NANYANG TECHNOLOGICAL UNIVERSITY

On-off attack in WSN and mitigations

HU HAO

Mar 10, 2015

NANYANG TECHNOLOGICAL UNIVERSITY

References

- 1. Alzaid, H., Foo, E., Nieto, J. G. and Ahmed, E. (2012), Mitigating On-Off attacks in reputation-based secure data aggregation for wireless sensor networks. Security Comm. Networks, 5: 125-144.
- 2. Sun Y L, Han Z, Yu W, et al. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks[C]//INFOCOM. 2006, 2006: 1-13.
- 3. Alzaid H, Alfaraj M, Ries S, et al. Reputation-based trust systems for wireless sensor networks: A comprehensive review[M]//Trust Management VII. Springer Berlin Heidelberg, 2013: 66-82.

NANYANG TECHNOLOGICAL UNIVERSITY

The damage effect of On-Off attack (OO)

Schemes	WSNs Attacks				Reputation Attacks			
	SF	SY	SD	RE	BM	BS	OO	NC
Michiardi & Molva [25]	•		••	••		••	•	
Buchegger & Boudec [13]	•	••	•	••	••		••	••
Ganeriwal & Srivastava [34]	•		••	••		••	••	•
Srinivasan et al. [14]	•	••	•	••			•	••
Boukerche et al. [26]	•		•				•	
Alzaid et al. [11]	•		•				••	
Yao et al. [17]	•	••	••		••	••	••	••
Shaikh et al. [10]	•		•		•	•	••	
Özdemir [33]	•		••	••	••	••	••	
Bouckerche & Ren [12]	•		•	••	••	••	••	
Chen et al. [31]	•	••	••	••			••	••
Xiao et al. [16]	••	••	••	••	••	••	••	••
Srinivasan et al. [15]	••		••	••	••	••	••	

	Robust
•	Partial damage
••	Maximum damage

SF: Selective forwarding

SY: Sybil attack

SD: Spoofed data

RE: Replay

BM: Badmouth

BS: Ballot stuffing

NC: New comer

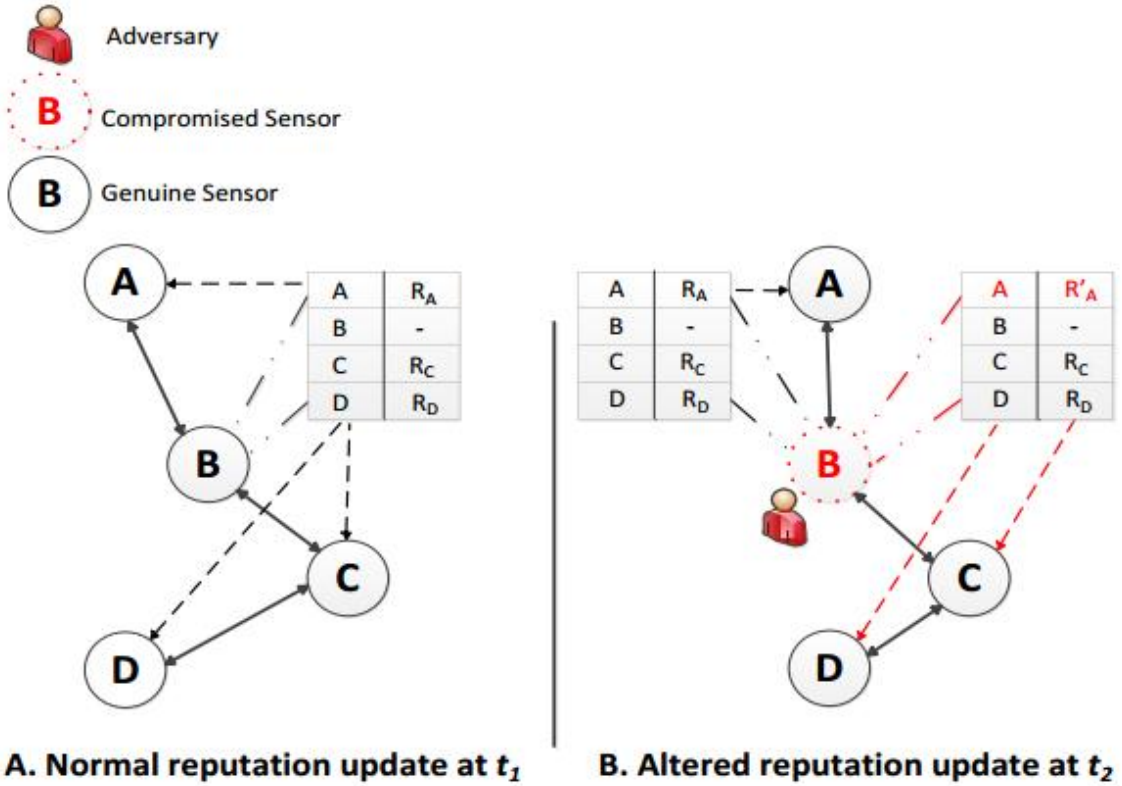
All reputation-based trust systems are vulnerable to this attack

