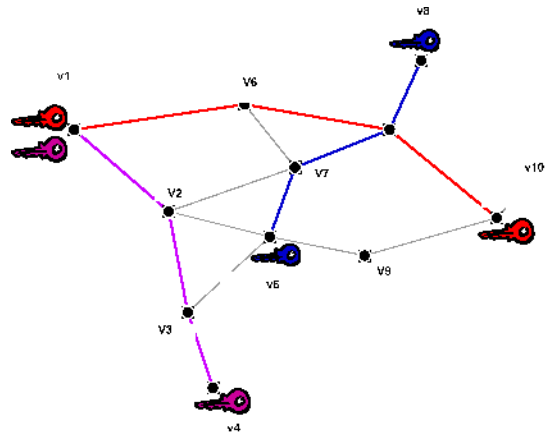
Pulse Protocol

- **Utilizes a periodic flood (the pulse) initiated by a single node (the pulse source) to provide routing and synchronization**
- **The *spanning tree* rooted at the pulse source is used to forward packets and serves as the center of the tree**
  - The nodes are able to *synchronize* with the periodic pulse, allowing idle nodes to power off their radios a large percentage of the time to conserve power
  - *For mobility, it is necessary that all nodes participate in the routing protocol*

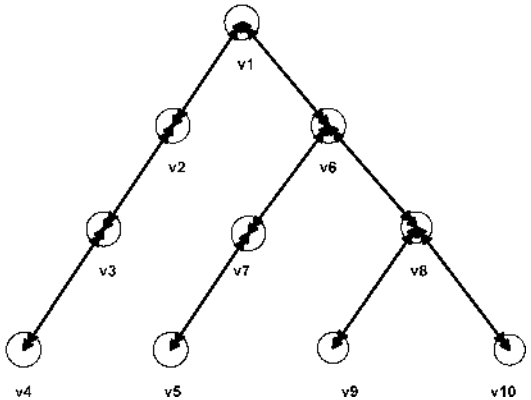


Pulse Protocol (Proactively updated spanning tree which is a compressed representation of the mesh)

Pulse Source



Pulse Source



PROCESS CONTROL SYSTEMS FORUM

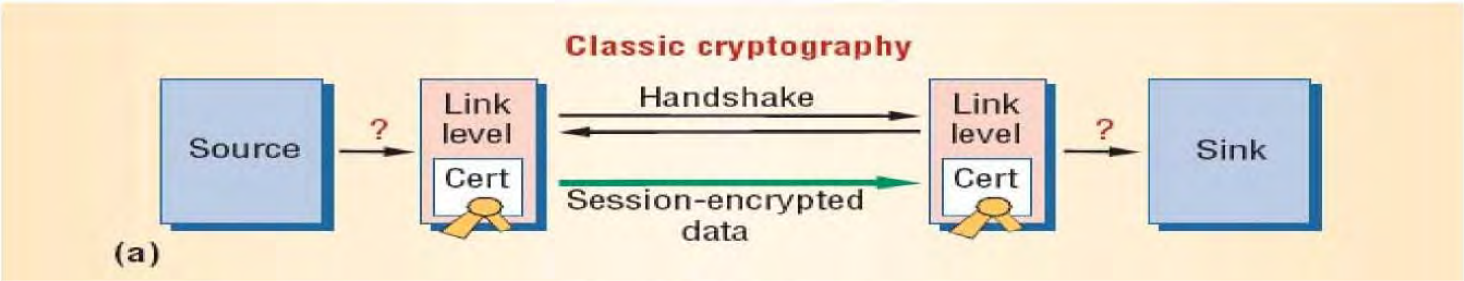
- *What type of encryption is used?*

Advanced Encryption

- Each device is initially given a collection of *keys* and makes use of *symmetric encryption (AES-256-CCMP)*
- Each devices utilizes a *hardware accelerator* for substantial increase in performance required for Quality of Service (QoS) over multiple hops
- Infrastructure mode utilizes *IEEE 802.11i/WPA2*
- Mesh infrastructure protects both data & control packets

- *What Key Management is scalable for wireless industrial networks? (Public vs. Broadcast)*

