Tattle Tale Security: An Intrusion Detection System for Medical Body Area Networks (MBAN)

Lanier Watkins*, Shreya Aggarwal*, Omotola Akeredolu*, William H. Robinson**, and Aviel Rubin*

Johns Hopkins University Information Security Institute*

Vanderbilt University**

Objectives

- To Identify and discuss the Remote Patient Monitoring Security Problem
- To discuss our approach
- To discuss Tattle Tail security operations
- To discuss our threat model
- To discuss Contiki Model demonstration

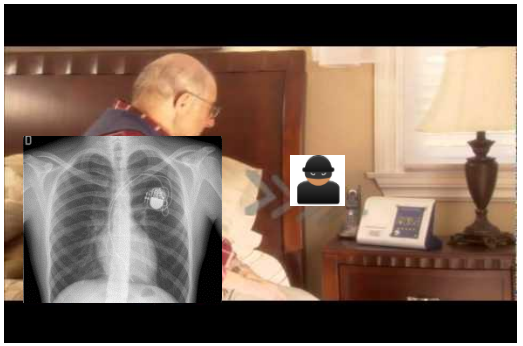
Agenda

- Remote Patient Monitoring Security Problem
- Previous Work
- Our Approach
- Tattle Tail Security Operations
- Threat Model
- Limitations/Assumptions
- Experimental Evaluation
- Contiki Hardware Model Demonstration
- Conclusion and Future Work

Current Problem:

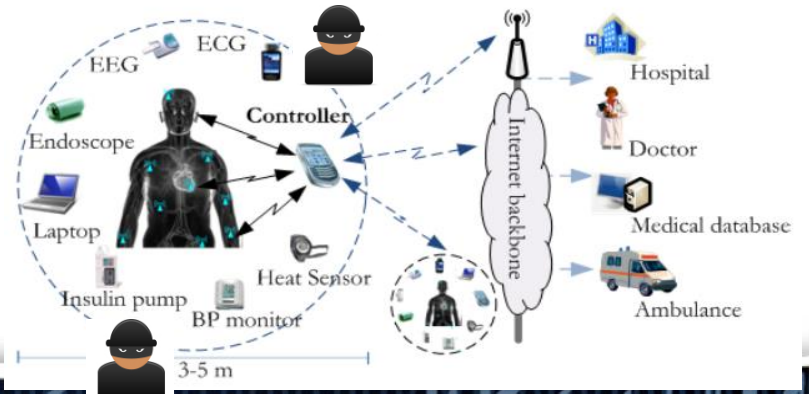
Vulnerabilities Plague Remote Patient Monitoring Networks

- IoT Healthcare market is forecasted to reach $14 Billion by 2022 [1]
- Remote Patient Monitoring (RPM) is the leading telemedicine application
  - Vulnerabilities have already been found in these networks
- RPM networks will become a ***collaborative network*** of IoT devices
  - Malware will eventually seep into these networks
- Security required down to node level



Merlin@home

- **ICS-CERT Advisory [2]**
  - MITM vulnerability



Previous Work

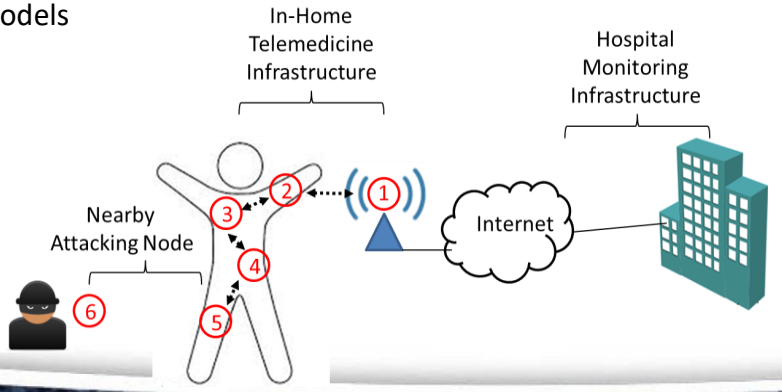
- Ma et al. proposed a Self-Adaptive Intrusion Detection (SAID) system, which works like an immune system capable of learning different pathogens and morphing to defend against new attacks. Rule set is likely complex and not feasible for real MBANS.
- Hai et al. proposed an intrusion detection system based on local and global agents that monitor packets moving in and out of each node and packet moving throughout the network, respectively. Rule set is likely complex and not feasible for real MBANS.
- Sampangi et al. proposed an encryption-based method that focuses on securing inter-sensor communication as well as securing communication with the gateway. Encryption will likely over use processing resources.

