Mitigation of the Spectrum Sensing Data Falsifying Attack in Cognitive Radio Networks

Rajorshi Biswas, Jie Wu, and Xiaojiang Du

Dept. of Computer and Information Sciences

Temple University

Road Map

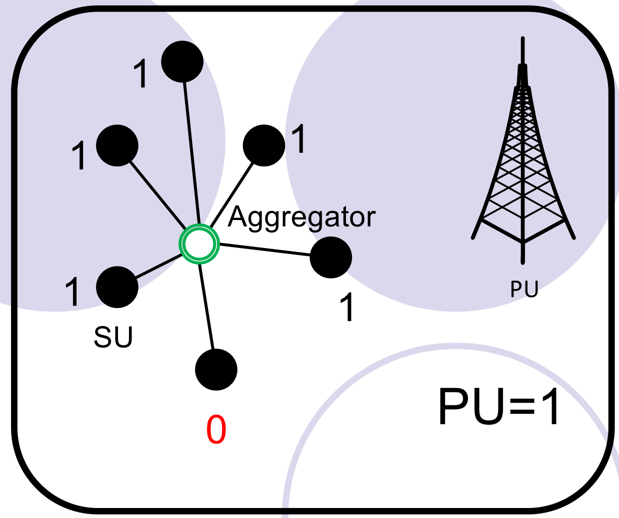
1. Cooperative spectrum sensing
2. Related work
3. Majority voting and existing models
4. Weighted majority voting with confidence
5. Simulation results
6. Extension: two-level majority voting
7. Conclusion

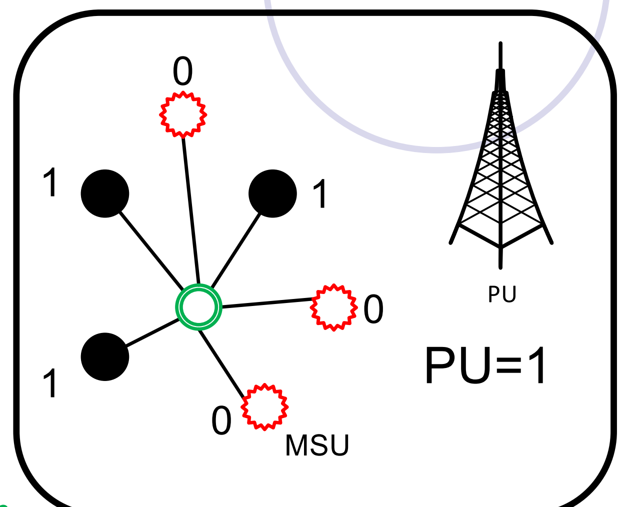
1. Cooperative Spectrum Sensing

- Primary user (PU)
  - Licensed user, high priority
- Secondary user (SU)
  - Send sensing information to aggregator
- Malicious secondary user (MSU)
  - Send opposite sensing information to aggregator
- Aggregator
  - Does majority voting
  - Results are sent back to SUs and MSUs

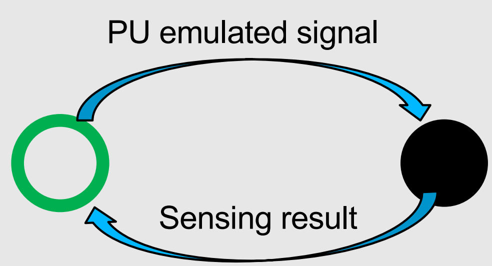
SU's wrong sensing and MSU's result can change aggregator's decision

Solution: reduce weight of MSUs through reputation





2. Previous Work

MSU detection systems	**Limitations**
Linear reputation-based system. SUs send raw sensing information to Aggregator. If a SU agrees with aggregator, reputation increases by "1" or decreases by "1". R. Chen, J. -. Park and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE INFOCOM 2008.	• Computation overhead is high for processing raw sensing information. • Linear reputation update mechanisms are not efficient enough.
Active transmission-based system.  T. Bansal, B. Chen, and P. Sinha, "Fastprobe: Malicious user detection in cognitive radio networks through active transmissions," in IEEE INFOCOM 2014.	• PU emulated signals can be detected. • MSU will respond correctly to emulated signal.

