Security of Mobile Ad Hoc and Wireless Sensor Networks

Edward Bonver
OWASP LA Board Member
Symantec Corporation
edward@owasp.org

OWASP
July, 2013

The OWASP Foundation
http://www.owasp.org

Agenda

- Intro
- What are MANETs and WSNs?
- Problem Space and Challenges wrt to Security

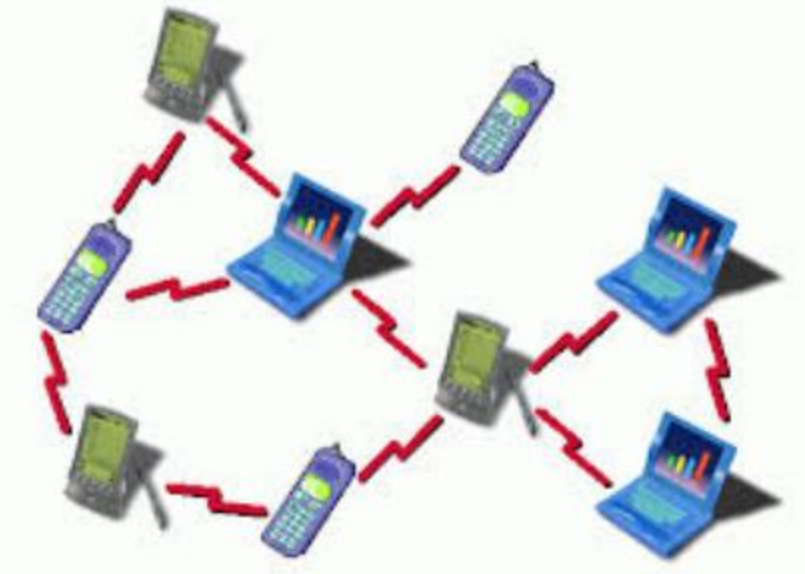
. . .

- Drinking @ BJ's Restaurant & Brewary, across the street

Who am I?

- Senior Principal Engineer, Office of the CTO, Symantec
  - Approaching 10 years @ Symantec
- Development @ QA engineering background
- Prior to Symantec: operating systems & networking protocols
- OWASP LA board member
- Father of three (future world changing persons)
  - Note to self: robot programming and first Emails…
- Computer Science Ph.D. student
- Famous for long introductions

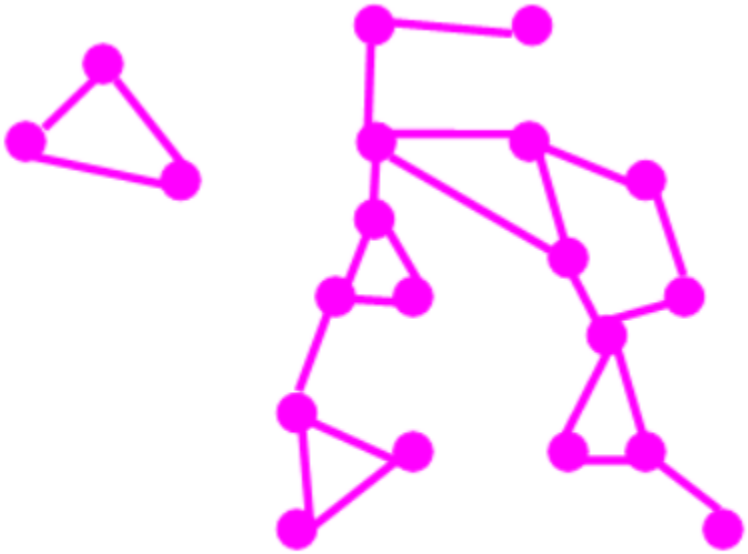
What are MANETs?



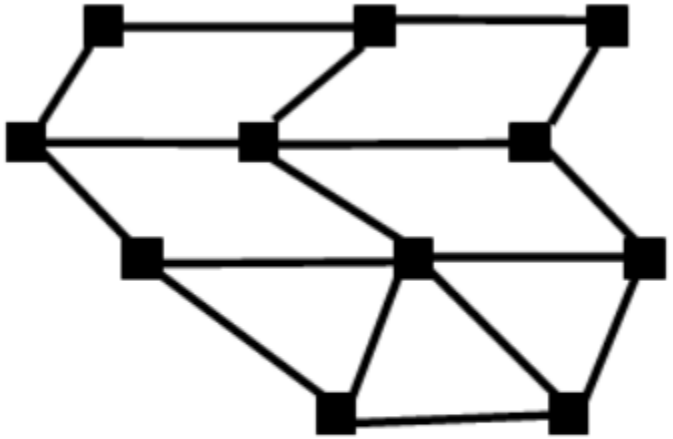
Mobile Ad-hoc Networks

- Do not rely on an existing infrastructure
- Wireless communications
- Mobile nodes (constantly changing topology)
- Nodes must be able to relay traffic, as communicating nodes might be out of range
- MANET can be self-forming and standalone or attached to other networks