TABLE I. COMPARISON WITH OTHER METHODS

Method	Description	Simulation	Threat Model
"Tattle Tale"	Anomalous Power Detection	Contiki	Active Attacks
Ma et al. [3]	Agent Based, Two-Hop	NS2	Routing Attacks
Hai et al. [4]	Major Voting, Two-Hop	Castalia	Routing Attacks
Sampangi et al. [5]	Encryption	Java Code	Key Attacks

Approach and Novelty of Method

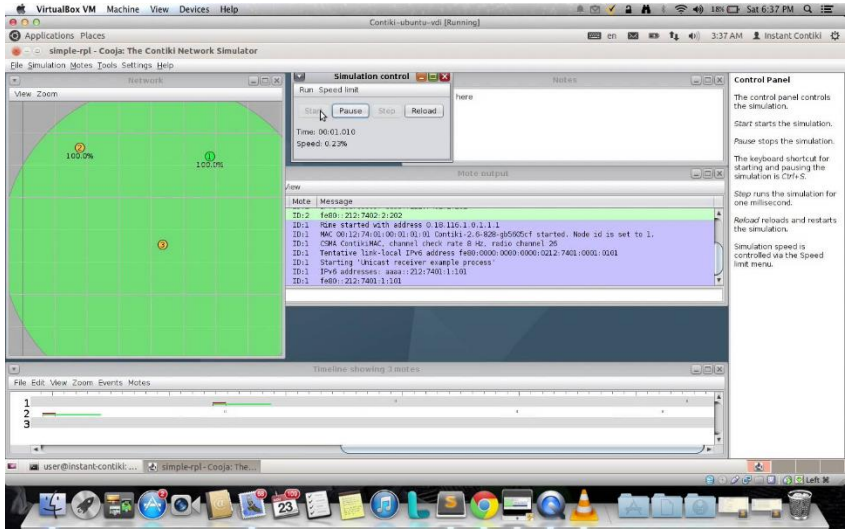
- Leveraged wireless sensor node research from our previous work (J. Chandramouli et al. [6]) to develop a security method for MBANS
  - Security on top of low energy routing protocol
    - Multi-hop – decreases node power usage
    - Fixed packet size – makes power consumption predictable
    - Synchronized dynamic duty cycling – every node sends traffic relative to battery power level
  - Reduces security to identifying nodes with anomalous power levels
  - Demonstrate feasibility using Contiki hardware model
    - Node Discovery
    - Multi-Hop Routing
    - Battery
    - Dynamic Duty Cycling
    - Packet Layout
    - Security Algorithm
    - Threat Models

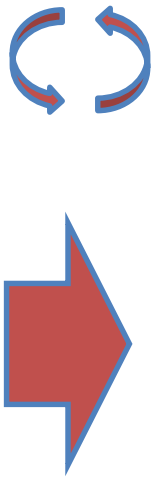


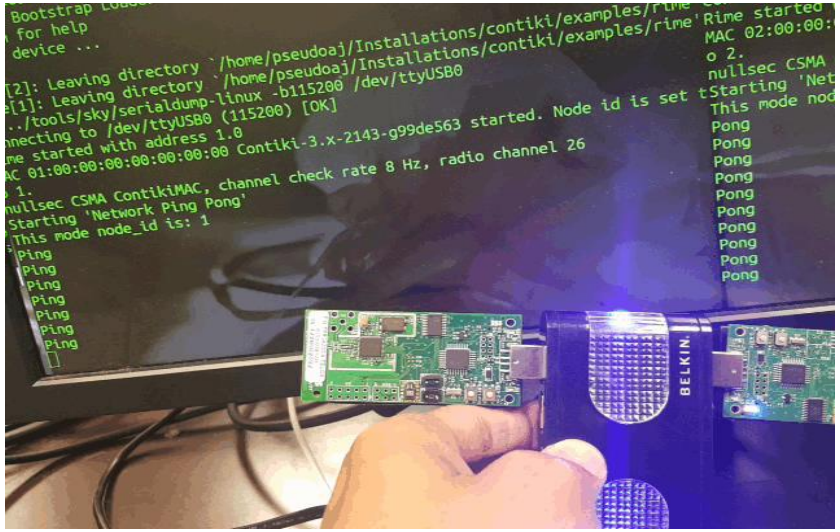
Benefit of Tattle Tail Security Method

- There is a clear path for Hardware Prototyping of Tattle Tail Security
  - Security algorithm written in software, tested in simulated hardware, and evaluated
  - Porting to hardware can be done a minimum number of times