3. Majority Voting and Existing Models

	SU1	SU2	SU3	SU4
Reputation	r1	r2	r3	r4
Sensing result	s1	s2	s3	s4

$$\hat{r}_i = \frac{r_i}{\sum r_i}$$

$\hat{r}_i$ = normalized reputation

Initial reputation=1

If $\sum s_i \hat{r}_i$ > 0.5
    Aggregator's decision=1
Else
    Aggregator's decision=0

Aggregator makes decision $\longrightarrow$ Update reputation of SUs and MSUs using Reputation Update Function (RUF)

Majority Voting and Existing Models

<u>Linear RUF:</u>

$r_{new} = (\mu)r_{old} + (1-\mu)x$

μ = priority of previous reputation

If SU's result = aggregator's result

$x = 1$

Else

$x = -1$ (or 0, no decrease)

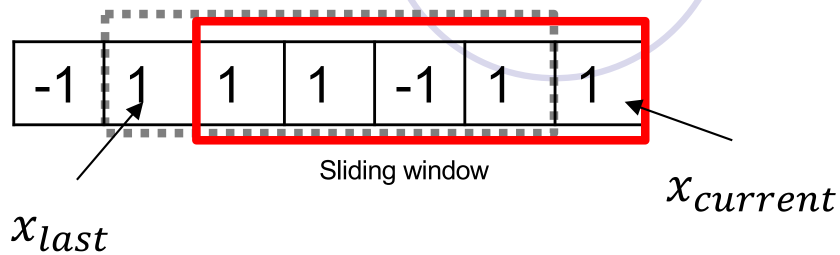
<u>Multiplicative RUF*:</u>

$r_{new} = r_{old}\exp(\eta x)$

η = learning rate: [0, 1]

<u>Multiplicative RUF with sliding window:</u>

$r_{new} = r_{old}\exp(\eta x_{current} - \eta x_{last})$



*S. Arora, E. Hazan, and S. Kale. "The multiplicative weights update method: a meta-algorithm and applications." Theory of Computing 8.1 (2012)

4. Weighted Majority Voting with Confidence

Adaptive Multiplicative RUF

- ρ_t = Normalized confidence
- $r_{new} = r_{old} \times \exp(x\,\eta\,\rho_t)$

Minority: 30

confidence

Majority: 70

$$\rho_t = \frac{|70-30|}{70+30} = 0.4$$

Ground truth

Time	0	100	200	300	400
PU	1	0	0	1	1

Sensing result

SU1	1	1	0	1	1
SU2	1	0	0	1	1
SU3	1	1	0	1	0
MSU1	1	1	1	0	0
MSU2	0	0	0	0	0

Majority voting

A	1	1	0	1	0

False positive

False negative

$\eta = 0.01$

reputation

SU1	1	2.71	7.38	20.08	54.59
SU2	1	2.71	1	2.71	7.38
SU3	1	2.71	7.38	20.08	54.55
MSU1	1	2.71	7.38	2.71	1
MSU2	1	0.36	0.13	0.36	0.13

High variance

A	1	1	0	1	0

Without confidence

ρ	0.6	0.2	0.6	0.2	0.2

reputation

SU1	1	1.82	2.22	4.05	4.95
SU2	1	1.82	1.49	2.71	3.32
SU3	1	1.82	2.22	4.05	4.95
MSU1	1	1.82	2.22	1.22	1
MSU2	1	0.54	0.44	0.81	0.67

