허위 경보 제로 정적 오류 분석기 사례 1

무인비행체 제어 소프트웨어에 특화시키기

장수원
(공동연구: 김유일,오학주,이우석)

서울대학교 프로그래밍 연구실

2010/08/25
소프트웨어 무결점 연구소 여름 워크샵

Goal

Zero false alarm

Buffer overflow

Static analyzer

for

UAV control software

from SNU FDCL LAB

Position 1

General-purpose & Sound & Zero false alarm

IMPOSSIBLE

But what if

focusing on one **SPECIFIC** software?

POSSIBLE

Position II

What's the use of such specialized analyzer?

Softwares sharing programming idioms

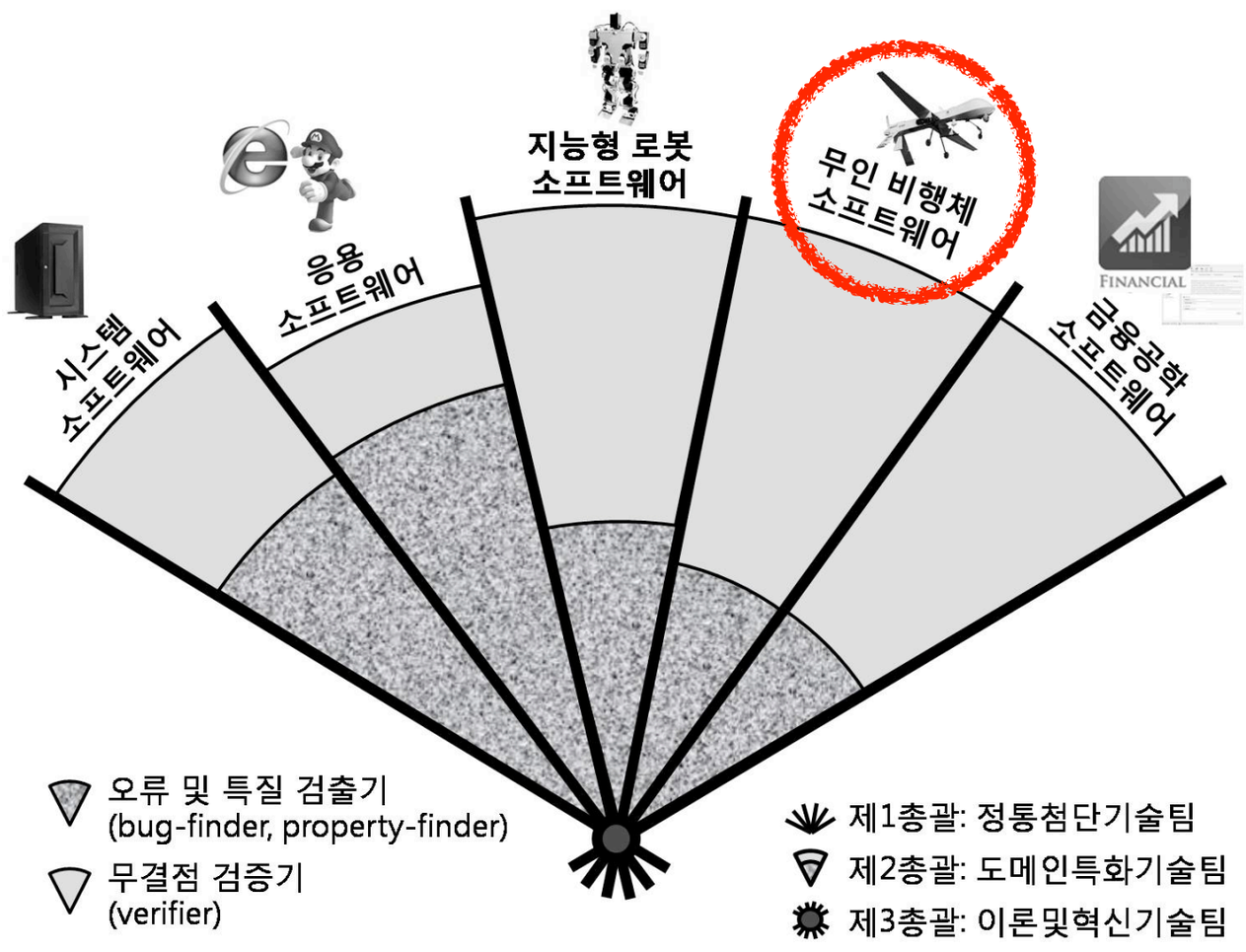
Analyzing UAV software's next releases
Analyzing similar softwares in the same domain

Expect zero false alarms

And...