MBAN Hardware Prototyping Design-Build-Test Cycle

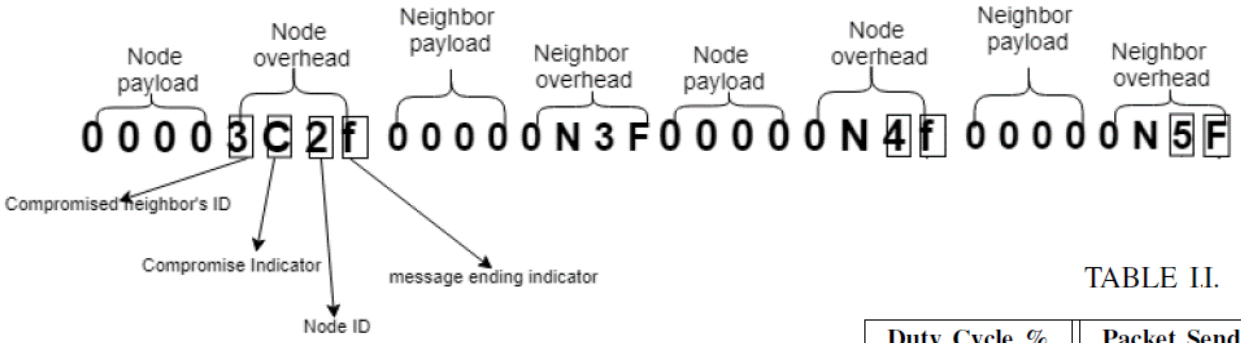






Tattle Tail Security Operations

- Fixed sized MBAN packets, uncompromised nodes have same size packets
- Compromised nodes have out of sync duty cycles, thus different sized payloads



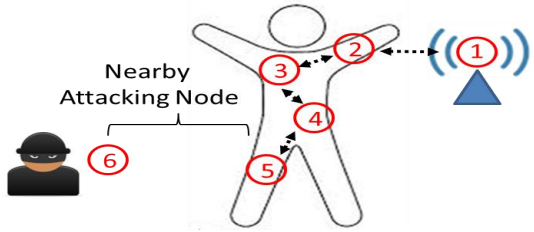


Table III. : Battery discharge simulation parameters. [7]

Sensor sampling rate (Hz)	Heart Rate	4
	ECG	20
	Body Temperature	0.2

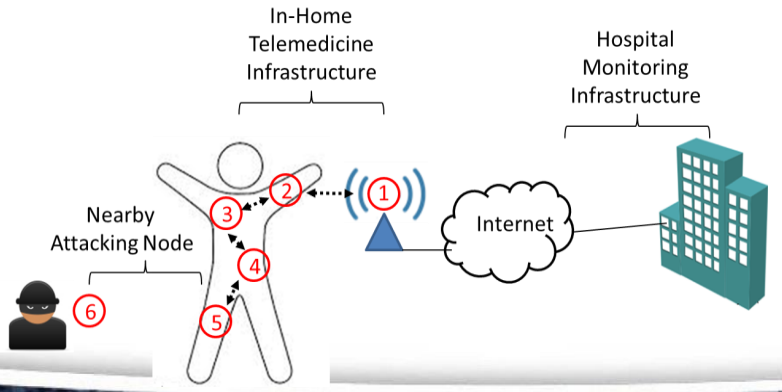
TABLE I.I. DUTY CYCLE LEVELS [6]

Duty Cycle %	Packet Send Rate	Energy Range
100	Po	E(n) >= 0.84*Eo(n)
35.5	Po/2	E(n) < 0.84*Eo(n) and >= 0.68*Eo(n)
11.5	Po/4	E(n) < 0.68*Eo(n) and >= 0.52*Eo(n)

