SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Avoiding monopolization: mutual-aid collusive attack detection in cooperative spectrum sensing

Jingyu FENG [1,3], Guangyue LU [1*], Yuqing ZHANG [2] & Honggang WANG [1]

[1]*Department of Communication Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;*
[2]*National Computer Network Intrusion Protection Center, University of Chinese Academy of Sciences, Beijing 101408, China;*
[3]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*

Appendix A Preliminaries

Appendix A.1 Cooperative spectrum sensing

A central identity called fusion center (FC) controls the process of Cooperative spectrum sensing (CSS): individual sensing, data reporting and decision making [1]. First, each SU exploits the energy detection to sense the signal of a PU via the sensing channel. Second, all SUs report their sensing data to FC via the reporting channel. Then FC combines the received local sensing information and determines the presence of PU.

Typically, individual sensing for PU signal with energy detection can be depicted as a binary hypothesis problem [2]:

$$y(t) = \begin{cases} n(t), & H_0 \\ h(t) \cdot s(t) + n(t), & H_1 \end{cases} \tag{A1}$$

where $y(t)$ represents the detected signal by each SU, $s(t)$ is the transferred PU signal, $h(t)$ is the channel gain of the sensing channel, $n(t)$ is the zero-mean additive white Gaussian noise, and t is the sample index. H_0 and H_1 denote the hypothesis of the inexistence and the existenc of PU signal, respectively. If the estimated energy of $y(t)$ is larger than the decision threshold, the existence of PU would be signal declared. Otherwise, there is no PU signal.

At the end of the individual sensing, the individual sensing data at each SU is determined. d_i indicates the individual sensing data of SU_i, which is generally expressed as a binary variable:

$$d_i = \begin{cases} 0, H_0 \\ 1, H_1 \end{cases} \tag{A2}$$

where "0" and "1" represent the hypothesis of the inexistence and the existenc of PU signal, respectively. Correspondingly, the final decision of FC is also binary under the "AND", "OR" and "Majority" rule. In the "AND" rule, FC makes d=1 if all d_i=1. The "OR" rule refers to d=1 if one d_i=1. The "Majority" rule requires at least a half of SUs to report 1. The "OR" rule works best when the number of SUs is large, whereas the "AND" rule works well when the number of cooperating users is small, and the "Majority" rule can be obtained from the k out of N rule under the condition when $k \geqslant N/2$ [1].

For the evaluation of the detection performance, the probabilities of individual detection P_d ($d_i = 1$ when the PU singal is using) and false alarm P_f ($d_i = 0$ when the PU singal is free) are defined .

In cooperative sensing, the probabilities of detection and false alarms for evaluating the performance of cooperative decisions are denoted by Q_d and Q_f, respectively, which can be written as [3]

$$\begin{aligned} Q_d &= Prob(H_1|H_1) = \sum_{k=l}^{N} \binom{N}{k} {P_d}^k (1-P_d)^{N-k} \\ Q_f &= Prob(H_1|H_0) = \sum_{k=l}^{N} \binom{N}{k} {P_f}^k (1-P_f)^{N-k} \end{aligned} \tag{A3}$$

It can be seen that the "OR" rule corresponds to the case of $l = 1$, the "AND" rule corresponds to the case of $l = N$ and the "Majority" rule corresponds to the case of $l \geqslant N/2$.

* Corresponding author (email: tonylugy@163.com)

Appendix A.2 Trust mechanism

Trust mechanism is increasing influence on many application scenarios, including e-commerce [4], P2P network [5], ad hoc network [6], online social communities [7], etc.

Trust mechanism also plays significant roles in CSS area, such as 1) assisting FC' reliable decision-making, 2) encouraging honset behaviors, and 3) preventing participating from attackers. Representative trust mechanism schemes are as follows. Zeng et al propose a reliable CSS scheme with trusted SUs assistance for mitigating SSDF attack in [8]. In [9], the authors consider trust as a competitive factor to punish attackers to access any vacant PU spectrum. In [10], the authors measure the trust value of each SU in CSS during the cognition cycle, and incorporate trust value into the data fusion to reduce the effect of attackers on final decision making. The commonality of these existing trust schemes is that the trust value of each SU is evaluated by its historical sensing behaviors and low weights are given to the sensing data for less trustworthy SUs when generating a final decision.