Low variance

A	1	1	0	1	1

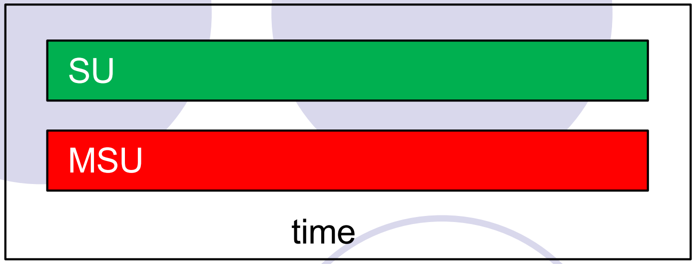
With confidence

5. Simulation

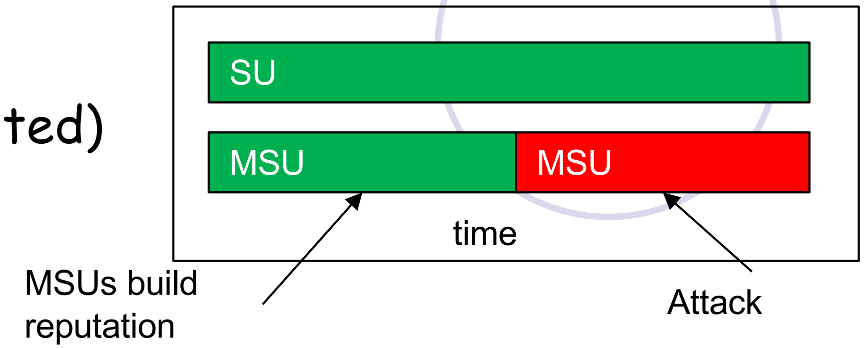
Settings and datasets

- Number of SUs: 10-50
- SU error rate: 0-0.3 (randomly selected)
- Number of MSUs: 7-50
- MSU error rate: 0.7-1 (randomly selected)
- Initial reputation: 1
- Sensing records of 100,000 timeslots.