On-off attack model

- The adversary, in this attack, aims to disturb the system's overall performance with the hope that it will not be detected or excluded from the network

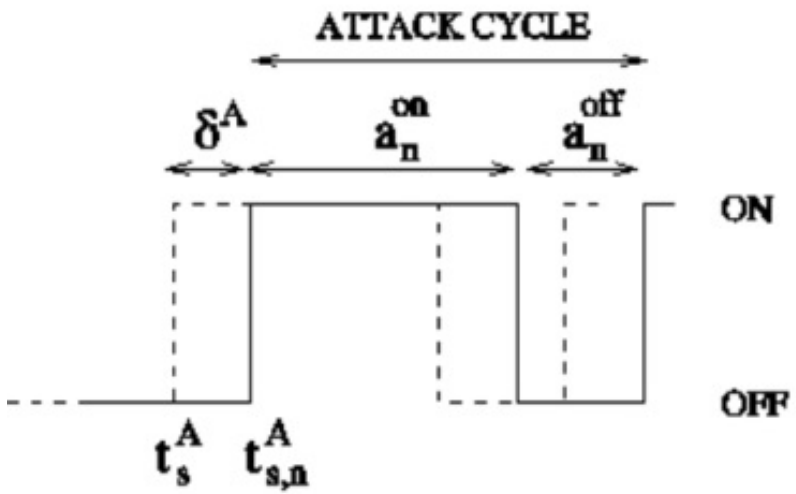
Figure shows a subset of genuine nodes where a node B shares its reputation table with neighboring nodes.

B is compromised after t_2 and behaves maliciously intermittently when it deals with nodes C and D by claiming that the reputation value for node A is R'_A instead of R_A



NANYANG TECHNOLOGICAL UNIVERSITY

On-off attack model (2)



$\delta^A \sim \Delta^A$: jitter for attack A

$t_s^A \sim T_s^A$: start time for attack A

$T_{s,n}^A = T_s^A + \Delta^A$

$t_{s,n}^A \sim T_{s,n}^A$: start time for attack A on node n

p : prob. that some node n is attacked or launches an attack

$a_n^{on} \sim A_n^{on}, a_n^{off} \sim A_n^{off}$

A_n^{on} : length of on-period

A_n^{off} : length of off-period

NANYANG TECHNOLOGICAL UNIVERSITY

Mitigation technique

- Add a fixed forgetting factor
- Main idea is to let performing k good actions at time t_1 is equivalent to performing good $k\beta^{t_2-t_1}$ good actions at t_2, where $0<\beta\leq 1$

Successful transaction times → $\mathrm{r}_{t_2} = \mathrm{r}_{t1}\hat{\beta} + \mathrm{r}_{t_2-t_1}$

