Security Requirements for PTP in real world deployment

Kamatchi Gopalakrishnan
kamatchi@juniper.net

Nov 6th – 8th 2012

ITSF - Nice, France

AGENDA

- Security Threats and Classification
- Methods to improve PTP security
- Protocol Intelligence
- Authentication and Data integrity
- Threats in Service Provider/Mobile Backhaul network
- Threats in Enterprise/Financial network
- Summary

SECURITY THREATS AND CLASSIFICATION

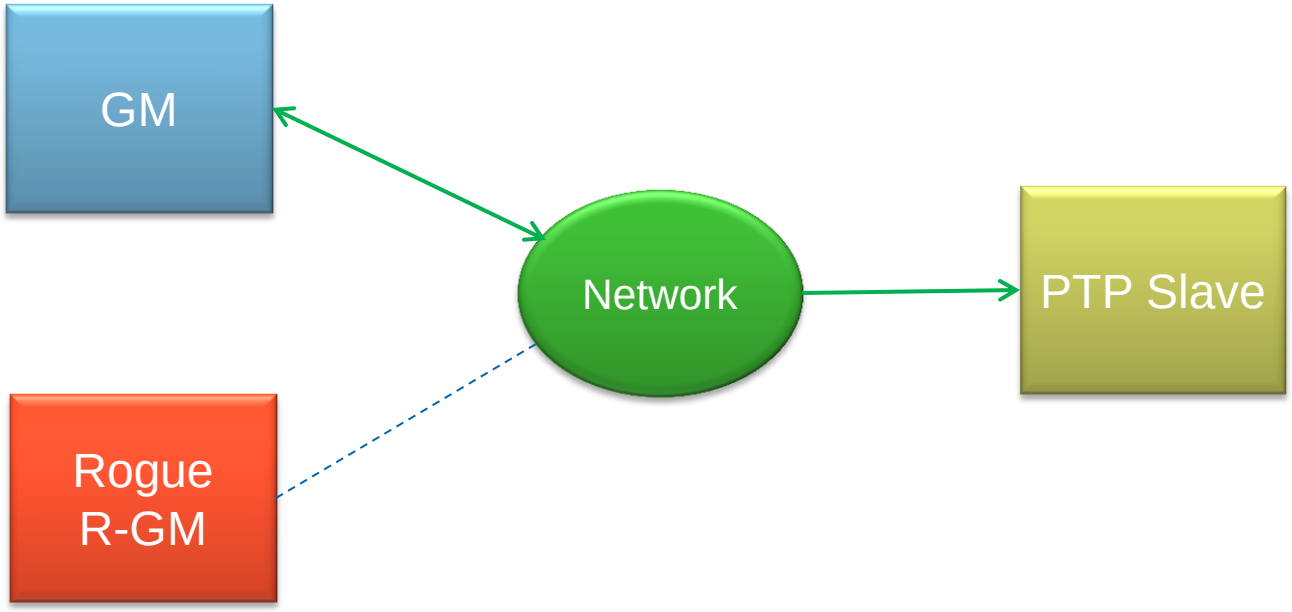
- Direct threats
  - Purpose of the threat is to attack/exploit PTP – Functionality, Accuracy.
- Indirect Threats
  - Purpose of the threat is to attack/exploit other protocols that in turn affects PTP.

DIRECT THREATS

- Rogue PTP Master
- Rogue BMCA trigger
- Denial of Service (DoS) using Rogue Slave
- Correction field Manipulation
- Packet Interception
- Packet Replay
- Address Spoofing
- Device compromise