With the commonality, a basic trust scheme called Baseline is described to abstract these existing trust schemes. Since the sensing data from SUs can be viewed as a binary variable ("1" or "0"), it is easy for them to behave two types of sensing results: honest or false. In this case, FC can initialize the trust value of each SU by two indexes: the number of honest sensing (hon) and the number of false sensing (fal). Recently, the beta function is one of the most popular designs using binary input (i.e., positive or negative) to evaluate trust value. It first counts the number of positive and negative behaviors a user has performed, and then calculates the trust value with beta probability density function denoted by Beta(α, β) [11].

$$Beta(\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{A4}$$

where θ is the probability of behaviors, $0 \leqslant \theta \leqslant 1$, $\alpha > 0$, $\beta > 0$.

Take the i-th SU (SU$_i$) as an example, hon_i and fal_i represent the number of honest sensing (positive) and false sensing (negative) conducted by SU$_i$. Its trust value t_i can be calculated as

$$t_i = Beta(hon_i + 1, fal_i + 1) \tag{A5}$$

Consider the condition $\Gamma(n) = (n-1)!$ when n is an integer [12]. It can be found that the expectation value of the beta function is $E[Beta(\alpha, \beta)] = \alpha/(\alpha+\beta)$. Therefore, t_i can be further described as

$$t_i = \frac{1 + hon_i}{2 + hon_i + fal_i} \tag{A6}$$

Appendix B Simulation results and discussion

Simulation results are presented that analyze MAC attack and show the performance of its defense scheme-DMAC. The general simulation setup is shown in Table B1.

The simulations are performed by cycle-based fashion. At each cycle, SUs are selected randomly to execute CSS actions with each other. After a few cycles, a trusted network topology is gradually generated by trust mechanism. FC then utilizes it to execute the following CSS actions, and update the trust value on the corresponding SUs.

To evaluate the strengthen of attacks, we compare relaxed collusive (RC) with MAC in terms of their attack success ratio and attack rounds for forming high-trust attackers. Briefly speaking, the behavior pattern for RC attackers is to fake sensing data in an unorganized way. MAC attackers, conducted by four attack procedures in a round mode, help with each other.

As shown in Figure B1, MAC attack can get higher attack success ratio than RC attack against the "AND", "OR" and "Majority" rule. For the "AND" rule, the threat of attacks is limited. The reason is that the "AND" rule refers the final decision as "1" only when all the sensing data from each SU are "1". Nevertheless, the "AND" rule has a disadvantage that final decision rule is "0" if an attacker fakes "0". For the "OR" rule, the threat of attacks is biggest. The "OR" rule refers the final decision as "1" so long as one attacker fakes "1". It can be seen that the threat to the "Majority rule increases with the percentage of attackers. The attackers can mislead the final decision when they become the majority. To make a reliable final decision, the "Majority" rule is a good choice for FC.

In trust mechanism, an attacker such as SU_i can be detected by $T_i < \varepsilon$. To increase its attack strengthen, SU_i need to be disguised as a high-trust attacker, i.e. $T_i \geqslant \varepsilon$. As shown in Figure B2, MAC attackers can form high-trust attackers with

Table B1 Description of simulation elements.

Parameters	Description	Default
N	Number of SUs	60
P	Number of PUs	5
$cycle$	Number of cycle simulation	100
$round$	Rounds of attack	50
p_a	Percentage of attackers	0∼50%
λ	Trust warning line	0.3
ε	Threshold of trust value	0.5
δ	Threshold of outlier value	0.8

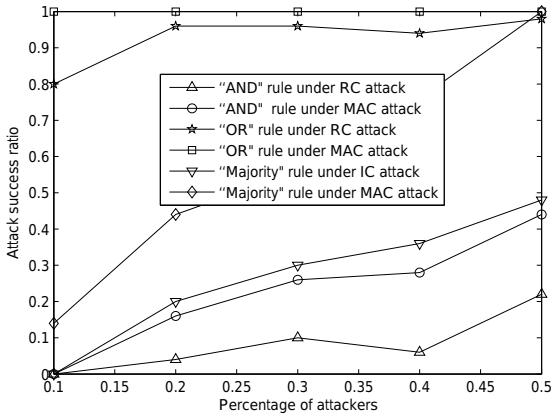

Figure B1 MAC attack success ratio vs. RC attack.