Unsuccessful transaction times → $s_{t_2} = s_{t1}\hat{\beta} + s_{t_2-t_1}$

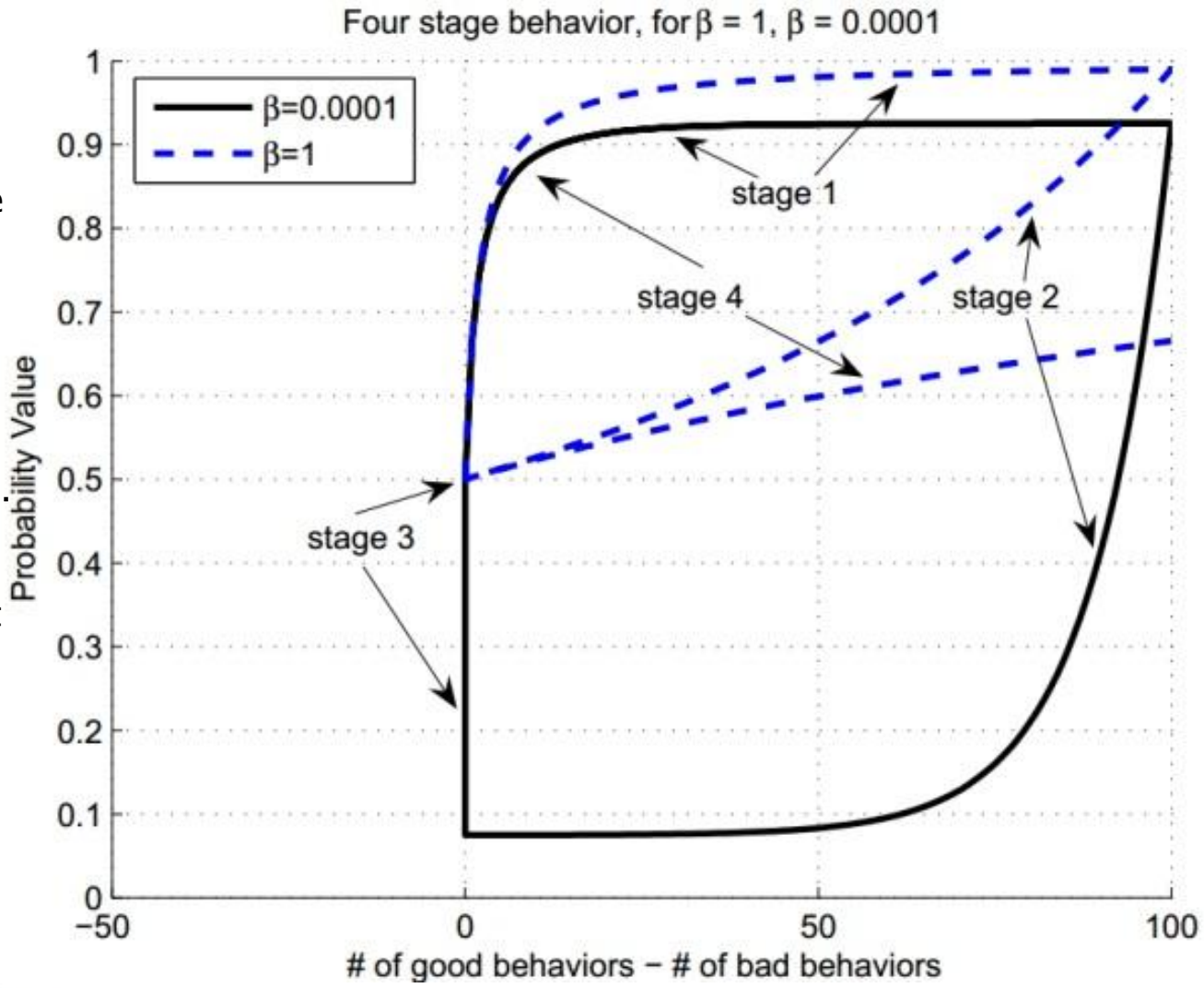
1. Sun Y L, Han Z, Yu W, et al. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks[C]//INFOCOM. 2006, 2006: 1-13.