MANET vs. “Traditional” Wireless Network



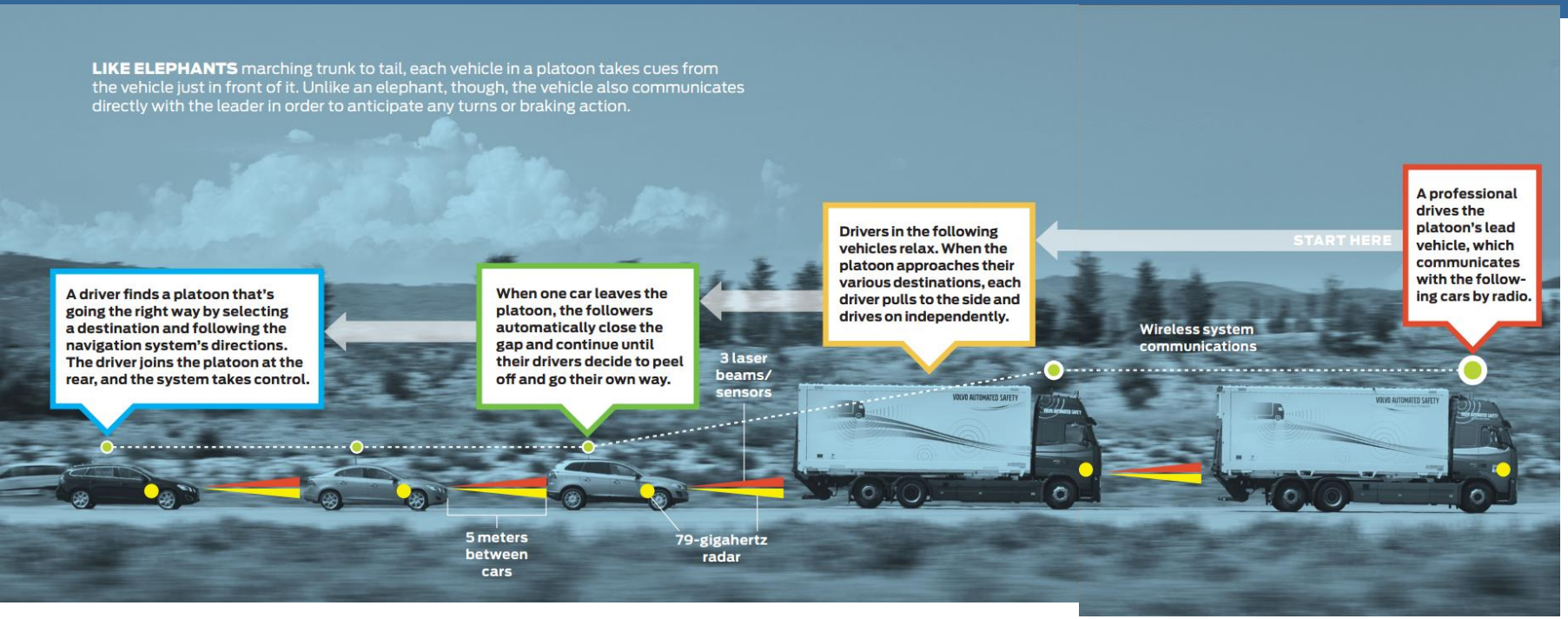
Mobile ad-hoc network



Wireless, fixed network

MANET Example: Vehicular Ad-Hoc Network (VANET)


VOLVO
HTK 167
VOLVO
VOLVO


LIKE ELEPHANTS marching trunk to tail, each vehicle in a platoon takes cues from the vehicle just in front of it. Unlike an elephant, though, the vehicle also communicates directly with the leader in order to anticipate any turns or braking action.
A professional drives the platoon's lead vehicle, which communicates with the following cars by radio.
START HERE
Drivers in the following vehicles relax. When the platoon approaches their various destinations, each driver pulls to the side and drives on independently.
When one car leaves the platoon, the followers automatically close the gap and continue until their drivers decide to peel off and go their own way.
A driver finds a platoon that's going the right way by selecting a destination and following the navigation system's directions. The driver joins the platoon at the rear, and the system takes control.
Wireless system communications
3 laser beams/ sensors
5 meters between cars
79-gigahertz radar

What are Wireless Sensor Networks?

