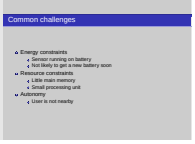
Common challenges

- Energy constraints
  - Sensor running on battery
  - Not likely to get a new battery soon
- Resource constraints
  - Little main memory
  - Small processing unit
- Autonomy
  - User is not nearby



Die ersten zwei Punkte sind auch in z.B. normalen Ad-Hoc Netzen zu finden. Die Autonomie kommt hier noch dazu.

What is misbehavior detection. . .

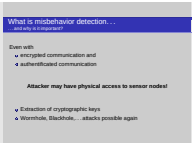
. . . and why is it important?

Even with

- encrypted communication and
- authentificated communication

Attacker may have physical access to sensor nodes!

- Extraction of cryptographic keys
- Wormhole, Blackhole,. . . attacks possible again

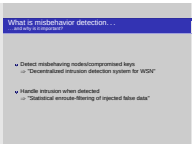


Unerwuenschtes Verhalten erkennen

What is misbehavior detection. . .

. . . and why is it important?

- Detect misbehaving nodes/compromised keys
  ⇒ "Decentralized intrusion detection system for WSN"
- Handle intrusion when detected
  ⇒ "Statistical enroute-filtering of injected false data"

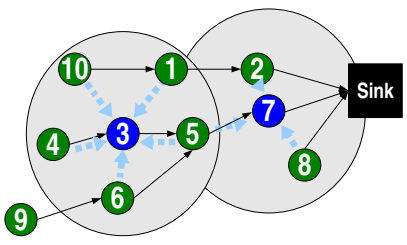


Grund für die Wahl dieser Systeme:

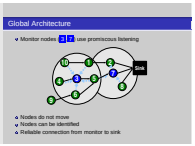
- IDS: Behandelt viele verschiedene Angriffe
- En-route: Behandelt Angriff, der nicht von IDS behandelt wurde. Und **erkennt** nicht nur, sondern reagiert auch automatisch

Global Architecture

- Monitor nodes (3, 7) use promiscous listening



- Nodes do not move
- Nodes can be identified
- Reliable connection from monitor to sink

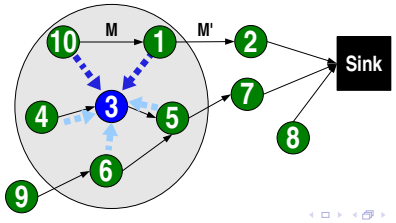


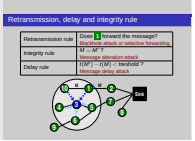
Zuverlässige Verbindung

Am zweiten Punkt, sieht man dass trotzdem noch Kryptographie gebraucht wird.

Retransmission, delay and integrity rule

Retransmission rule	Does **1** forward the message? Blackhole attack or selective forwarding
Integrity rule	$M = M'$? Message alteration attack
Delay rule	$t(M') - t(M) <$ treshold ? Message delay attack

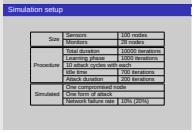




Unterschied zwischen Delay und Blackhole

Simulation setup

Size	Sensors	100 nodes
	Monitors	28 nodes
Procedure	Total duration	10000 iterations
	Learning phase	1000 iterations
	10 attack cycles with each	
	Idle time	700 iterations
	Attack duration	200 iterations
Simulated	One compromised node	
	One form of attack	
	Network failure rate	10% (20%)



- Die Parameter für die Regeln werden zu Beginn während einer Lernphase ermittelt.

Detection effectivness
Simulation results

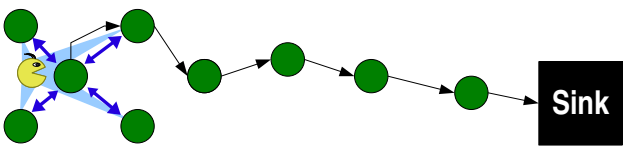
	Small Message Buffer		Large Message Buffer	
Attack	DR	FP	DR	FP
Message delay	bad	few	good	hardly any
Blackhole	good	**too many**	good	few
Selective forwarding	medium	**too many**	good	few
Wormhole	good	many	good	few
Message repetition	good	few	good	hardly any
Jamming	good	medium	good	few
Data alteration	good	**too many**	medium	few

DR=Detection Rate **FP**=False Positives

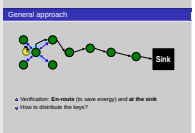
Einige Ergebnisse haben ihre Grundzüge in der Art der Simulation.

- Tabelle erklären!!!
- Detection rate = Prozentuale Erkennungsrate
- False Positives: Erkennung eines falschen Angriffs oder Netzwerkfehler als Angriff
- Message Buffer ist bezeichnend fuer den **Trade-off** von Effizienz und Resourcen
- Data alteration: 10% Netzwerkfehler sind einfach unrealistisch, CRC Checksummen
- Welche Art von Ebene 1 und 2 Protokoll verwendet wird, ist nicht spezifiziert.

General approach

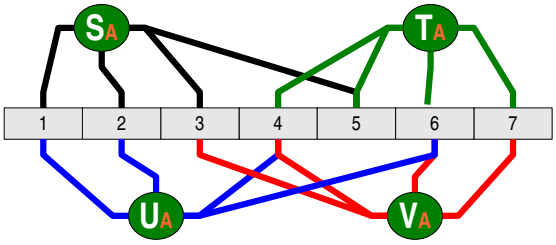


- Verification: **En-route** (to save energy) and **at the sink**
- How to distribute the keys?

