Handout: Detecting Misbehavior in Wireless Sensor Networks

Nils Knappmeier

Datum: 20.1.2006

1 Intrusion detection system

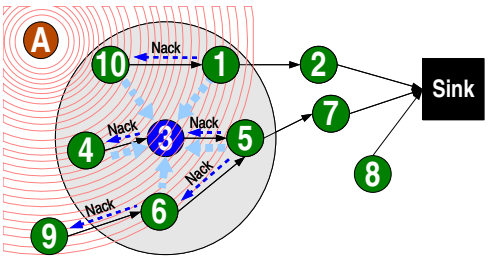
1.1 Ruleset

Role	Attack	Failure
Router	Message delay	
	Blackhole	Message loss
	Selective forwarding	
	Wormhole	
	Message repetition	
	Jamming	Message collision
	Data alteration	Data alteration

Recognized attacks and similar network failures

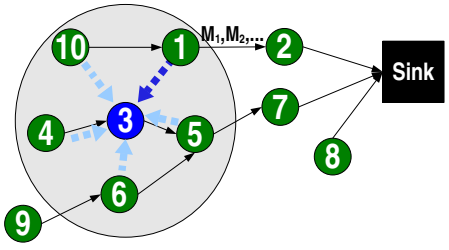
Jamming rule

Jamming rule	Number of message collisions $>$ treshold Jamming attack



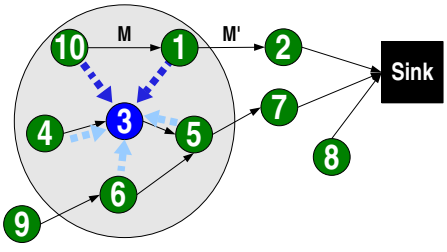
Interval rule and message repetition rule

Interval rule	$min_t < t(M_2) - t(M_1) < max_t$ Exhaustion attack or negliciency attack
Repetition rule	$M_1 = M_2 = \ldots = M_k$ for $k < treshold$ Repetition attack



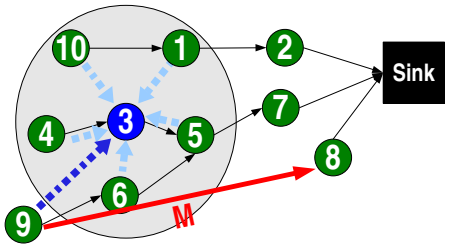
Retransmission, delay and integrity rule

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



Radio transmission range rule

Radio transmission range	"I should not be able to hear 7 !" Wormhole attack

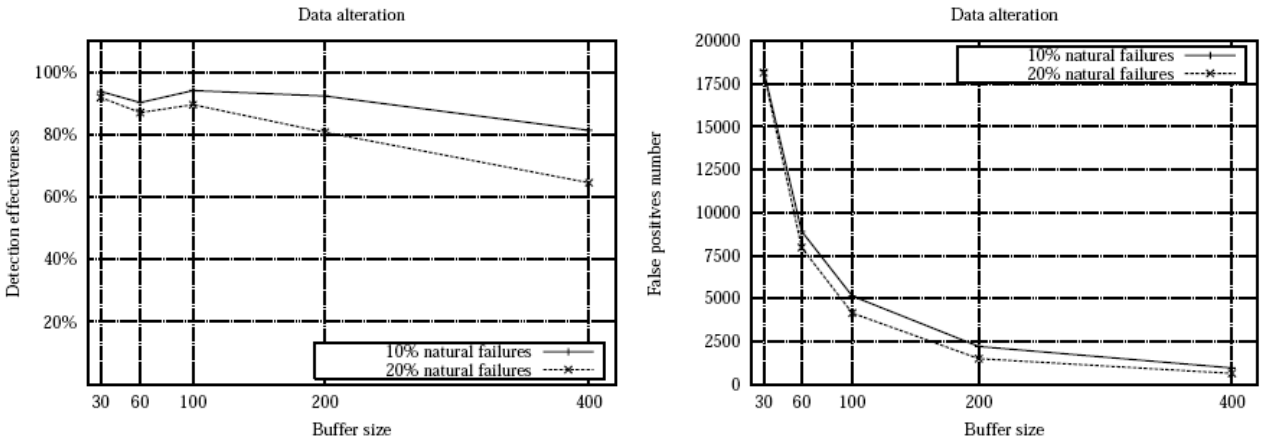


1.2 Evaluation

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%)

Simulation results (example)