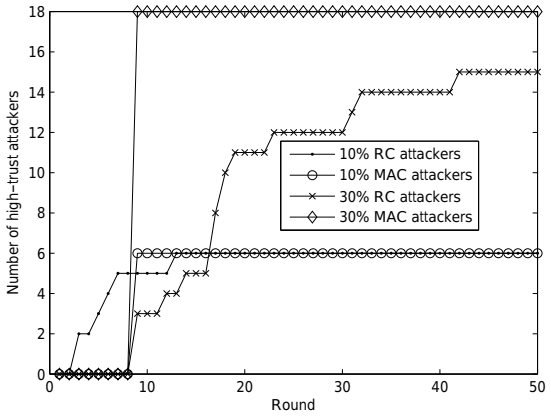

Figure B2 MAC attack vs. RC attack under forming high-trust attackers.

less rounds of attack. Generally speaking, RC attackers improve their trust by reporting honest sensing data sometimes, whereas MAC attackers can help with each other and improve their trust by employing a quick recovery "trust-improving". So, MAC attackers can become high-trust faster than RC attackers.

To defend against MAC attack, the first important measure is to suppress the increase of MAC attackers' trust value. Therefore, we choose an MAC attacker randomly to observe the variation of its trust value with the Baseline and DMAC scheme. Figure B3 shows that MAC strategies make the attacker's trust value fluctuate along with cycles. Such trust value usually outweighs ε in the Baseline scheme. Fortunately, his trust value can be reduced by the DMAC scheme after 25 cycles. This is because the DMAC scheme can filter out "the number of honest sensing" of MAC attackers and prevent this index in trust evaluation.

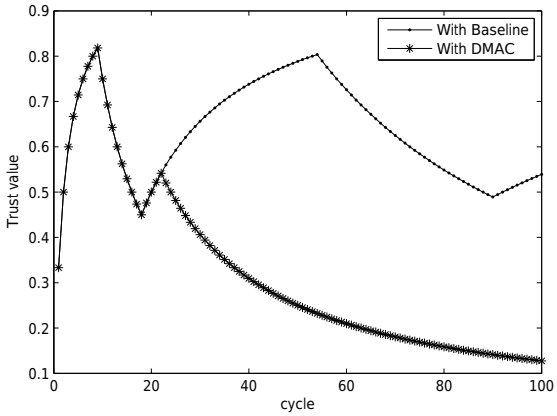

Figure B3 Variation of an MAC attacker's trust value.

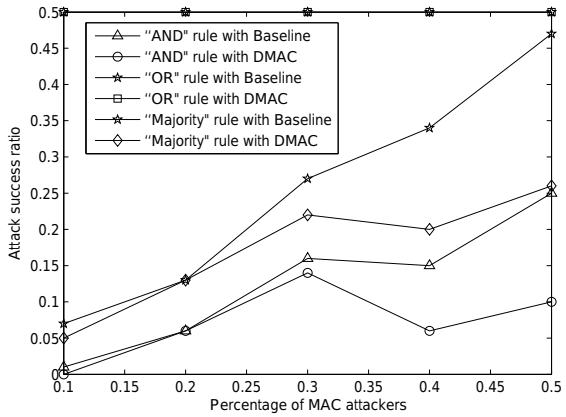

Figure B4 Suppressing MAC attack success ratio.

We can also find in Figure B4, the DMAC scheme can suppress MAC attack success ratio better than Baseline under the "AND" and "Majority" rule. For the "OR" rule, only one false "1" data can make the final decision as "1". In summary, to make a reliable final decision, the "OR" rule is not a good choice with the threat of MAC attack.