- Normal Operation Example: 2222 0N2f 3333 0N3f 4444 0N4f 5555 0N5f
- Attack Operation Example: 2222 3C2f 33 0N3f 4444 0N4f 5555 0N5f

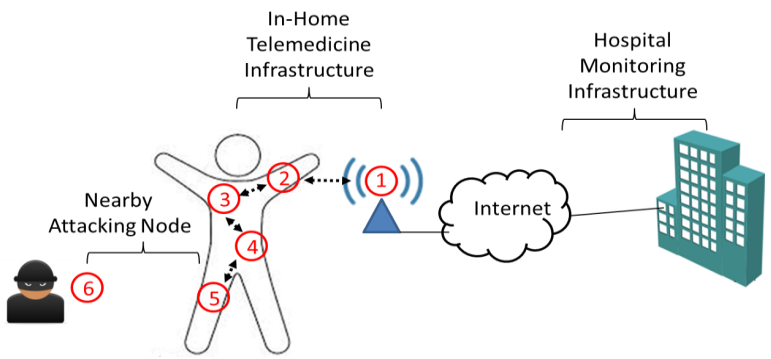
Threat Model

- 3 Type of Active Attacks
  - Node Capture Attack
    - Attacker node connects to target node and assumes control of target
    - The process of connecting to target dissipates target's batteries, which is detectable by our method
  - Denial of Service Attack
    - Attacker node connects to target and continues to send packets to it until target dies
    - The process of continuously sending packets to target dissipates target's batteries, which is detectable by our method
  - Replay Attack
    - Attacker node forwards an old packet to the target
    - The process sending an old packet to target dissipates target's batteries, which is detectable by our method. Takes longer for neighbor to detect.



Limitations and Assumptions

- No Micro Attacks
  - Attackers closers than node's neighbor
- No Passive Attacks
  - Do not dissipate power
- No Multiple Attacks
  - Were not tested, but can likely detect

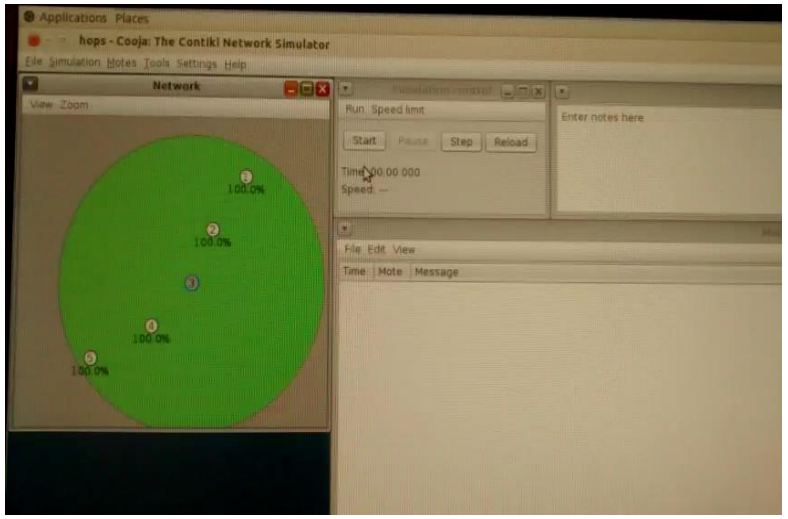


- Received packets are acknowledged with minimum length packet
- Nodes know how to account for energy loss of new neighbors that are skipping over their nearest neighbor due to compromise
- More complex node compromise logic is possible at the gateway
- Detection time is appropriate to identify immediate threats
- Sacrificing precision is not a significant for MBAN application

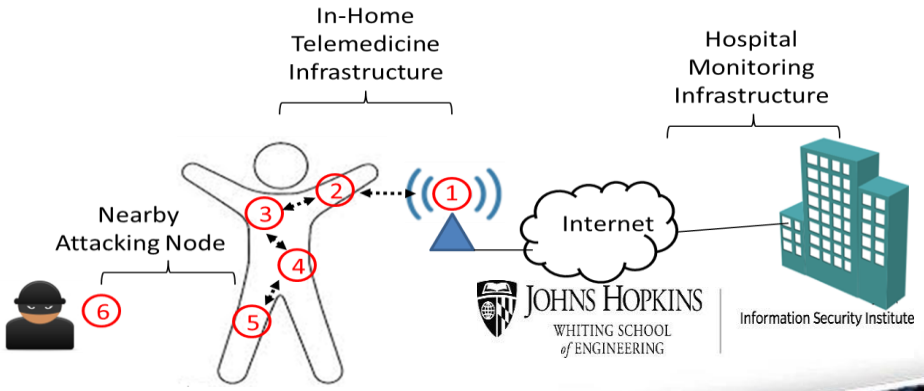
Experimental Evaluation: Setup and Procedure