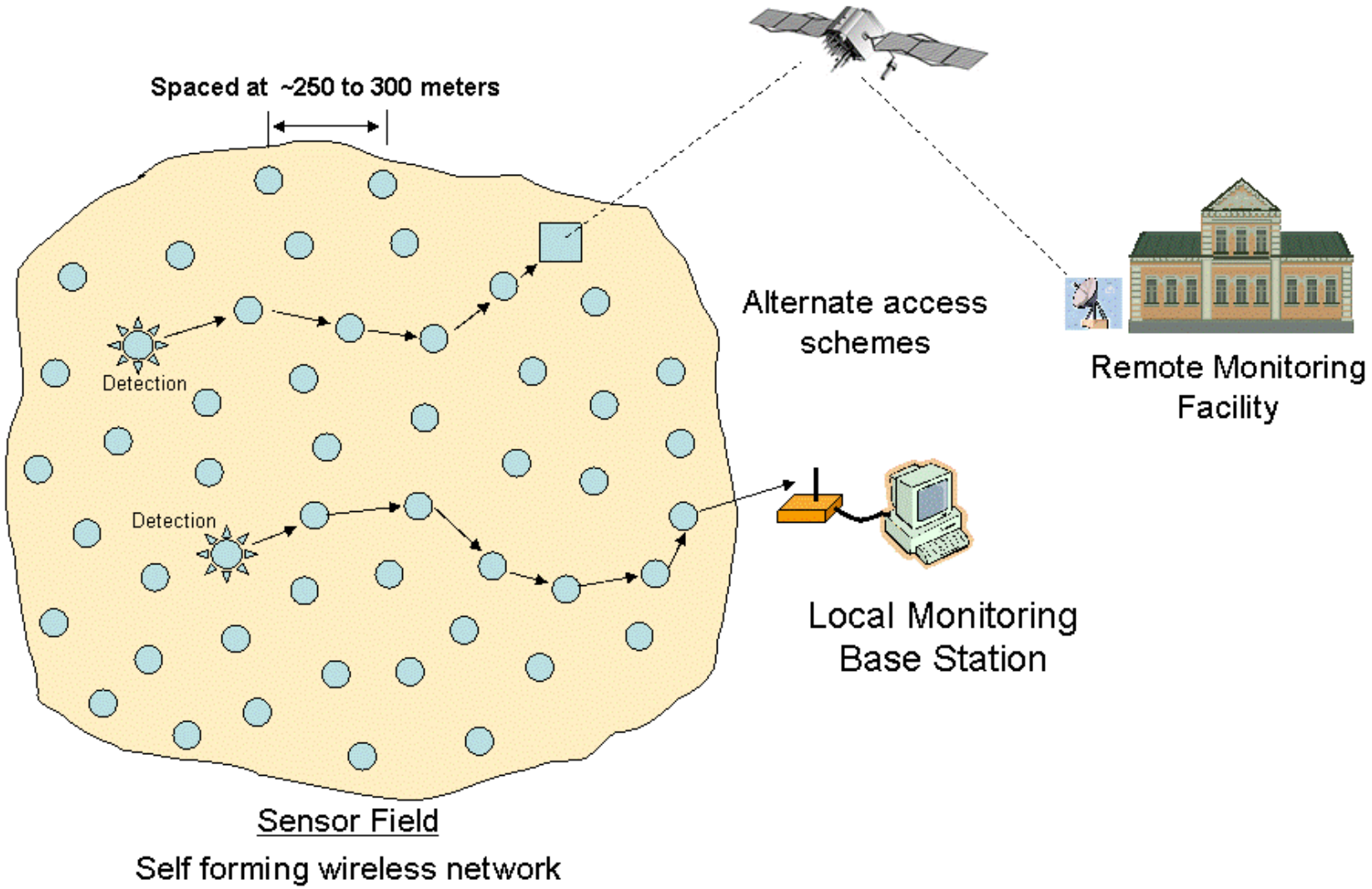
Sensor Network

- Consists of a number of small nodes
- Each node is capable of:
  - Communications
  - Sensing
  - Computation
- Typically, measures physical phenomena

Wireless Sensor Network

- Each sensor node is equipped with a radio transceiver, microprocessor, sensors.
- Such nodes can autonomously form a network, through which sensor readings can be propagated
- Data can be processed as it travels through the network, because nodes have some intelligence