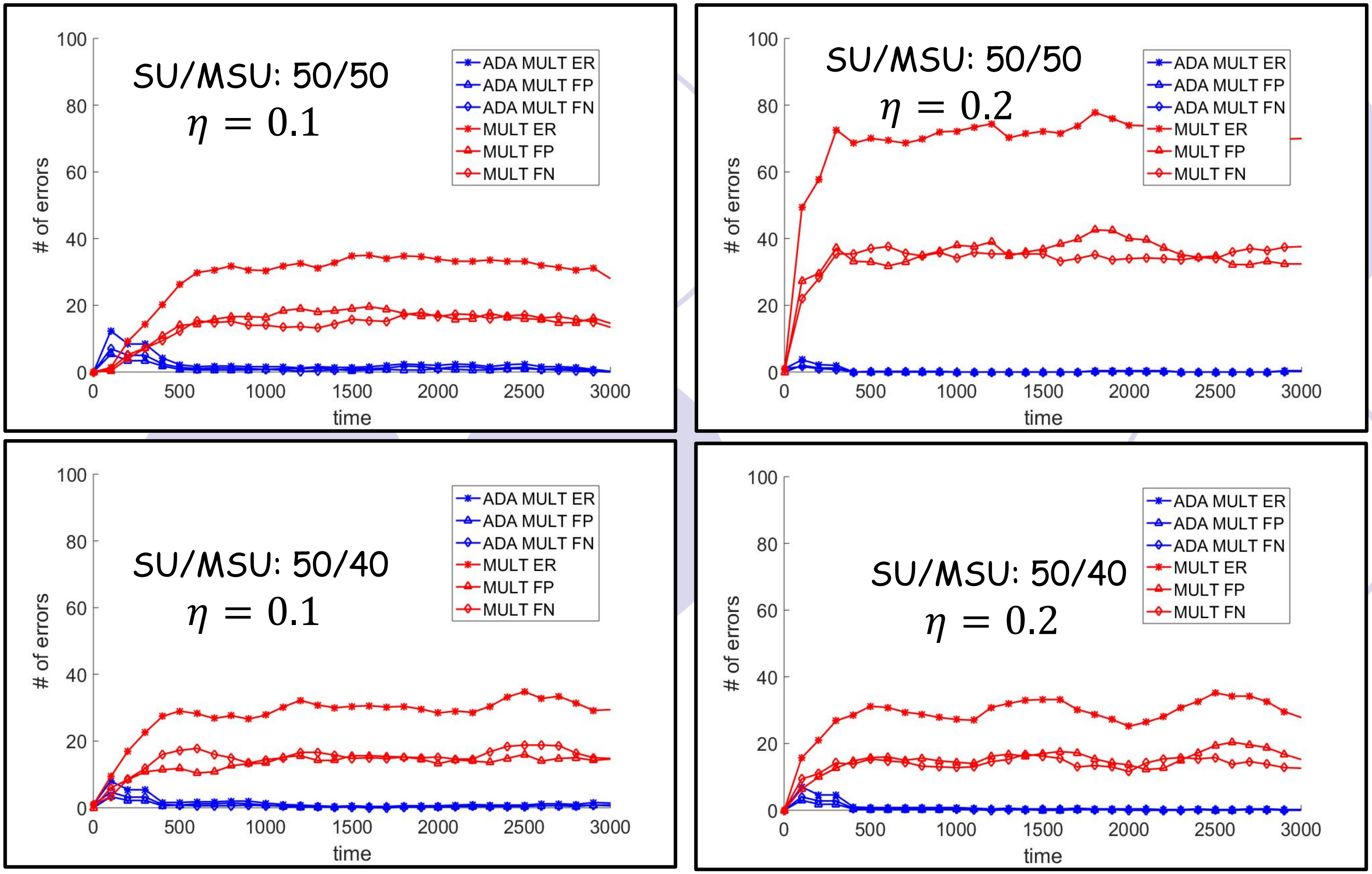
Dataset type 1



Dataset type 2



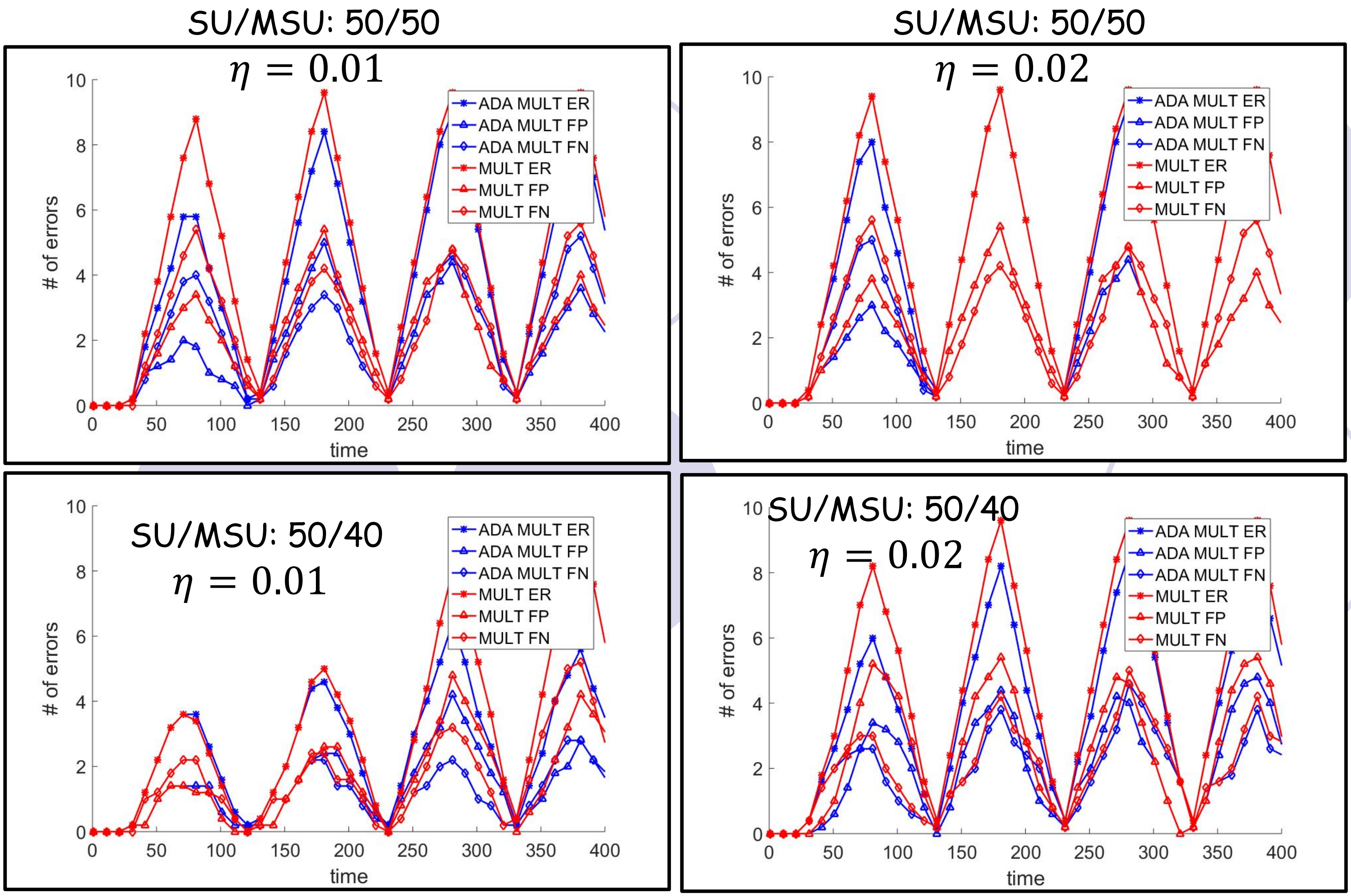
Multiplicative vs. Adaptive Multiplicative RUF



Dataset type 1 Used for simulation.