- Experimental Setup
  - Contiki, WSN operating system with simulated hardware nodes using Cooja
    - 6 sensor nodes
      - 5 nodes (nodes 1-5) are MBAN and gateway
      - 1 node (node 6) is the attacker node
    - All MBAN nodes start with same battery level
    - Each node sends a packet per round
    - Energy dissipation per round based on First Order Radio Model
    - As power level dissipates, all nodes duty cycle at same rate

Contiki and Cooja Tesbded



- Experimental Procedure
  - Nodes find neighbors during discovery
  - Attacker node is outside of discovery
  - Normal node operation commences
  - Attacker node wages 1 of 3 attacks
    - All attacks are active, attacker communicates with target
  - Nodes announce their activity



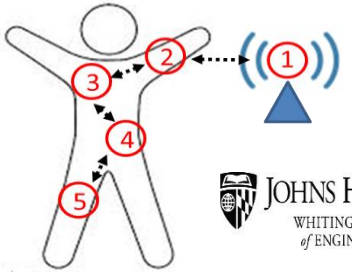
Contiki Hardware Model: Normal Operation

Hardware Nodes Start-Up		
00:00.5	ID:2	Rime started with address 2.0
00:00.5	ID:2	MAC 02:00:00:00:00:00:00:00 Contiki-2.6-900-ga6227e1 started. Node id is set to 2.
Node Discovery		
00:04.3	ID:4	Got announcement from 3.0, id 135, value 0, rss -34, distance 2
00:04.3	ID:4	Adding new neighbor 3.0
00:04.3	ID:4	Neighbors List:
00:04.3	ID:4	ID: 5.0, Distance: 2
00:04.3	ID:4	ID: 1.0, Distance: 6
00:04.3	ID:4	ID: 2.0, Distance: 3
00:04.3	ID:4	ID: 3.0, Distance: 2
Normal MBAN Operation 1 Round		
00:16.6	ID:4	ROUND: 1
00:16.6	ID:4	Forwarding packet with content 01239N4f01239N5FFFFFFFFFFFFFFFF and size 33 to 3
00:16.6	ID:4	Battery: 9764
00:16.7	ID:3	Message received '01239N4f01239N5FFFFFFFFFFFFFFFF' with size 33 from 4
00:16.7	ID:3	Battery: 9882
00:17.0	ID:5	ROUND: 1
00:17.0	ID:5	Send Rate: 4 bits
00:17.0	ID:5	Forwarding packet with content 01239N5FFFFFFFFFFFFFFFFFFFFFFFF and size 33 to 4
00:17.0	ID:5	Battery: 9764
00:17.1	ID:4	Message received '01239N5FFFFFFFFFFFFFFFFFFFFFFFF' with size 33 from 5
00:17.1	ID:4	Battery: 9646
00:17.2	ID:3	ROUND: 1
00:17.2	ID:3	Send Rate: 4 bits
00:17.2	ID:3	Forwarding packet with content 01239N3f01239N4f01239N5FFFFFFFF and size 33 to 2
00:17.2	ID:3	Battery: 9764
00:17.3	ID:2	Message received '01239N3f01239N4f01239N5FFFFFFFF' with size 33 from 3
00:17.3	ID:2	Battery: 9882
00:24.5	ID:2	Forwarding packet with content 01239N2f01239N3f01239N4f01239N5F and size 33 to 1
00:24.5	ID:2	Battery: 9764
00:24.5	ID:6	ROUND: 2
00:24.6	ID:4	ROUND: 2
00:24.7	ID:1	GATEWAY: Message received '01239N2f01239N3f01239N4f01239N5F' with size 33 from 2
00:24.7	ID:1	ROUND: 2

Rime communications protocol stack

Each node sends and receives discovery packets to build its neighbor list

Each node sends its data along with its neighbors data toward the gateway node (node 1)