Wireless Sensor Network

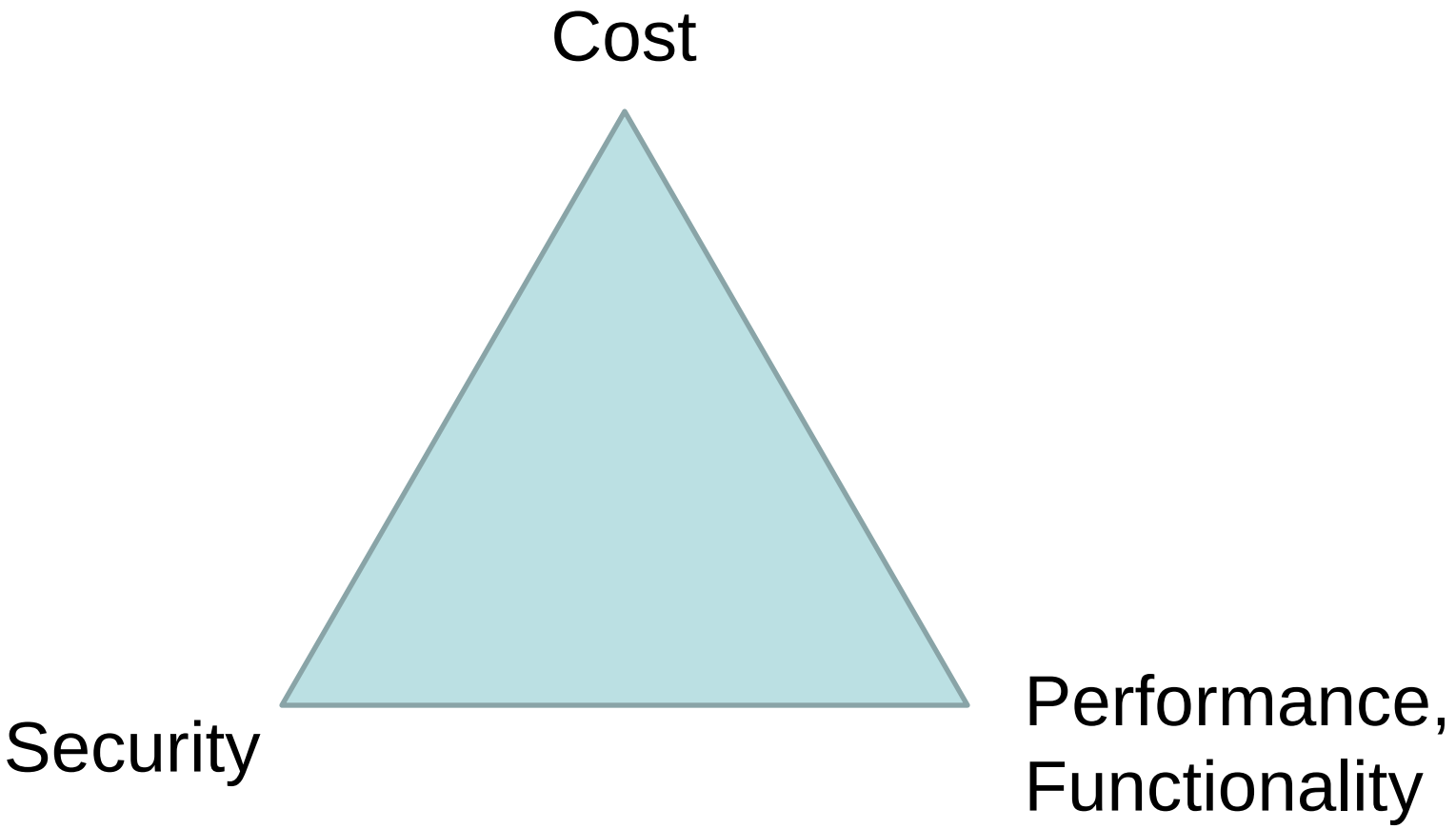


Typical WSN Applications

- Weather survey in hard-to-access geographical locations (e.g., mountains, ocean floor)
- Battlefield (e.g., surveillance and reconnaissance)

Security in MANETs and WSNs

Security Trade-offs



Types of Attacks

- Application Layer:
  - Malicious code, Repudiation
- Transport Layer:
  - Session hijacking, Flooding
- Network Layer:
  - Black Hole, Worm Hole, Link Spoofing, Location disclosure etc.
- Data Link/MAC:
  - Malicious Behavior, Selfish Behavior
- Physical:
  - Interference, Traffic Jamming, Eavesdropping

Types of Attacks (cont.)

- Passive (difficult to detect)
- Active
- External
  - External malicious nodes attempting to DoS the network
- Internal
  - A (compromised) node that's already an authorized part of the network, performing malicious actions
  - Compromised nodes can use security measures to protect their attacks

Security Challenges

- Resource scarcity
- Highly susceptible to physical attacks (e.g., node capture)
- Sensor networks closely interact with people and with their physical environments
- Communication patterns differ from traditional networks

Physical Security

- Main concern: node-capture
- How vital is this node? What functionality do adversaries have access to now? Keys? Sensor data? Etc.
- "I am behind a firewall" mentality

- Drastically different threat model

Crypto-related Challenges

Key Management

- Trust model
- Key creation
- Key distribution
- Key storage

Key Establishment: Take One

- Simplest thing ever: one shared key

Key Establishment: Take Two

- Use a single shared key to establish a set of link keys

Securing WSNs

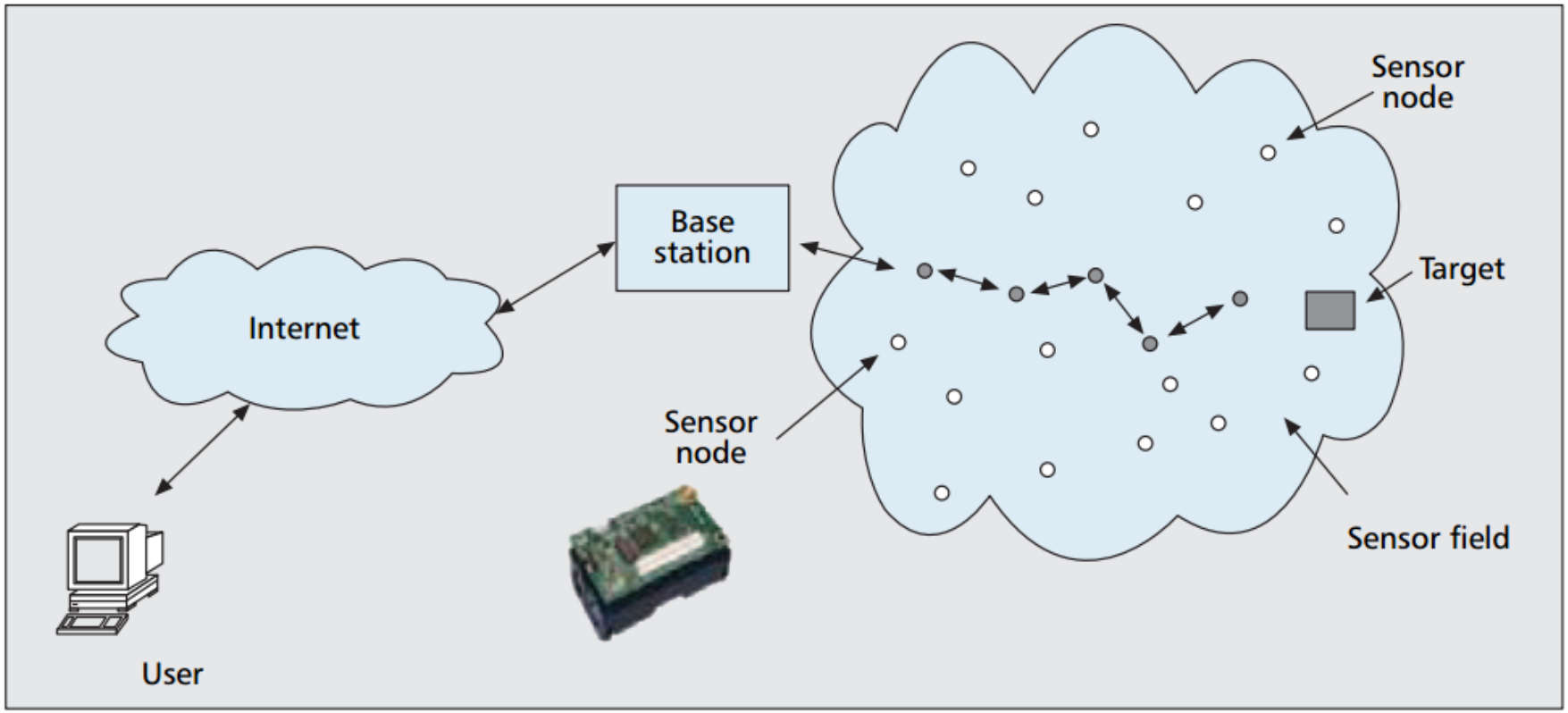
- Symmetric key crypto was the only way to address encryption, until recently.
  - Does not scale for WSNs.
- Use Identity-Based Encryption
  - Nodes can exchange information that uniquely identifies each node, and can be used to exchange keys and to encrypt data