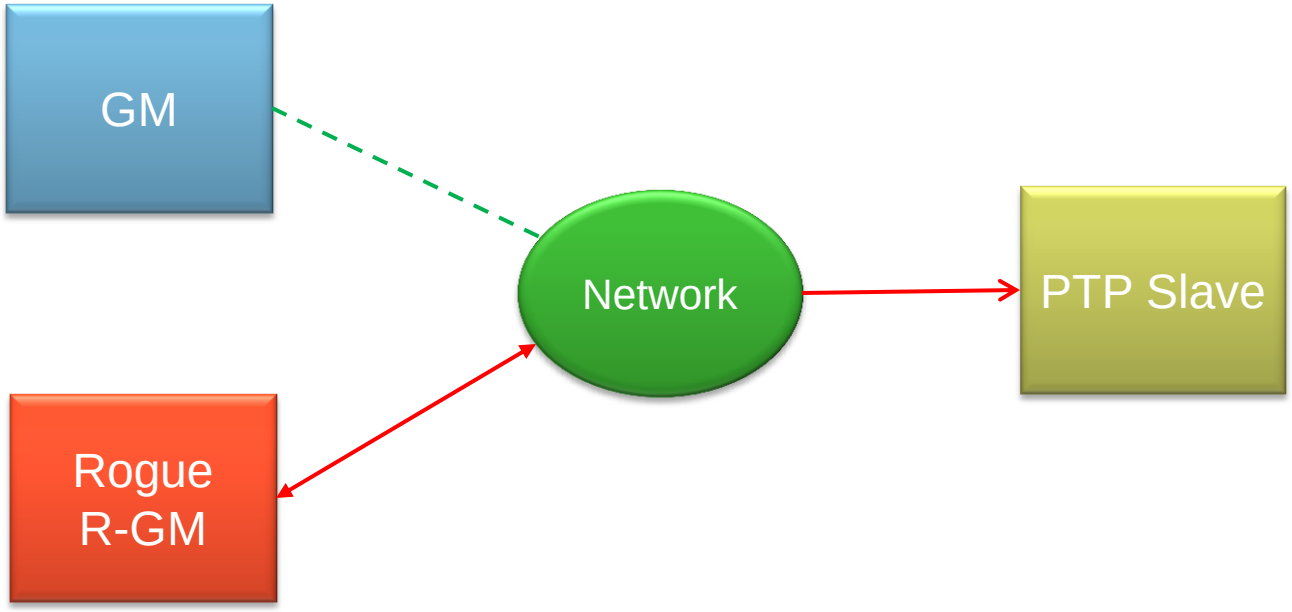
DIRECT THREAT:
ROGUE BMCA TRIGGER - GENUINE GM (ACTIVE)

GM (P1) > R-GM (P1)



DIRECT THREAT:
ROGUE BMCA TRIGGER – ROGUE GM (ACTIVE)

R-GM (P1) > GM (P1)