ROSAEC Center's flagship projects

UAV software analyzer



UAV Code Properties

- 5008 Lines C code
- No dynamic memory allocations
- No recursions & No multiple calls
- Linear relation between index variables
- Infinite loop, but finitely stable

Specialization

	Before Specialization	After Specialization
false/total alarms #	11/27	0/16
false alarm ratio	41%	0%
time(s)*	0.19	14.8

* Intel Core2Duo 2.66Ghz / 4GiB

Specialization

- Octagon relational domain
- Delayed widening
- Selective relational analysis
- Variable dependence analysis

Before Specialization

- Sparrow : industrial-level general purpose analyzer
- 16 bugs are found
- 11 false alarms

UAV Bug : Case 1

Buffer index not properly managed : 9/16

Buffer overflow

```
do
{
  if(s[m]==',') n_comma++;
  m++;
} while(!(n_comma==9));
```

offset: [0; ∞], size: [100; 100]

s is input from hardware

buffer overflow when input doesn't have sufficient commas

UAV Bug : Case 2

Trivial buffer access mistake : 3/16

```
void GPS_CHECK(void)
{
  ...
  static char sentence1[100];
  ...
  static int j=0;
  while(LSR1&0x01==
     ...
     if(sentence1[j-2]=='*' || ...)
     ...
   }
}
```

Buffer overflow

offset: [-2; 73], size: [100; 100]

||

UAV Bug : Case 3

Trivial array initialization mistakes : 4/16

```
double th[1][5]=
{-0.28, 0.51,-4.53,-0.65,3.16};
```

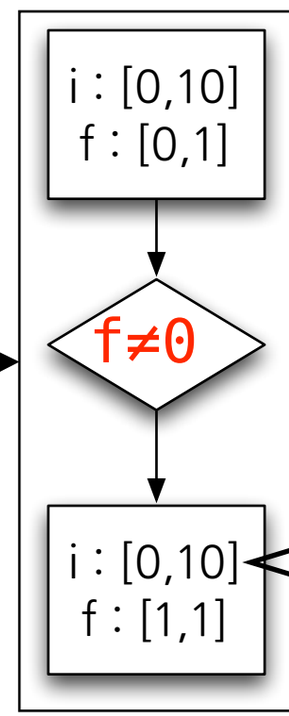
Why False Alarms?

- Interval-based analyzer
- No relational information
- Precise loop analysis impossible w/o Relational information

UAV False Alarm Case

```
i:=0; /* index */
f:=0; /* flag */
buf[10];

while(true) {
  if(f=0) {
    f:=1; i:=0;
  } else /*f≠0*/{
    buf[i]=io();
    i++;
    if(i=10) {
      f:=0;
    }
  }
}
```



- $f \neq 0 \rightarrow i < 10$
- No relational information between i and f
- Cause a false alarm

Removing False Alarms

- Relational information → More precise analysis
- Only need relation between 2 variables
- Octagon is enough (cf. polyhedron, ...)