(Oliveira, et al., 2007)

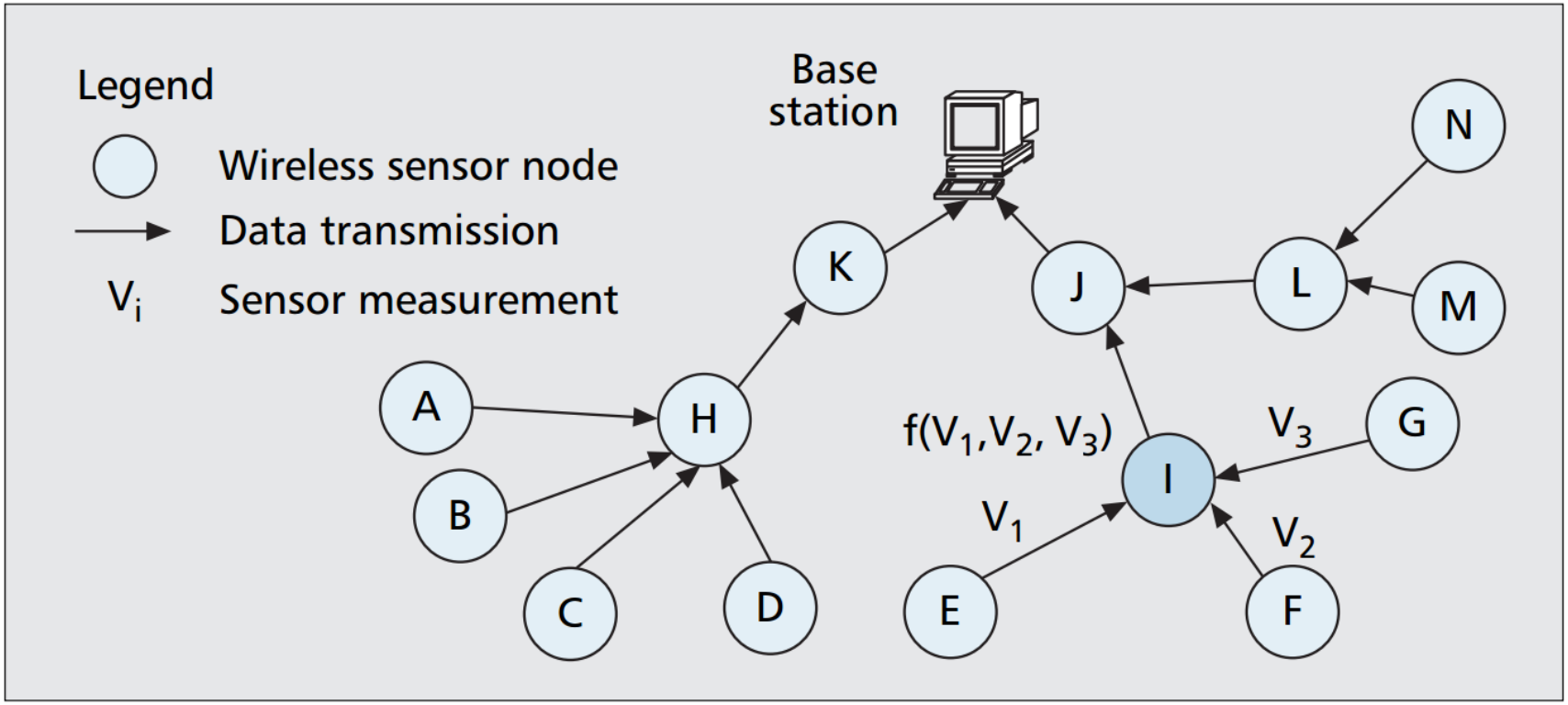
Comparing Crypto Schemes for WSNs

	Symmetric key Cryptography	Public Key Cryptography	Identity-Based Cryptography
Computational Complexity	Low	High	High
Communication Overhead	Low	High	Low
Key Distribution	Problematic	Complex	Simple
Number of Keys	O(n2)	O(n)	n
Key Directory	At Each Node	At Each node or Key Center	No
Non-Repudiation	No	Yes	Yes
Forward Encryption	No	No	Yes