False positive (FP), False negative (FN), Error (ER), Adaptive multiplicative (ADA MULT), Multiplicative (MULT)

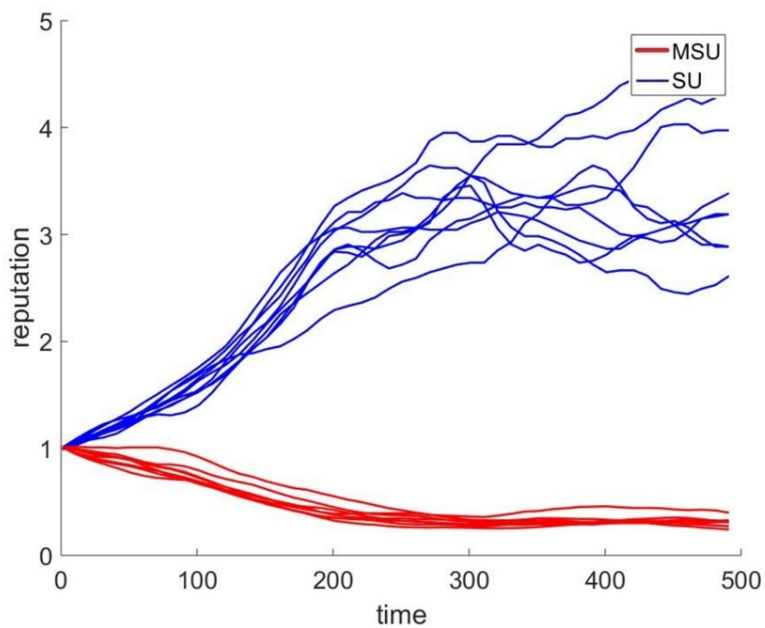
Multiplicative vs. Adaptive Multiplicative RUF