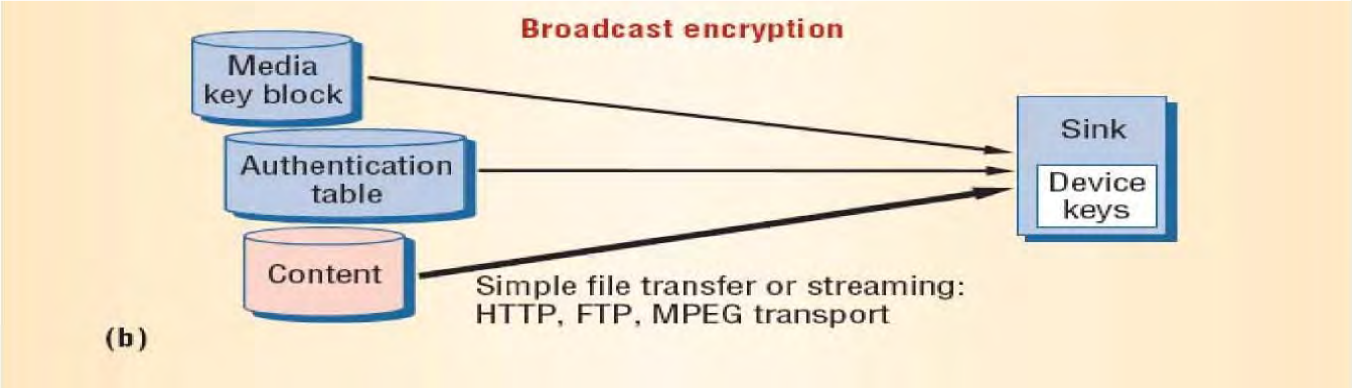
Public Key (PK) Key Management



- **PK uses asymmetric encryption makes forging digital signatures difficult due to mathematic code complexity**
- **Link level handshake for authorization and the key exchange is easier to eavesdrop**
- **Used to establish a secure user session**
- **Management is more complex for large groups of users**

Broadcast Key Management (as used by the Cable industry)

- **First introduced in 1994, known as "*Broadcast Encryption*"**
- **Used today, as a framework for secure communications over a broadcast channel, such as pay-TV, or the Internet**
- **Used to transmit content to a large group of devices**
- **Sender may control access to media content**
- **Managed by broadcast inclusion or exclusion**



Broadcast Encryption (BE) (Mesh Networks)

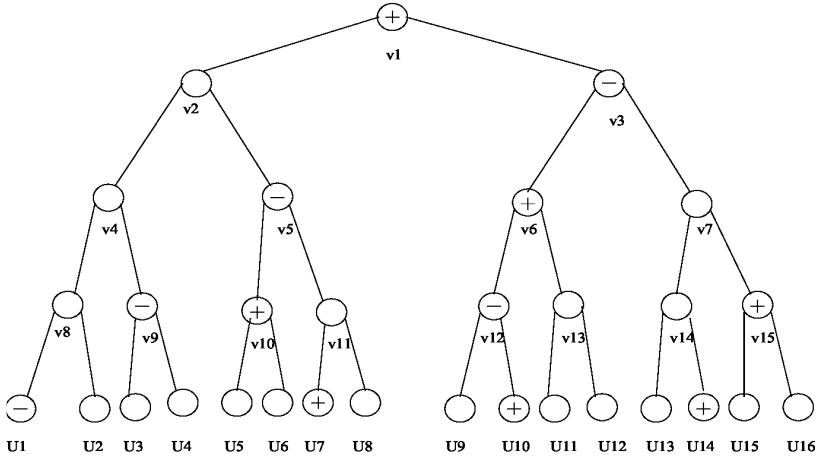
- **Goals for use of BE with mesh networks**
  - Provide scalable method for a large number of devices and secrets may only be exchanged between privileged devices
  - Coalitions of devices the are not in the privileged set cannot obtain a shared secret to decrypt information
  - Provides a means to partition network into subsets of nodes with keys for data and control
  - Multiple keys can be used to identify members of a group and define policies for traffic handling

Broadcast Encryption (BE) (in general)

- **Hides keys deep in the OS making it difficult to detect**
- **Replaces the digital signature with the use of a Hash Message Authentication Code (HMAC)**
- **Combines high performance with easy management**
- **Each device has pre-arranged set of keys and must be authorized by the administrator to join the network**
- **Each device will use a Secret Key to compute and verify the MAC, used during transactions to verify that a device is "trusted" and allowed to participate in the network**

BE Algorithm: Layered Subset Difference (LSD)

- **Each device performs inexpensive operations to decrypt a message**
- **LSD scheme uses *less than 1 kilobyte of storage* for each node, and the pulse source can revoke any *r* out of 2^28 *nodes* by sending on average a message of length 2*r*.**



Summary

- **High Performance**
  - L2 multi-layer switching allows ANY L3 protocol enabling converged services such as VoIP, video multi-casting, real-time applications, and mobility.
- **Proactive Route Selection**
  - Pulse Protocol with Medium Time Metric (MTM) provides proactive route selection for wireless mesh mobility.
- **Hardware Accelerators**
  - Optimizes performance for Quality of Service over multiple hops
- **LSD BE**
  - provides scalable, yet easy key management to insure that all devices are "*Trusted*" to participate in packet routing and additional traffic handling for large groups of devices.
- ***Together they offer secure wireless mesh mobility***

Industrial Plants Un-Wired!

- Thank you!