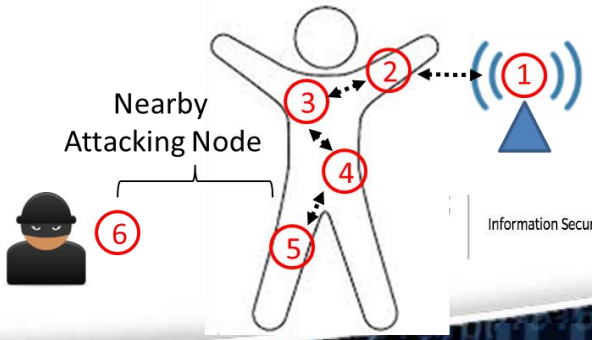


JOHNS HOPKINS WHITING SCHOOL of ENGINEERING | Information Security Institute

Contiki Hardware Model: Node Capture Attack

Node 6 Captures Node 3 and Node 2 Detects Power Dissipation In Node 3, Notifies the Gateway Twice, and Gateway Tells All Other Nodes to Ignore Node 3		
01:28.5	ID:6	ROUND: 10
01:28.5	ID:6	CAPTURED NODE ATTACK TO 3
01:28.5	ID:6	Forwarding packet with content HIHI9N6F and size 9 to 3
01:28.7	ID:3	Message received 'HIHI9N6F' with size 9 from 6
01:28.7	ID:3	Battery: 7632
01:29.3	ID:3	Forwarding packet with content PASS9N3F and size 9 to 6
01:29.3	ID:3	Battery: 7209
01:29.3	ID:3	Forwarding packet with content 019N3f019N4f01239N5FFFFF and size 25 to 2
01:29.3	ID:3	Battery: 7164
01:29.4	ID:6	Message received 'PASS9N3F' with size 9 from 3
01:37.3	ID:3	Forwarding packet with content 09N3f239N4f01239N5FF and size 21 to 2
01:37.3	ID:3	Battery: 6565
01:37.4	ID:2	Message received '09N3f239N4f01239N5FF' with size 21 from 3
01:37.4	ID:2	Battery: 8060
01:44.6	ID:2	COMPROMISED: Wrong send rate
01:44.6	ID:2	Forwarding packet with content 233C2f09N3f239N4f01239N5 and size 25 to 1
01:44.6	ID:2	Battery: 8015
01:44.7	ID:1	GATEWAY: Message received '233C2f09N3f239N4f01239N5' with size 25 from 2
01:44.7	ID:1	ROUND: 12
01:44.7	ID:1	GATEWAY: Mote 3 may be compromised...
01:45.3	ID:3	Battery: 6547
01:52.6	ID:2	COMPROMISED: Wrong send rate
01:52.6	ID:2	Forwarding packet with content 013C2f19N3FFFFFFFFFFFFF and size 25 to 1
01:52.6	ID:2	Battery: 7952
01:52.7	ID:1	GATEWAY: Message received '013C2f19N3FFFFFFFFFFFFF' with size 25 from 2
01:52.7	ID:1	ROUND: 13
01:52.7	ID:1	GATEWAY: Mote 3 may be compromised...
01:52.7	ID:1	GATEWAY: Mote 3 is compromised. Broadcasting...
01:52.7	ID:5	Broadcast message received from Gateway: 'G3CF'
01:52.8	ID:4	Broadcast message received from Gateway: 'G3CF'
01:52.8	ID:2	Broadcast message received from Gateway: 'G3CF'

- Attacker node 6 communicates with node 3
- Node 3 experiences a drop in battery power level, but then tries to continue its normal operations
- Node 2 detects Node 3's incorrect send rate
- Node 2 reports the compromise to the gateway
- Gateway reports compromise to all other nodes

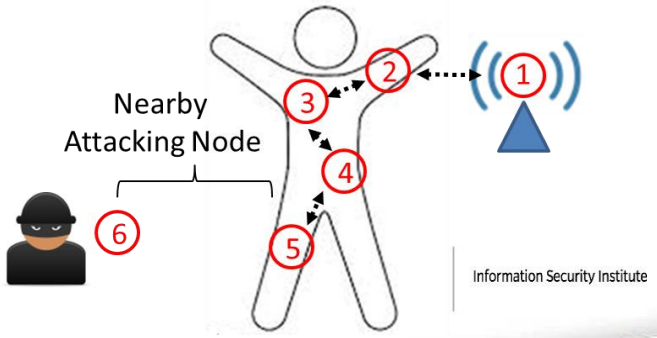


Contiki Hardware Model: DoS Attack

Node 6 DoS Attack on Node 5 Until Node 5 Dies, After A Couple of Rounds Node 4 Realizes Node 5 Is Dead and Notifies Gateway, and Gateway Notifies All Other Nodes