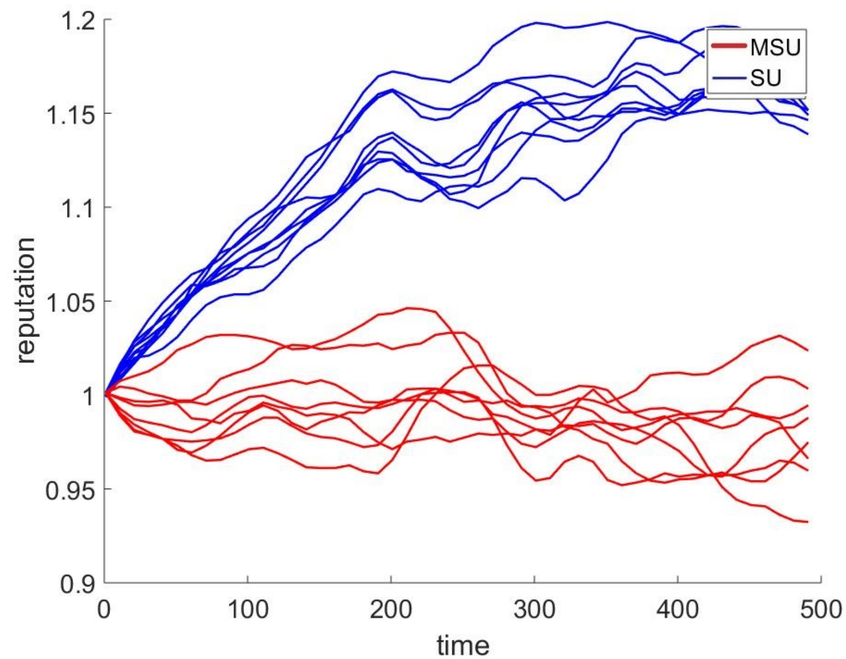
Dataset type 2 Used for simulation.

False positive (FP), False negative (FN), Error (ER), Adaptive multiplicative (ADA MULT), Multiplicative (MULT)