Since MAC attackers always report "1" no matter whether PU spectrums are present, the probabilities of false alarms (Q_f) should be analyzed by comparing DMAC with Baseline. The Q_f simulation is based on the energy detection by performing 5000 rounds of Monte Carlo detection, in which the primary signal is a baseband QPSK modulated signal under the AWGN (additive white Gaussian noise) environment. The parameters used in the Q_f simulation are set as: the sampling frequency is f_s=1KHz, the time-bandwidth product is m=50, and the average SNR is -8dB.

As shown in figure B5, we vary the percentage of MAC attackers to observe Q_f. For the "AND" rule, the damage of MAC attack is limited in Q_f. For the "OR" rule, the damage of MAC attack in Q_f is the most, but DMAC can suppress Q_f better than Baseline under the "OR" rule. It can be seen that the damage of MAC attack under the "Majority" rule is also limited in the DMAC scheme, but amplifies with the percentage of MAC attackers in the Baseline scheme.

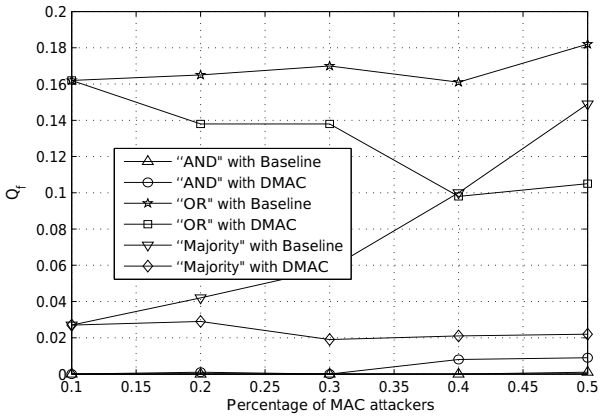

Figure B5 Suppressing Q_f at MAC attack.

References

1 Akyildiz I F, Lo BF and Balakrishnan R. Cooperative spectrum sensing in cognitive radio networks: A survey. Physical Communication, 2011, 4:40-62

2 Peh E, Liang Y C, Guan Y L, et al. Optimization of cooperative sensing in cognitive radio networks: a sensing-throughput tradeo view, IEEE Transactions on Vehicular Technology, 2009,58: 5294-5299

3 Zhang W and Mallik R K. Cooperative Spectrum Sensing Optimization in Cognitive Radio Networks. In Proceedings of IEEE International Conference on Communications, Beijing, 2008: 3411-3415

4 Morid M A and Shajari M. An enhanced e-commerce trust model for community based centralized systems. Electronic Commerce Research, 2012, 12: 409-427

5 Li X Y, Zhou F and Yang X D. Scalable feedback aggregating (SFA) overlay for large-Scale P2P trust management. IEEE Transactions on Parallel and Distributed Systems, 2012, 23:1944-1957

6 Boukerche A, Ren Y and Pazzi R. An adaptive computational trust model for mobile ad hoc networks. In Proceedings of the 5th International Conference on Wireless Communications and Mobile Computing, Leipzig, 2009. 191-195

7 Mohaisen A, Hopper N and Kim Y. Keep your friends close: incorporating trust into social-network-based sybil defenses. In Proceedings of 30th IEEE INFOCOM Conference, Shanghai, 2011. 1943-1951

8 Zeng K, Peng Q H, Tang Y X. Mitigating spectrum sensing data falsification attacks in hard-decision combining cooperative spectrum sensing. Sci China Inf Sci, 2014, 57: 042318

9 Feng J Y, Lu G Y, Chang H. Behave well: how to win a pop vacant band via cooperative spectrum sensing. KSII Transactions on Internet and Information Systems, 2015, 9:1321-1336

10 Pei Q Q, Yuan B B, Li L, et al. A sensing and etiquette reputation-based trust management for centralized cognitive radio networks. Neurocomputing, 2013, 101: 129-138

11 Jϕsang A, Ismail R.The beta reputation system. In Proceedings of the 15th Bled Electronic Commence Conference, Bled, 2002.1-14

12 Gamma function. http://en.wikipedia.org/wiki/Gamma function