00:32.5	ID:6	DOS ATTACK TO 5
00:32.5	ID:2	Forwarding packet with content 01239N2f01239N3f01239N4f01239N5F and size 33 to 1
00:32.5	ID:2	Battery: 9528
00:32.5	ID:6	Forwarding packet with content 00009N6F00000000000000000000000 and size 33 to 5
00:32.6	ID:5	Message received '00009N6F00000000000000000000000' with size 33 from 6
00:32.6	ID:5	Battery: 7680
00:32.7	ID:5	Battery: 0
00:32.7	ID:5	Message received '00009N6F00000000000000000000000' with size 33 from 6
00:32.7	ID:5	Battery: 0
00:32.8	ID:3	Message received '01239N4f01239N5FFFFFFFFFFFFFFFF' with size 33 from 4
00:32.8	ID:3	Battery: 9410
00:32.9	ID:1	GATEWAY: Message received '01239N2f01239N3f01239N4f01239N5F' with size 33 from 2
00:56.7	ID:4	COMPROMISED: Not receiving messages
00:56.7	ID:1	ROUND: 6
00:56.7	ID:4	Forwarding packet with content 01235C4FFFFFFFFFFFFFFFFFFFFFFFF and size 33 to 3
00:56.7	ID:4	Battery: 8938
00:56.8	ID:3	Message received '01235C4FFFFFFFFFFFFFFFFFFFFFFF' with size 33 from 4
00:56.8	ID:3	Battery: 8702
00:57.2	ID:3	ROUND: 6
00:57.2	ID:3	Send Rate: 4 bits
00:57.2	ID:3	Forwarding packet with content 01239N3f01235C4FFFFFFFFFFFFFFFF and size 33 to 2
00:57.2	ID:3	Battery: 8584
00:57.3	ID:2	Message received '01239N3f01235C4FFFFFFFFFFFFFFFF' with size 33 from 3
00:57.3	ID:2	Battery: 8702
01:04.6	ID:2	ROUND: 7
01:04.6	ID:2	Send Rate: 4 bits
01:04.6	ID:2	Forwarding packet with content 01239N2f01239N3f01235C4FFFFFFFF and size 33 to 1
01:04.6	ID:2	Battery: 8584
01:04.6	ID:6	ROUND: 7
01:04.7	ID:1	GATEWAY: Message received '01239N2f01239N3f01235C4FFFFFFFF' with size 33 from 2
01:04.7	ID:1	ROUND: 7
01:04.7	ID:1	GATEWAY: Mote 5 may be compromised...

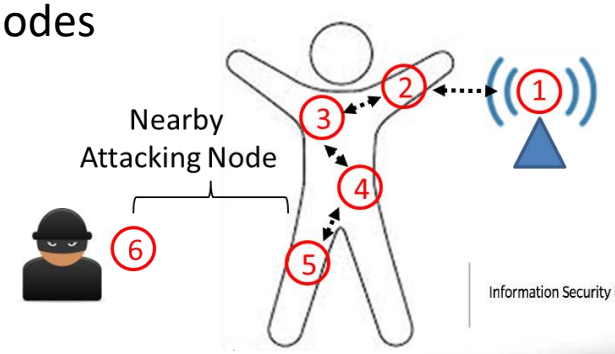
- Attacker node 6 does DoS on node 5
- Node 5's battery power level eventually drops to 0
- After several rounds, Node 4 realizes Node 5 sends no packets
- Node 4 reports the compromise to the gateway
- The gateway reports compromise to all other nodes