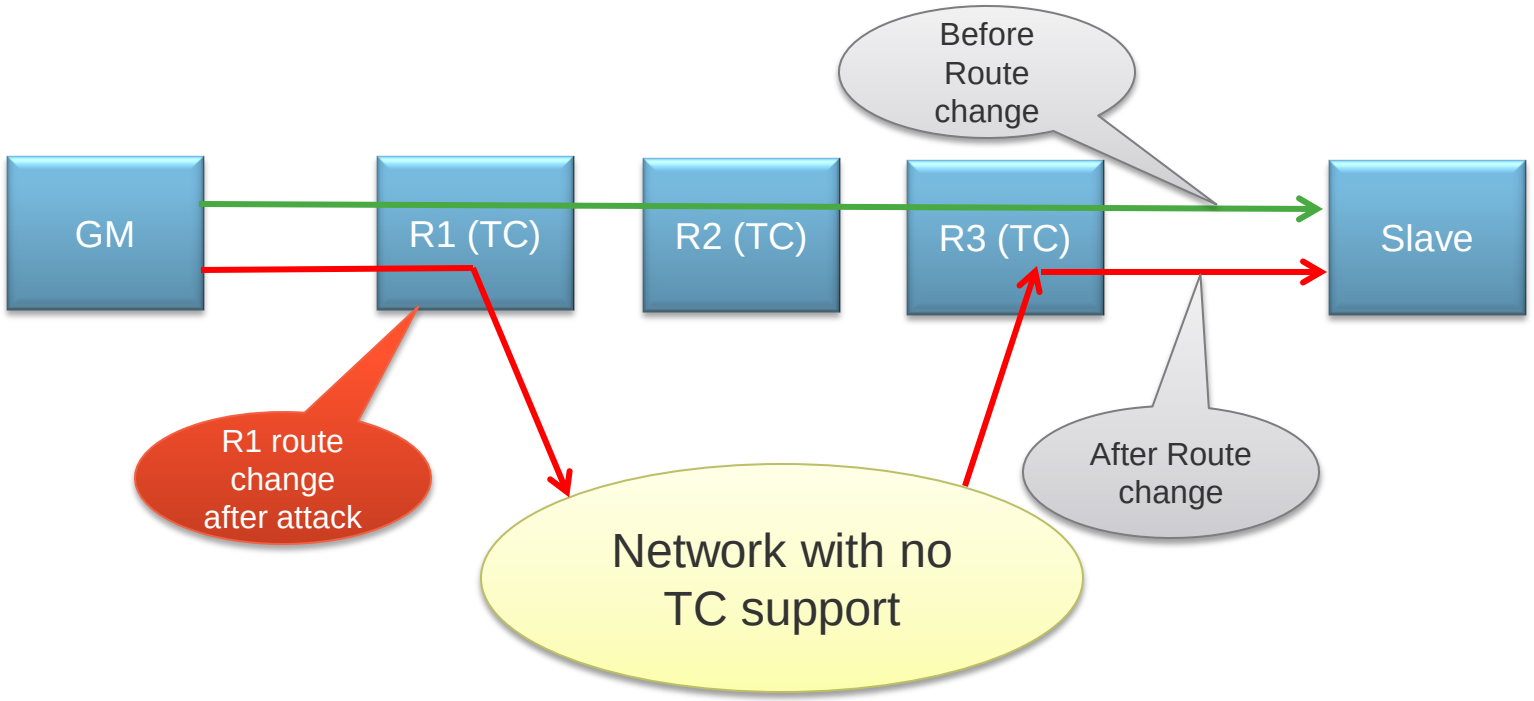


Mitigation: Authentication of GM

INDIRECT THREATS

- Route Change (route injection attack)
- Correction field time-stamping inaccuracy in case of TC
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Infected/Malfunctioning machines causing excessive traffic and resource depletion.
- New Network Upgrade – Creating a loop

INDIRECT THREAT: ROUTE CHANGE (ROUTE INJECTION ATTACK)

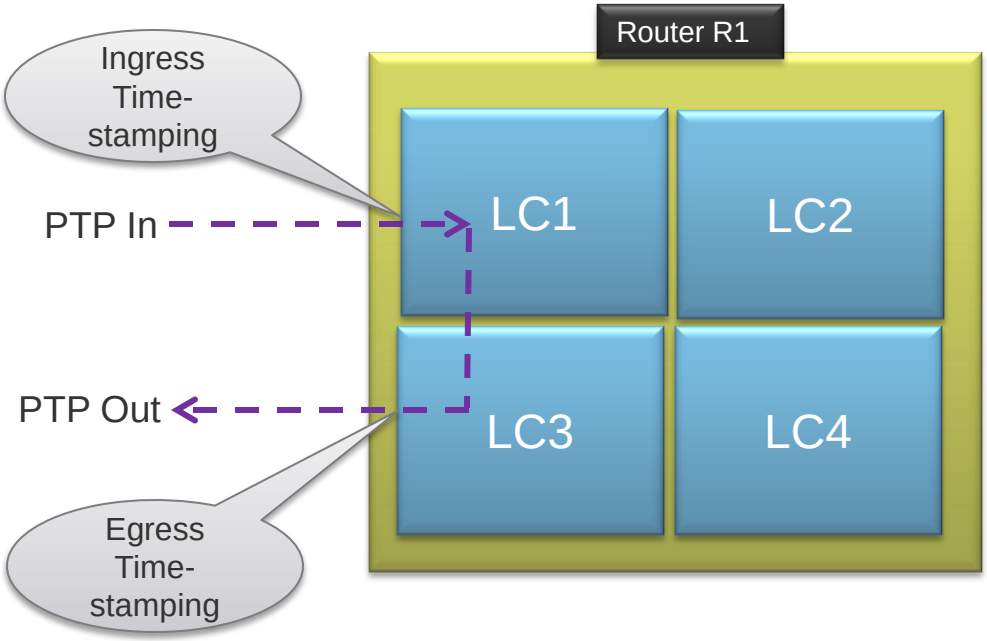


1. Downgraded PTP accuracy
2. Mitigation
   a. Interpretation of Correction field value
   b. TTL value
   c. Record route info

INDIRECT THREAT
CORRECTION FIELD INACCURACY IN TC

- Resident time = (Egress – Ingress)
- Different ways to calculate and update the correction field for resident time (Ingress to Egress)
  - Inline correction field update both at Ingress and Egress (1)
    At Ingress = Correction field – Ingress time-stamp
    At Egress = Correction field + Egress time-stamp
  - Update correction field only at Egress (2)
    At Ingress = Store Ingress time stamp at end of packet
    At Egress = Subtract Egress time stamp from Ingress time-stamp
  - Out of band correction field update in case of two step mode
- In case of inline correction field update - if Egress does not support PHY time-stamping, PTP packets will be sent out with invalid value in correction field.
- Or If Ingress and Egress PHY time-stamping differs. Lets say (1) and (2)