Multiplicative vs. Adaptive Multiplicative RUF



Multiplicative

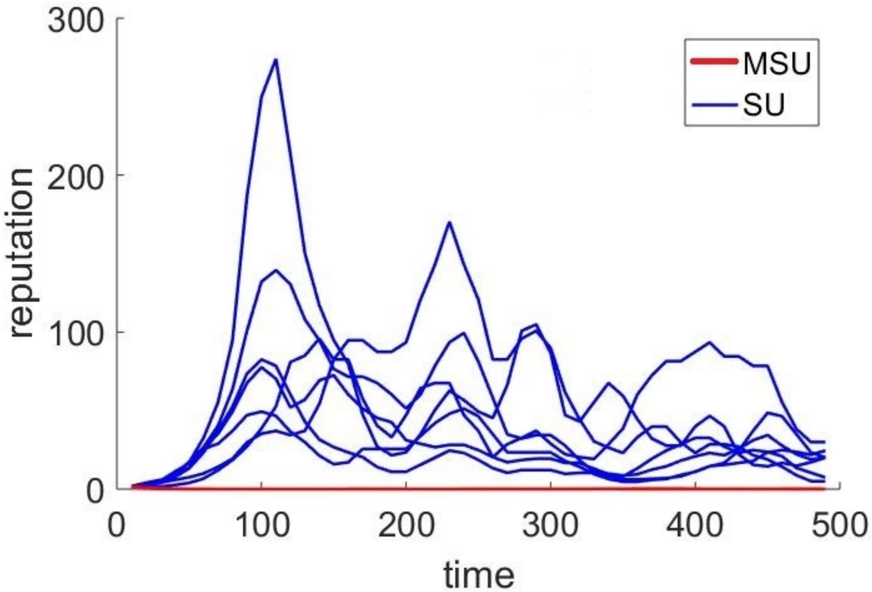


Adaptive multiplicative

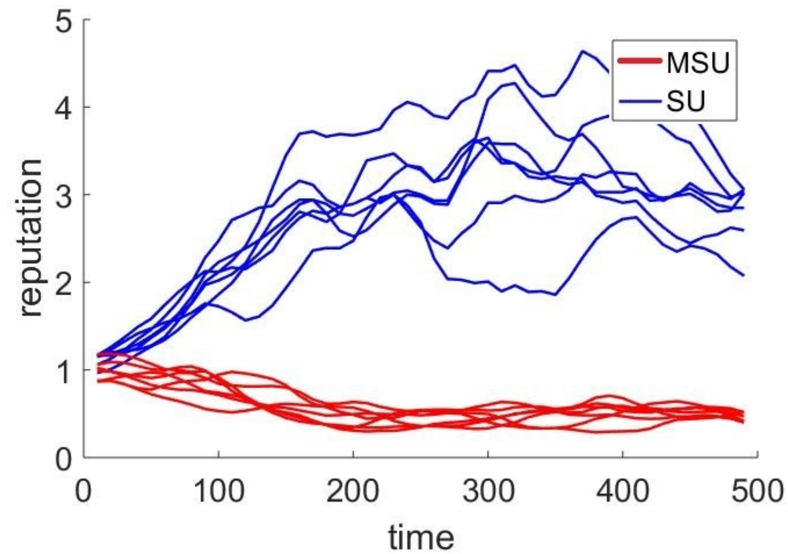
Dataset type 1 with $\eta = 0.01$

- Both work fine.
- High variation of reputation in multiplicative RUF may leads to more errors.

Multiplicative vs. Adaptive Multiplicative RUF



Multiplicative



Adaptive multiplicative

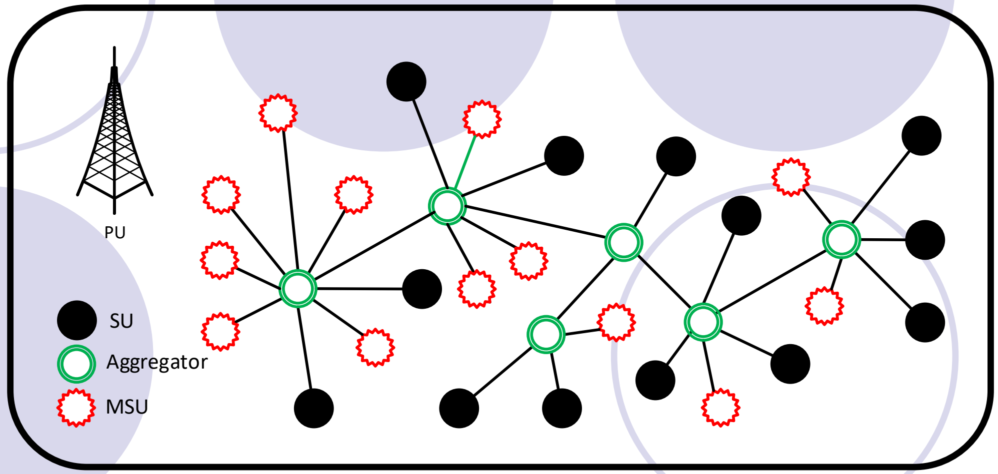
Dataset type 2 with $\eta = 0.01$

- High variation of reputation in multiplicative RUF leads to more errors.

6. Extension: Two-Level Majority Voting

A simple illustration

- 13 MSUs (clustered)
- 13 SUs
- 2 wrong aggregators
- 4 correct aggregators.