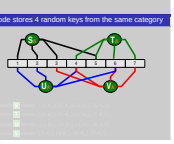


Mehrere Knoten verifizieren und unterschreiben den Bericht mit einer MAC-Signatur.
Normalerweise wuerde man jedem Knoten einen MAC-Key zuweisen. Dann koennten wir aber nicht "unterwegs" pruefen, ob die Signaturen stimmen.
Ein MAC-Key insgesamt ist auch keine Alternative...

A node stores 4 random keys from the same category

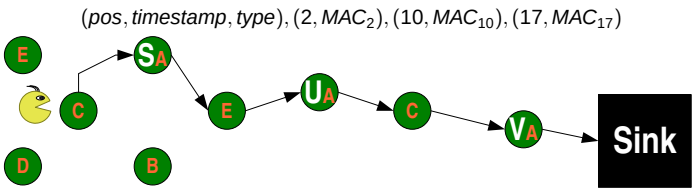


- Node S stores: $\{(1, K_1), (2, K_2), (3, K_3), (5, K_5)\}$
- Node T stores: $\{(4, K_4), (5, K_5), (6, K_6), (7, K_7)\}$
- Node U stores: $\{(1, K_1), (2, K_2), (4, K_4), (6, K_6)\}$
- Node V stores: $\{3, K_3\}, (4, K_4), (6, K_6), (7, K_7)\}$

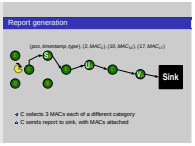


Das hier ist ein **Beispiel**.
Erklären, was die Buchstaben bedeuten

Report generation



- C selects 3 MACs each of a different category
- C sends report to sink, with MACs attached



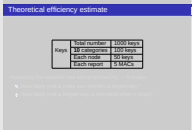
Bloom filter um den Rattenschwanz hinten dran zu verkleinern.
Die 3 MACs kann frei gewählt werden. Die Zahl stellt einen Kompromiss von Sicherheit und Benutzbarkeit des Systems dar. (Es müssen ja auch genug Kategorien in der Gegend vorhanden sein)

Theoretical efficiency estimate

Keys	Total number	1000 keys
	10 categories	100 keys
	Each node	50 keys
	Each report	5 MACs

Assuming the attacker has compromised $N_c < 5$ nodes.

- How likely that a node can identify a forged key?
- How likely that a forged key is identified after h hops?



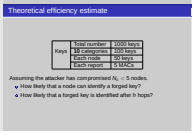
Wenn nach n Schritten ein gefälschter MAC erkannt wird, wird das Paket natürlich auch nach n Schritten gefiltert.
Die **Simulation** hat diese Ergebnisse nur bestätigt und wird deswegen nicht aufgeführt.

Theoretical efficiency estimate

Keys	Total number	1000 keys
	10 categories	100 keys
	Each node	50 keys
	Each report	5 MACs

Assuming the attacker has compromised $N_c < 5$ nodes.

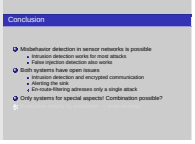
- How likely that a node can identify a forged key?
- How likely that a forged key is identified after h hops?



Wenn nach n Schritten ein gefälschter MAC erkannt wird, wird das Paket natürlich auch nach n Schritten gefiltert.
Die **Simulation** hat diese Ergebnisse nur bestätigt und wird deswegen nicht aufgeführt.

Conclusion

1. Misbehavior detection in sensor networks is possible
   - Intrusion detection works for most attacks
   - False injection detection also works
2. Both systems have open issues
   - Intrusion detection and encrypted communication
   - Alerting the sink
   - En-route-filtering adresses only a single attack
3. Only systems for special aspects! Combination possible?
4. Evaluation mostly by simulation → level-of-detail



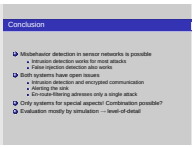
Ein Angriff, nur Erkennung, nur Reagieren (Reputation)

Conclusion

1. Misbehavior detection in sensor networks is possible
   - Intrusion detection works for most attacks
   - False injection detection also works
2. Both systems have open issues
   - Intrusion detection and encrypted communication
   - Alerting the sink
   - En-route-filtering adresses only a single attack
3. Only systems for special aspects! Combination possible?
4. Evaluation mostly by simulation → level-of-detail

Detecting Misbehavior in Wireless Sensor Networks 20.1.2005 25 / 1

2006-01-23
Detecting Misbehavior in Wireless Sensor Networks
Conclusion
Conclusion



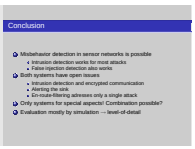
Ein Angriff, nur Erkennung, nur Reagieren (Reputation)

Conclusion

1. Misbehavior detection in sensor networks is possible
   - Intrusion detection works for most attacks
   - False injection detection also works
2. Both systems have open issues
   - Intrusion detection and encrypted communication
   - Alerting the sink
   - En-route-filtering adresses only a single attack
3. Only systems for special aspects! Combination possible?
4. Evaluation mostly by simulation → level-of-detail

Detecting Misbehavior in Wireless Sensor Networks 20.1.2005 25 / 1

2006-01-23
Detecting Misbehavior in Wireless Sensor Networks
Conclusion
Conclusion



Ein Angriff, nur Erkennung, nur Reagieren (Reputation)10% Fehlerrate bei der Integrität ist lächerlich. Schwer zu begreifen, was eigentlich genau simuliert wird.

Conclusion

1. Misbehavior detection in sensor networks is possible
   - Intrusion detection works for most attacks
   - False injection detection also works
2. Both systems have open issues
   - Intrusion detection and encrypted communication
   - Alerting the sink
   - En-route-filtering adresses only a single attack
3. Only systems for special aspects! Combination possible?
4. Evaluation mostly by simulation → level-of-detail

Detecting Misbehavior in Wireless Sensor Networks 20.1.2005 25 / 1