Routing and Intrusion Detection-related Challenges


Sensor node
Base station
Target
Internet
Sensor node
Sensor field
User

Aggregation Trees in WSNs

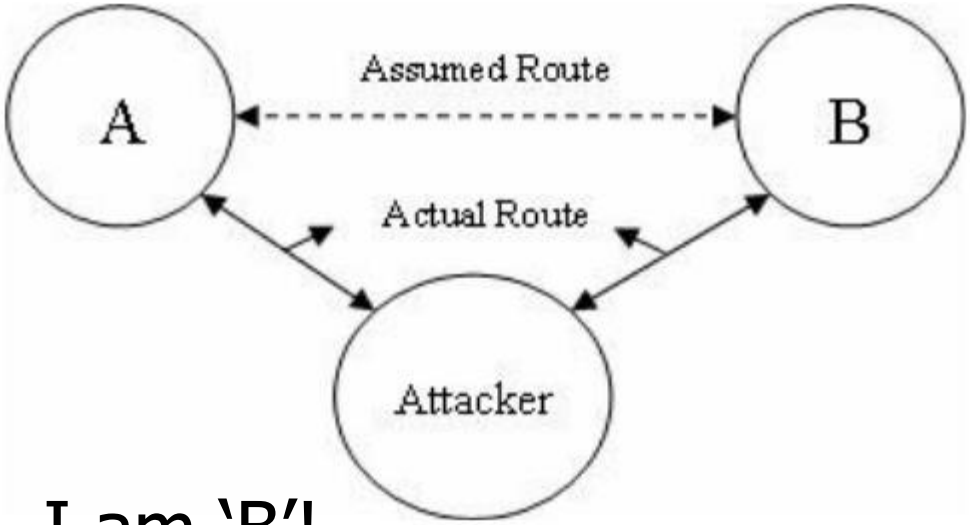


Types of Routing Protocols

- Proactive
  - Typically table-driven and distance-vector protocols
- Reactive (source-initiated on-demand)
- Hybrid

Attacks

Spoofing (Man-in-the-Middle)

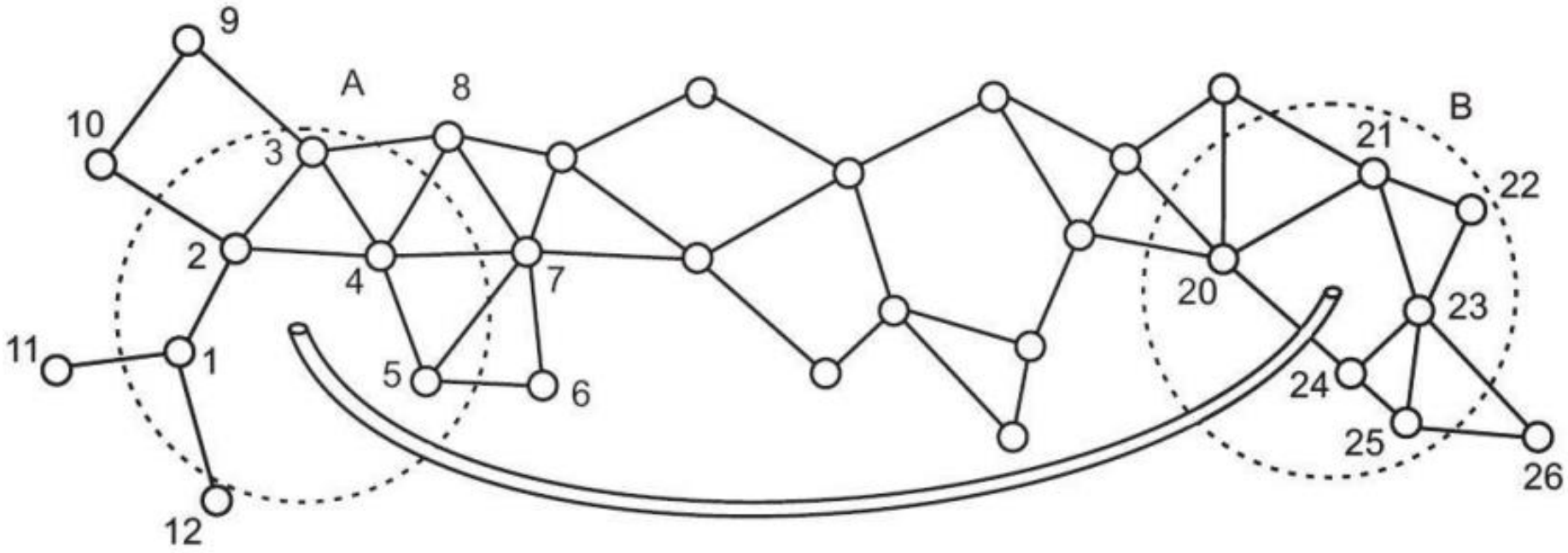


I am 'B'!