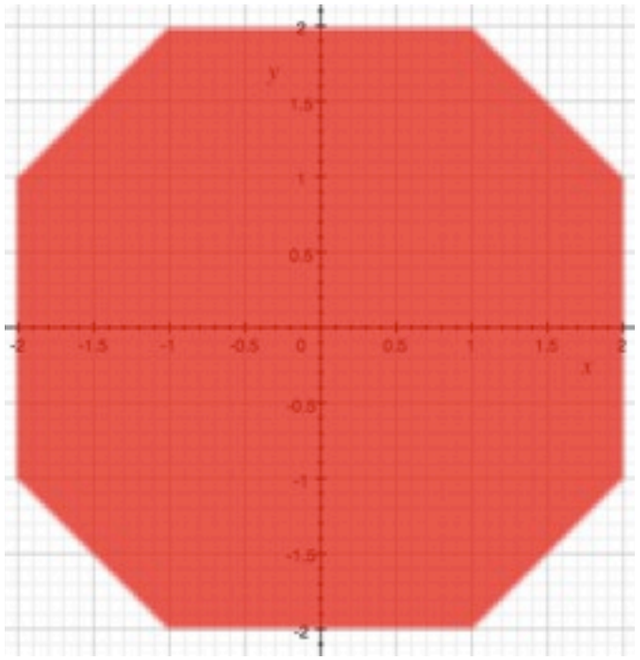
Octagon Domain

[Mine 2006]

Intuitively,

interval
+
bounds of sum & difference of 2 variables

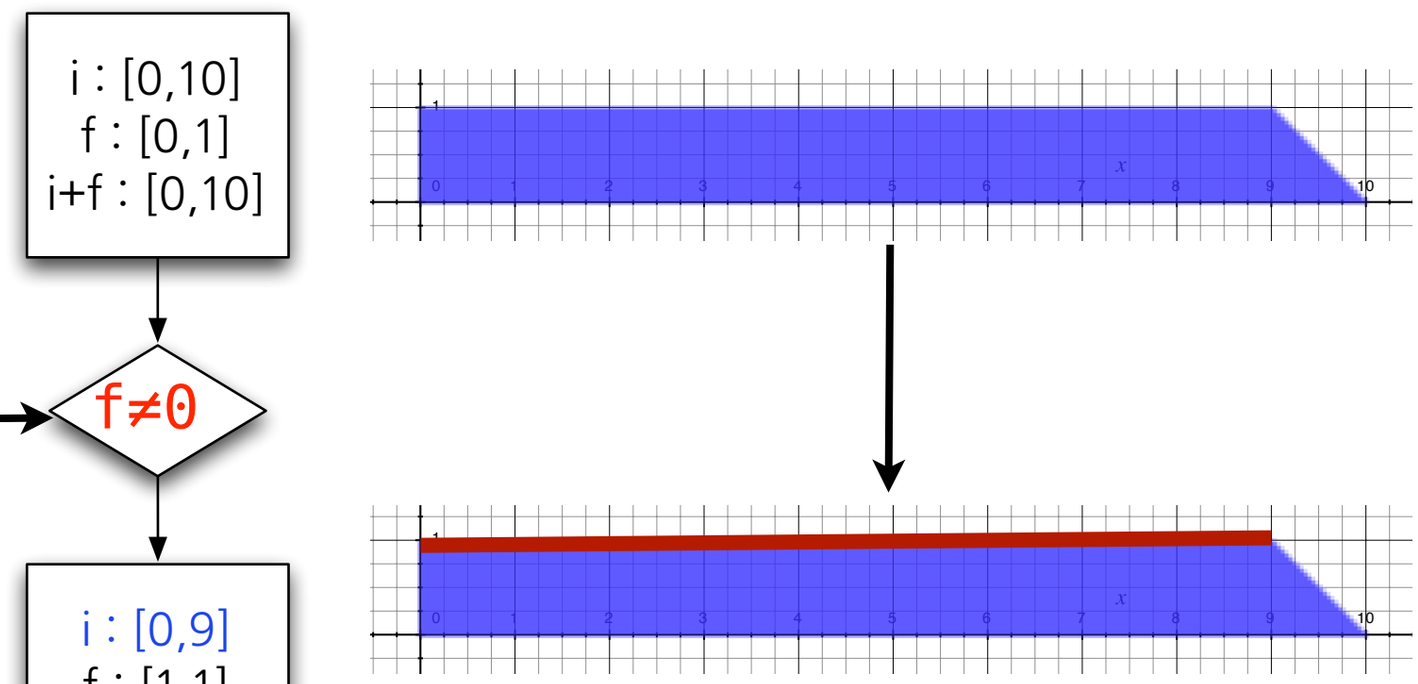
$$
\begin{array}{cccccc}
 & -2 & \leq & x & \leq & 2 \\
\wedge & -2 & \leq & y & \leq & 2 \\
\wedge & -3 & \leq & x - y & \leq & 3 \\
\wedge & -3 & \leq & x + y & \leq & 3
\end{array}
$$



Removing False Alarm Case

```
i:=0; /* index */
f:=0; /* flag */
buf[10];

while(true) {
  if(f=0) {
    f:=1; i:=0;
  } else /*f≠0*/ {
    buf[i]=⊤;
    i++;
    if(i=10) {
      f:=0;
    }
  }
}
```



- Using relation information (i+f : [0,10])

Adopt Octagon But...