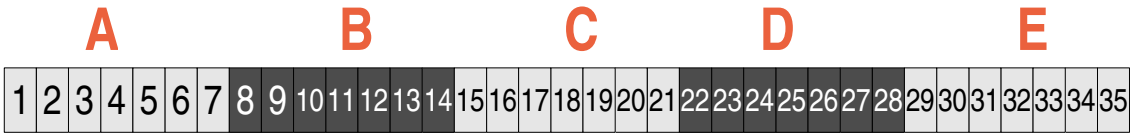


Detection rate and false positives for the data alteration attack

2 En-route-filtering of injected false data

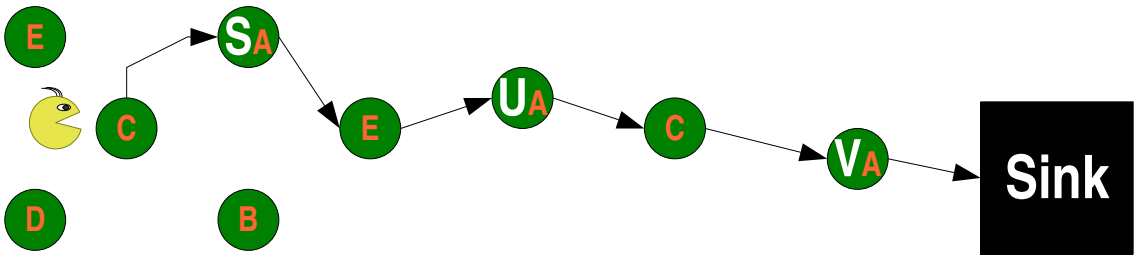
2.1 Key distribution

Keys, categories, index numbers



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: $\{3, K_3), (4, K_4), (6, K_6), (7, K_7)\}$



2.2 Report generation and filtering

Report generation

1. Stimulus detected
2. $report = (pos, time, type)$ verified
3. Neighors return $(i, MAC(report, K_i))$
4. 3 MACs from distinct categories selected

Finally: $(pos, timestamp, type), (2, MAC_2), (10, MAC_{10}), (17, MAC_{17})$sent to sink

Statistical en-route filtering

- 2 MACs from the same category? Invalid MAC found? $\Rightarrow$ Drop
- MACs not verifiable or correct? $\Rightarrow$ Forward

Filtering at the sink

Verification **all** MACs attached to the report

2.3 Evaluation

Theoretical efficiency estimate

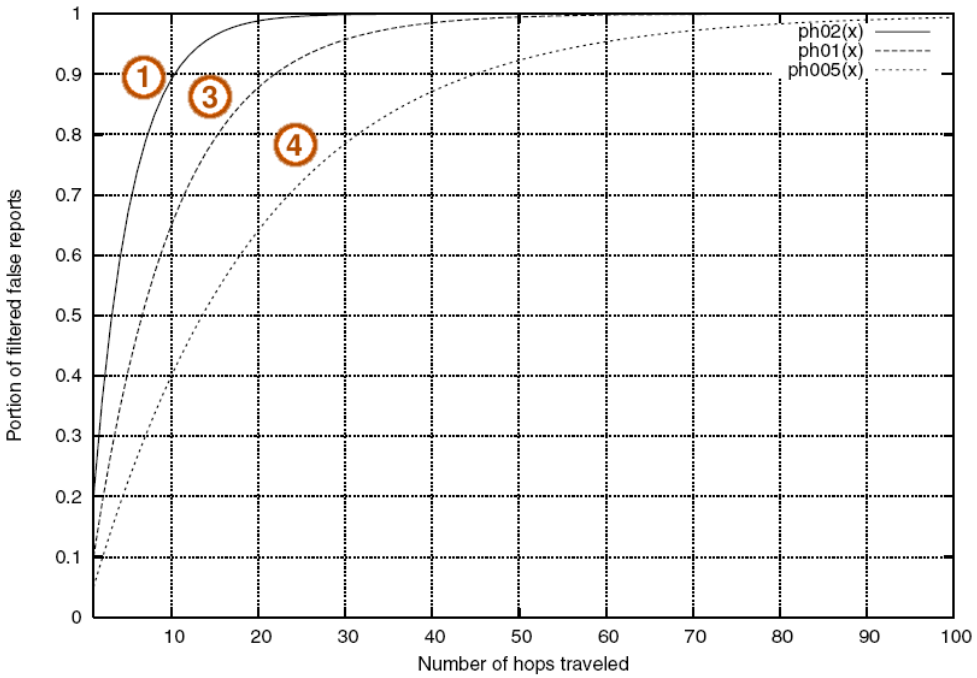
- Total number of keys: $N = 1000$
- Number of categories: $n = 10$
- Number of key per category: $m = 100$
- Number of keys per node: $k = 50$
- Number of MACs per report: $T = 5$
- Number of compromised categories $N_c < 5$
- How likely that a node can identify a forged key?

$$p_1 \quad = \quad \frac{T - N_c}{n} \cdot \frac{k}{m} \quad = \quad \frac{k(T - N_c)}{N}$$

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

$$p_h \quad = \quad 1 - (1 - p_1)^h$$

Packets dropped after n hops...



3 Quellen

References

[1] Decentralized Intrusion Detection in Wireless Sensor Networks, Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz, Hao Chi Wong, October 2005, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks Q2SWinet '05

[2] Statistical En-route Filtering of Injected False Data in Sensor Networks, Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang, UCLA Computer Science Departement, Los Angeles