Fabrication

- Malicious node sends false (but "valid") routing messages, to change the topology
  - e.g.: neighbors B and C are no longer available

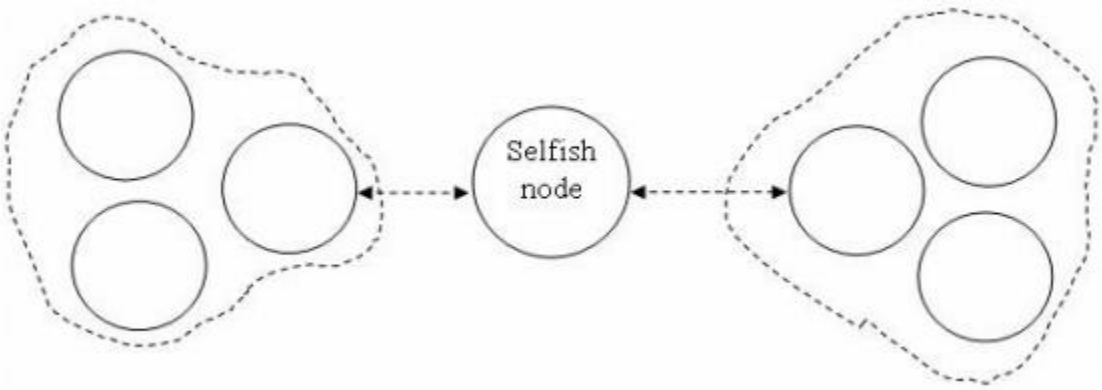
Wormhole Attack



Modification

- Tamper with the packet's data payload (attack on integrity)

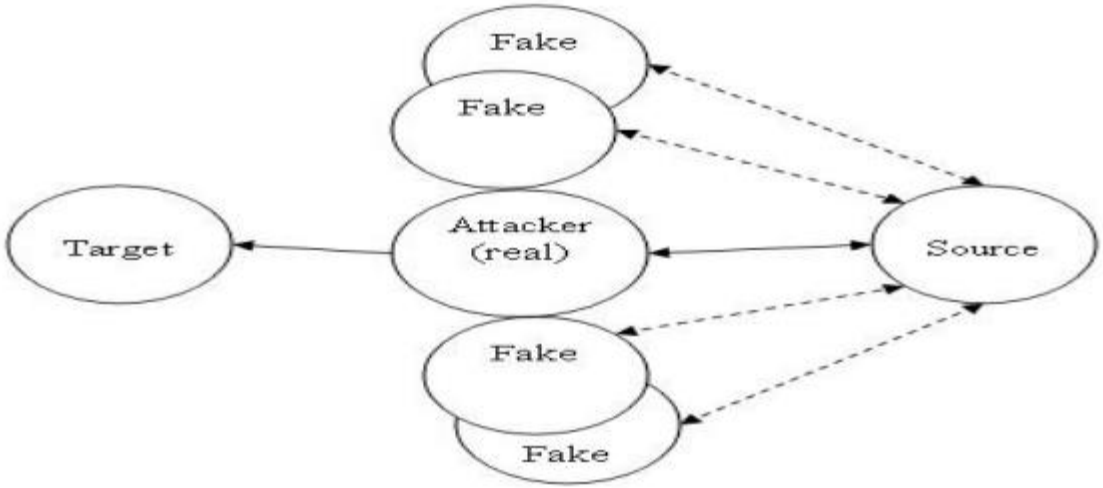
Denial of Service



- In general ad-hoc networks are supposed to withstand DoS better than fixed networks

Sinkholes

- Malicious node tries to attract all traffic to itself
  - e.g. by faking to be the best route for other nodes



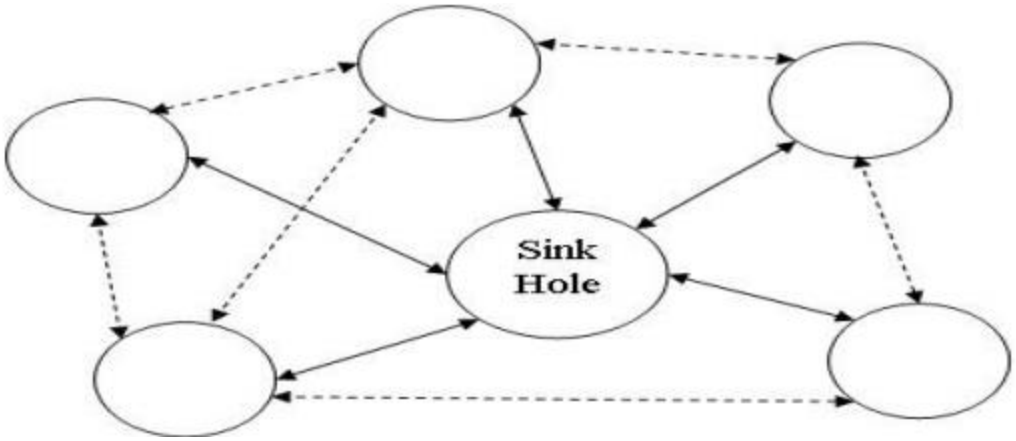
Sleep Depravation

- A.k.a. Resource Consumption Attack

- Consume battery on the target by constantly communicating with it (routing updates, relay requests, etc.)

Sybil Attack

- Malicious node takes on identity of many other nodes, again, making other nodes communicate with it.