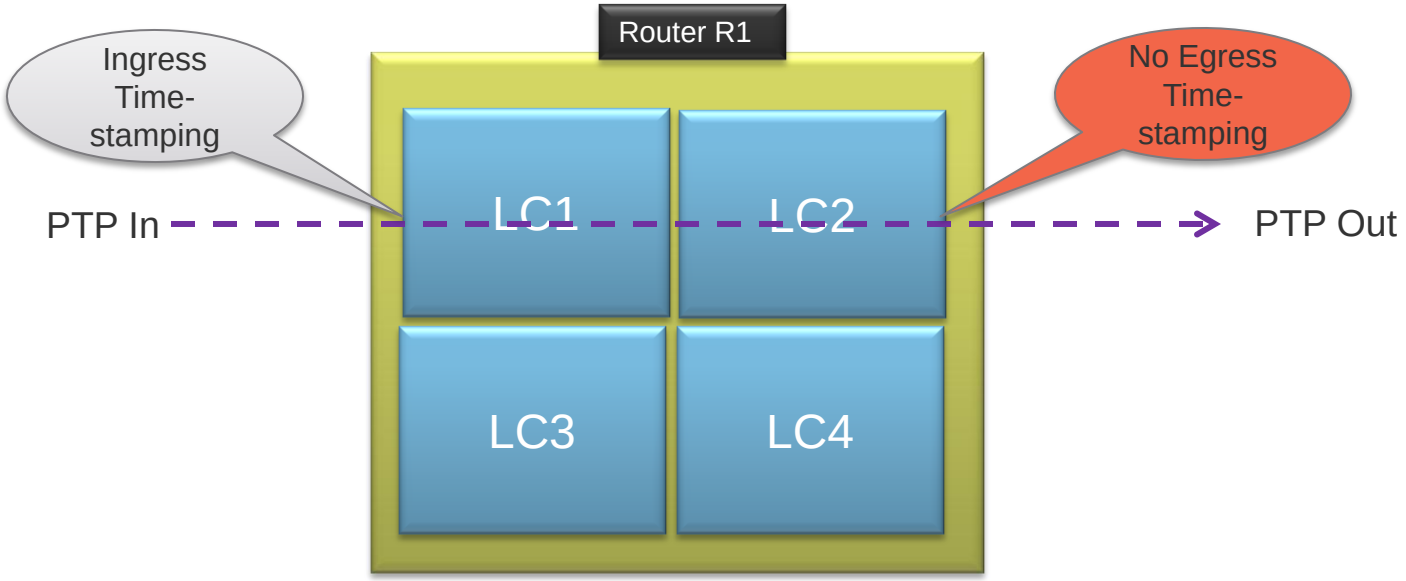
TC INLINE CORRECTION FIELD UPDATE: - NORMAL OPERATION



LC1 and LC3 inline PHY time-stamping capable

LC2 and LC4 NO PHY time-stamping capable

TC INLINE CORRECTION FIELD UPDATE: - ROUTE CHANGE



LC1 and LC3 inline PHY time-stamping capable

LC2 and LC4 NO PHY time-stamping capable

Mitigation: Ensure all line cards support TC and support same method to update the correction field.

METHODS TO IMPROVE PTP SECURITY PART 1: PROTOCOL INTELLIGENCE

- User based filtering – To prevent Rogue Master and Rogue Slave associations
- TTL based path length detection – useful for route-change detection
- Usage of correction field to detect packet legibility
- Record route based path information – useful for route-change detection
- DoS attack detection and mitigation
- Monitoring and Incident recording/reporting

VERY SIMPLE (PTP) SERVO ALGORITHM

- Set an alignment interval (say 2 or 5 minutes)
- Set target min-packets or lucky packets to be received during alignment interval (ex: 10 packets)
- Set target threshold value (Say: 1usec)
- Set the rate with which adjust the calculated phase (Ex: 5, 25 or 100 nsec/sec)
- Now if 10 packets received within the alignment interval ranging with in the target threshold value either adjust the new phase/Time or do not react to the phase/time determined.

- Modified algorithm would consider the following before taking decision to apply the change in phase in case of route change.

- Compare the TLL value received to detect the hop change
- Compare the record route information for change
- Compare the correction field value change in connection with TTL and/or record route changes.

Assumption: PTP over IPv4 in Transparent Clock mode.

METHODS TO IMPROVE PTP SECURITY
PART 2: AUTHENTICATION AND DATA-INTEGRITY

- Authentication
  - Identification and Authorization
  - Authentication of Master
  - Authentication of Slave
  - Authentication of Transparent clocks (p2p)
  - Authentication of Announce messages
  - Configured keys or infrastructure based key distribution
- Data Integrity
  - Integrity of packet using message digestion/hashing (MD5 or SHA)

PTP DEPLOYMENT - TWO AREAS OF INTEREST

- Service provider/Mobile Backhaul network
  - Threat: Mostly Indirect threats like network route-change, Incorrect correction-field update, DoS, DDoS, Network upgrade
  - Damage: Accuracy degradation
  - Possible Solution: Protocol Agnostic support
- Enterprise/Financial network
  - Threat: Both Direct and Indirect attacks possible.
  - Damage: False time, Accuracy degradation
  - Possible solution: Authentication, Data-integrity and Protocol Agnostics

SUMMARY

- Threats and severity depends on where the PTP is deployed.

- Processing and handling of some additional information like TTL, record route or Correction field, the route change can be determined and packet servo can be implemented to take into these factors before deciding on the time calculation and /or adjustment.

everywhere