Contiki Hardware Model: Replay Attack

Node 6 Replays Old Packet To Node 4, Node 4 Forwards Replayed Packet As Well As Normal Packets, Node 4 Sees A Battery Power Drop, Node 3 Detects It And Notifies The Gateway		
00:56.5	ID:6	REPLAY ATTACK TO 4
00:56.5	ID:6	Forwarding packet with content 01239N2f01239N3f01239N4f01239N5F and size 33 to 4
00:56.5	ID:2	ROUND: 6
00:56.6	ID:2	Send Rate: 4 bits
00:56.6	ID:2	Forwarding packet with content 01239N2f01239N3f01239N4f01239N5F and size 33 to 1
00:56.6	ID:2	Battery: 8820
00:56.6	ID:4	Message received '01239N2f01239N3f01239N4f01239N5F' with size 33 from 6
00:56.6	ID:4	Battery: 7316
00:56.7	ID:1	GATEWAY: Message received '01239N2f01239N3f01239N4f01239N5F' with size 33 from 2
00:56.8	ID:3	Battery: 8775
00:57.1	ID:5	Battery: 9174
00:57.1	ID:4	Message received '01239N5FFFFFFFFFFFFFFFFFFFFFFFF' with size 33 from 5
00:57.1	ID:4	Battery: 7035
00:57.2	ID:3	ROUND: 6
00:57.2	ID:3	Send Rate: 4 bits
00:57.2	ID:3	Forwarding packet with content 01239N3f01239N2f01239N3f01239N4f and size 33 to 2
00:57.2	ID:3	Battery: 8539
01:05.1	ID:4	Battery: 6872
01:05.2	ID:3	ROUND: 7
01:05.2	ID:3	Send Rate: 4 bits
01:05.2	ID:3	COMPROMISED: Wrong send rate
01:05.2	ID:3	Forwarding packet with content 01234C3f239N4f01239N5FFFFFFFFFF and size 33 to 2
01:05.2	ID:3	Battery: 8376
01:12.6	ID:2	Forwarding packet with content 01239N2f01234C3f239N4f01239N5FFF and size 33 to 1
01:12.6	ID:2	Battery: 8348
01:12.7	ID:1	GATEWAY: Message received '01239N2f01234C3f239N4f01239N5FFF' with size 33 from 2
01:12.7	ID:1	ROUND: 8
01:12.7	ID:1	GATEWAY: Mote 4 may be compromised...

- Attacker Node 6 replays old packet to node 4
- Node 4 experiences a drop in battery power level, but then tries to continue its normal operations
- Node 3 eventually detects Node 4's incorrect send rate
- Node 3 reports the compromise to the gateway
- The gateway notifies all other nodes



Conclusion and Future Work

- Tattle Tail Security
  - Security implemented on top of low power routing mechanism
  - Clear path to hardware prototyping
- Future Work
  - Relax limitations
  - Implement additional lightweight security mechanisms (e.g., obfuscation, use of nonce)

Questions?

Lanier Watkins, PhD
Senior Cyber Security Research Scientist
Lawrence R. Hafstad Fellow, JHU/ISI
Chairman of JHU Engineering Professionals CS & Cyber Security MS Programs
Lanier.Watkins@jhuapl.edu
404-406-5426

JOHNS HOPKINS WHITING SCHOOL of ENGINEERING | Information Security Institute

References

1. Zion Market Research, “Global IoT Healthcare Market Will Reach USD 14,660 million by 2022”,https://globenewswire.com/news-release/2018/02/01/1329984/0/en/Global-IoTHealthcare-Market-Will-Reach-USD-14-660-million-by-2022-Zion-Market-Research.html
2. https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01A
3. Ma, Jianqing, et al. “SAID: A Self-Adaptive Intrusion Detection System in Wireless Sensor Networks.” Information Security Applications Lecture Notes in Computer Science, pp. 6073.
4. Huh, Eui-Nam, and Tran Hong Hai. “Lightweight Intrusion Detection for Wireless Sensor Networks.” Intrusion Detection Systems, 2011, doi:10.5772/14849.
5. Sampangi, Raghav V. “A Security Suite for Wireless Body Area Networks.” International Journal of Network Security and Its Applications, vol. 4, no. 1, 2012, pp. 97116.
6. Chandramouli, J. M., et al. Using Network Traffic to Infer Compromised Neighbors in Wireless Sensor Nodes. In IEEE Annual Consumer Communications and Networking Conference (CCNC), 2017, pp. 10221023., doi:10.1109/ccnc.2017.7983279.
7. J. Khan et al. “Battery Life Cycle and Transmission Power Profile Analysis of a Wireless Body Area Network with Implanted Nodes” In Proceedings of International Symposium on Medical Information and Communication Technology, 2010.