NANYANG TECHNOLOGICAL UNIVERSITY

Mitigation technique

When the system does not forget, i.e. β = 1, this attacker has positive trust value in stage (2). That is, this attacker can have good trust values even after he has performed many bad actions. When using a large forgetting factor, the trust value may not represent the latest status of the entity. As a consequence, the malicious node could cause a large amount of damage in a stage that is similar to stage (2).

2. When using a small forgetting factor, the attacker's trust value drops rapidly after it starts behaving badly in stage (2). However, it can regain trust by simply waiting in stage (3) while the system will forget his bad behaviors quickly.



NANYANG TECHNOLOGICAL UNIVERSITY

Mitigation technique

- To defend against the on-off attack, we propose a scheme that is inspired by a social phenomenon – while it takes long-time interaction and consistent good behaviors to build up a good reputation, only a few bad actions can ruin it.

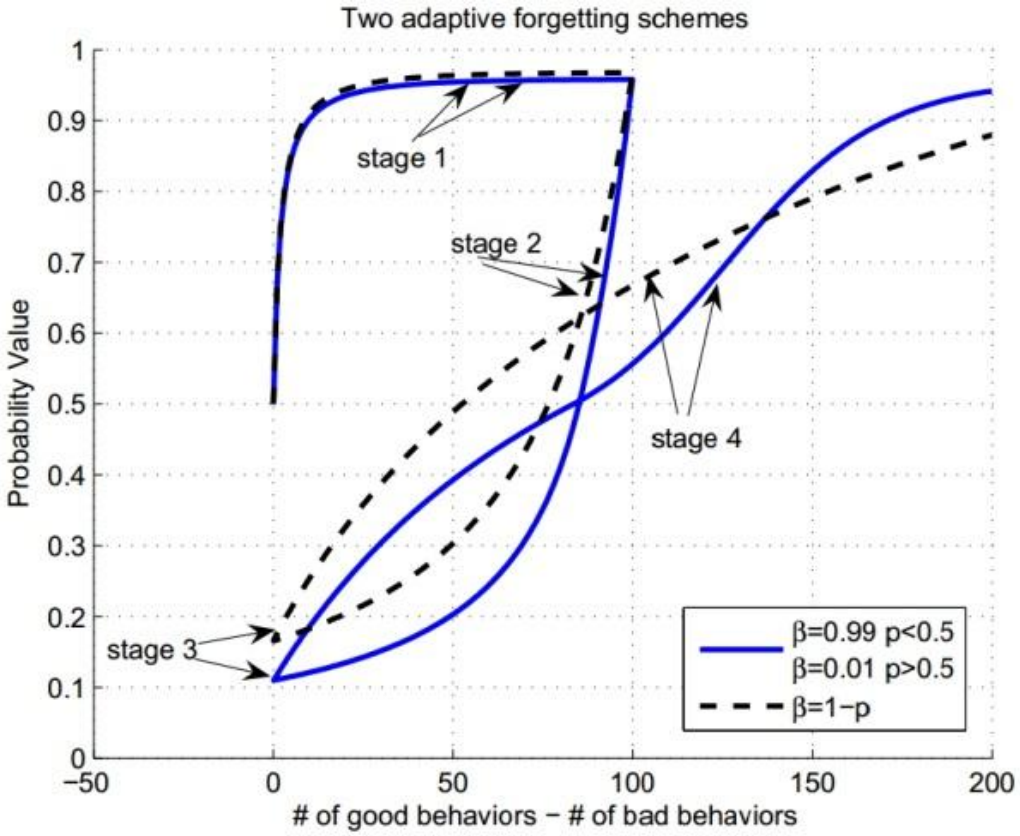
- This implies that human remember bad behaviors for a longer time than they do for good behaviors

NANYANG TECHNOLOGICAL UNIVERSITY

Mitigation technique

$$\beta = 1 - p, \text{ where } p = P\{subject : agent, action\}$$

$$\text{or, } \beta = \beta_1 \text{ for } p \geq 0.5; \text{ and } \beta = \beta_2 \text{ for } p < 0.5,$$



NANYANG TECHNOLOGICAL UNIVERSITY

- Thank you!