Attacking the Sensors

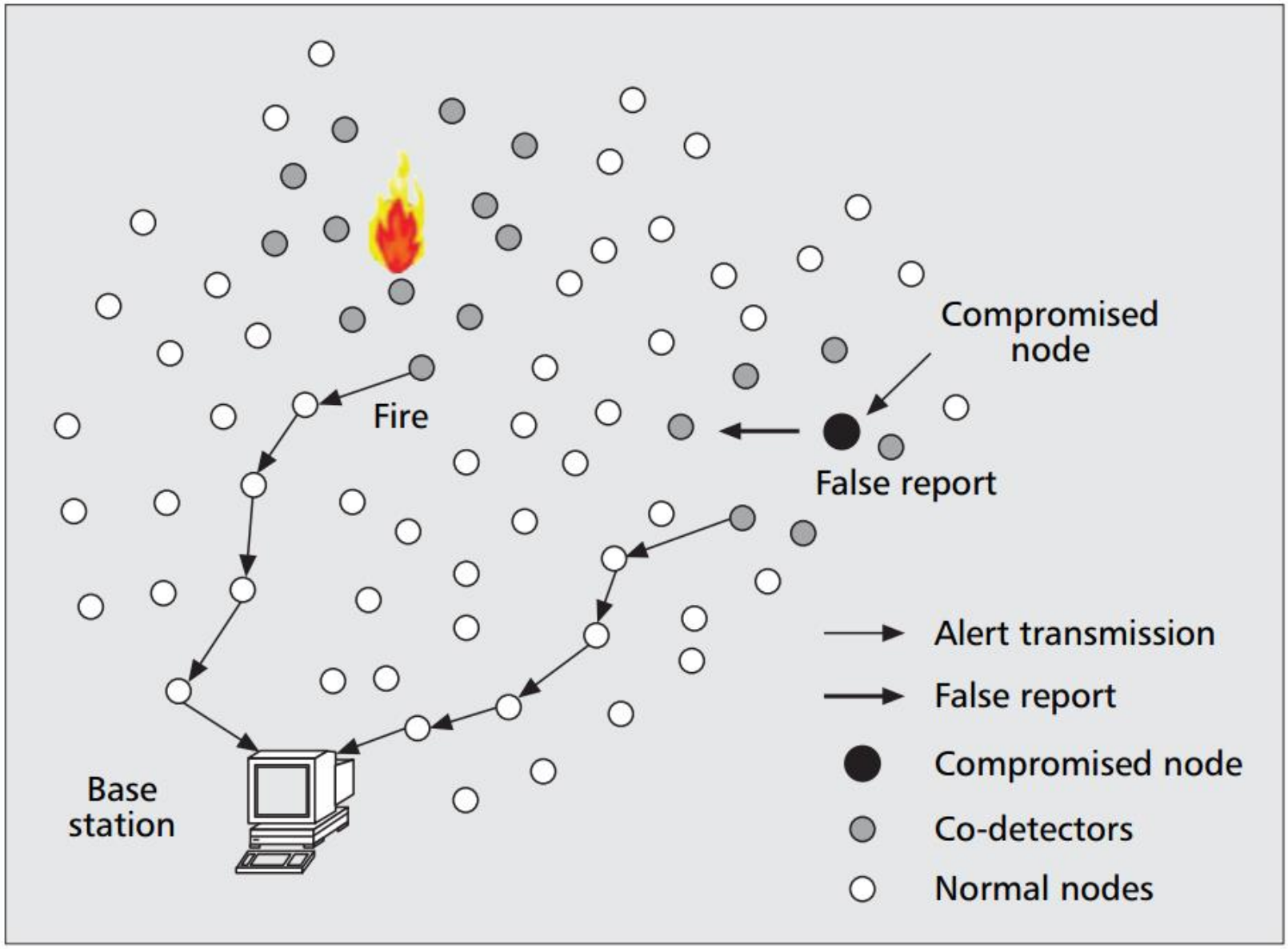
- Tampering with the surrounding environment to full the sensors

- In general, WSNs are well positioned to detect such attacks

Other Attacks

- Eavesdropping
- Black hole attack
  - Malicious node falsely advertises routes without having actual routes established
- Byzantine attack
  - confuse target nodes with non-optimal routing updates
- Flooding (the entire network vs. DoS of a single node)
- Replay attack
- Location disclosure attack

Detecting Malicious Events



References

- Ahmed, A. A., Shi, H., & Shang, Y. (2003). *A Survey on Network Protocols for Wireless Sensor Networks.* Paper presented at the Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on.
- Coelingh, E., & Solyom, S. (2012). All Aboard the Robotic Road Train. *Spectrum, IEEE, 49*(11), 34-39. doi: 10.1109/MSPEC.2012.6341202
- Oliveira, L. B., Dahab, R., Lopez, J., Daguano, F., & Loureiro, A. A. F. (2007). *Identity-Based Encryption for Sensor Networks.* Paper presented at the Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on.
- Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in Wireless Sensor Networks. *Commun. ACM, 47*(6), 53-57. doi: http://doi.acm.org/10.1145/990680.990707
- Sharifi, M., Ardakani, S. P., & Kashi, S. S. (2009). *SKEW: An Efficient Self Key Establishment Protocol for Wireless Sensor Networks.* Paper presented at the Collaborative Technologies and Systems, 2009. CTS '09. International Symposium on.
- Sun, B., Osborne, L., Xiao, Y., & Guizani, S. (2007). Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks. *Wireless Communications, IEEE, 14*(5), 56-63. doi: 10.1109/MWC.2007.4396943

Conclusion

- Don’t treat MANETs & WSNs as your average network
- Large problem space wrt security
- Always backup your PowerPoint presentations!

Q&A

Thank You!

Edward Bonver
edward@owasp.org

OWASP