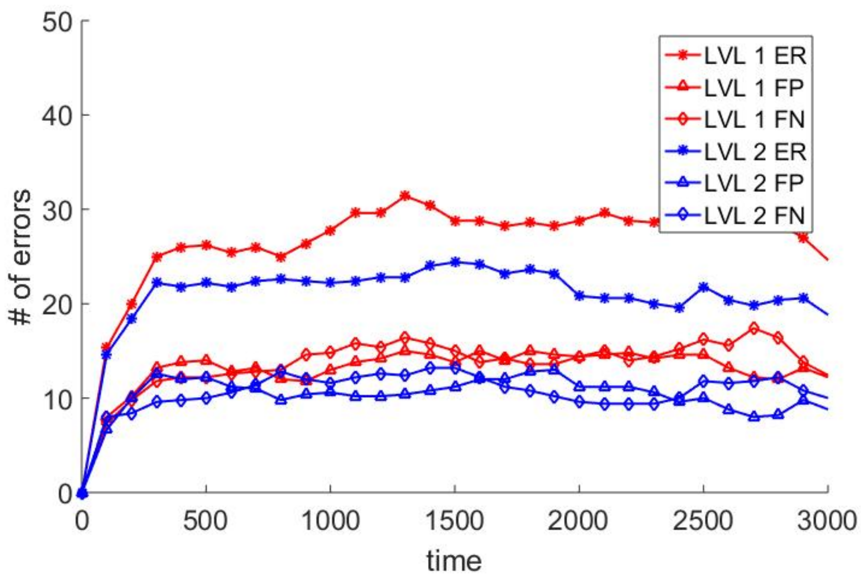


MSUs may win in one-level voting

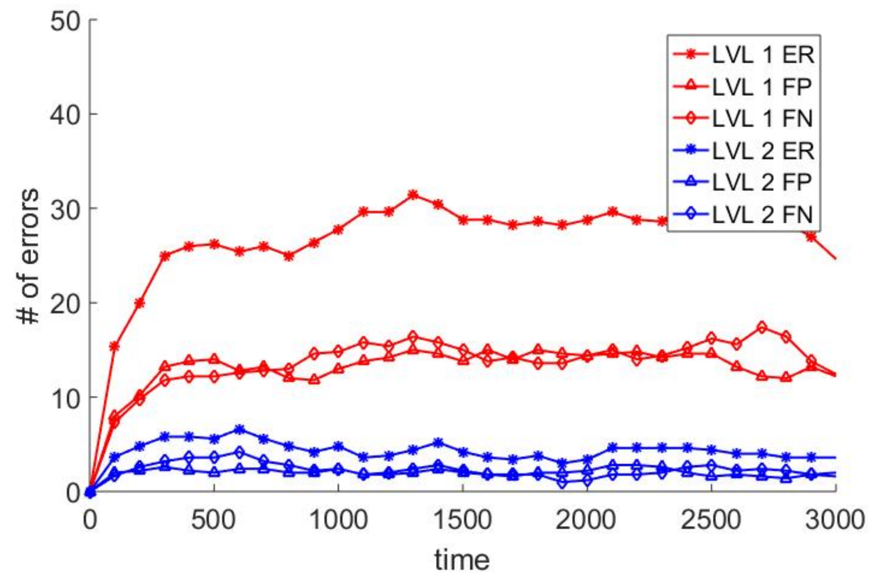
MSUs cannot win in two-level voting

Connected dominating set based distributed aggregator selection process

Two-Level vs. One-Level Voting



MSUs are sparse (uniform).



MSUs are clustered.

False positive (FP), False negative (FN), Error (ER), Level 1 (LVL 1), and Level 2 (LVL 2)

Dataset type 2 with $\eta = 0.01$

SU/MSU: 50/40

80% MSU: clustered

20% MSU and all SU: uniformly distributed

- Two-level voting works better when MSUs are clustered

7. Summary

- Adaptive multiplicative RUF using confidence
- Adaptive multiplicative RUF works better than other RUFs
- Two-level voting produces less errors than one-level voting