Only 1 false alarm is removed

	Original	Octagon	Oct + Dep + DW
False/Total	11/27	10/26	0/16
False alarm ratio	41%	37%	0%
Time(s)	0.19	10.6	14.8

What happened?

Pruning memory with ‘e≠e’ is impossible

```
i := 0;
buf[17];

while(true)
{
    buf[i]:=io();
    i++;
    if(i=17) {
        i:=0;
    } else {
        skip;
    }
}
```

$[0,0] \triangledown [0,1] = [0,+\infty]$

$[1,+\infty]$

$[17,17]$

$[0,0]$

$[1,+\infty]$

$[0,0] \sqcup [1,+\infty] = [0,+\infty]$

Imprecise Analysis

Delayed widening?

No widening until stable

```
i := 0;
buf[17];

while(true)
{
    buf[i]:=⊤; /* I/O */
    i++;
    if(i=17) {
        i:=0;
    } else {
        skip;
    }
}
```

$[0,0] \sqcup [0,16] = [0,16]$

$[1,17]$

$[17,17]$

$[0,0]$

$\boxed{[1,16]}$

More precise

$[0,0] \sqcup [1,16] = [0,16]$

Scalability : Problem

- First try : track all variable pairs' relations
- Memory exhausted in 4GiB machine.
- 385^2 variable relations in UAV Software

Scalability : Solution

Selective relational analysis

- Global non-relational analysis
- Select variables alarm depends on
- Apply relational analysis to the selected only.

Dependence Analysis
for Selective Relational Analysis

x depends on y $\leftrightarrow$ if y changes, x may change

dependence analysis $\leftrightarrow$ find all variables that each variable depends on

```
x := y + z
w := x + y
```

w depends on {x, y,z}

```
if (x + y < 10)
  z := 1
```

z depends on {x, y}

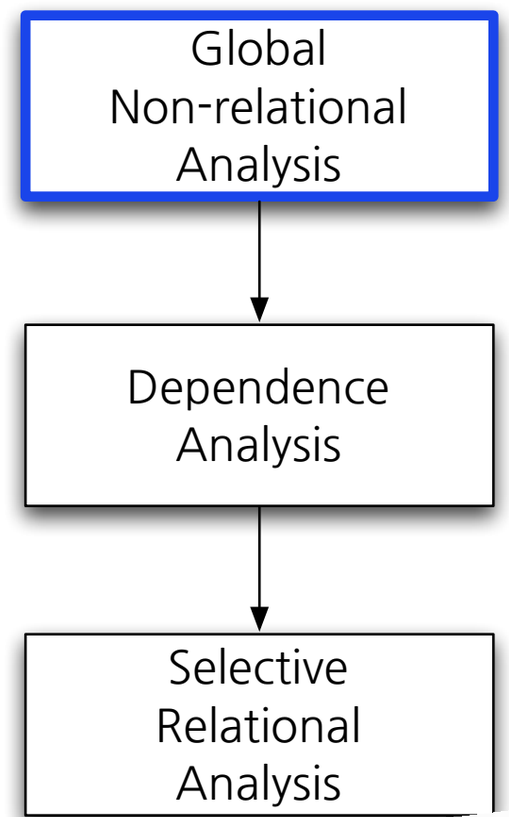
Dependence Analysis
for Selective Relational Analysis

- Find variable sets that each alarm depends on
- Analyze relevant statements only
- Reducing # of relations tracked greatly
  - $385^2 \rightarrow 18.2^2$ per alarm on average

Selective Relational Analysis

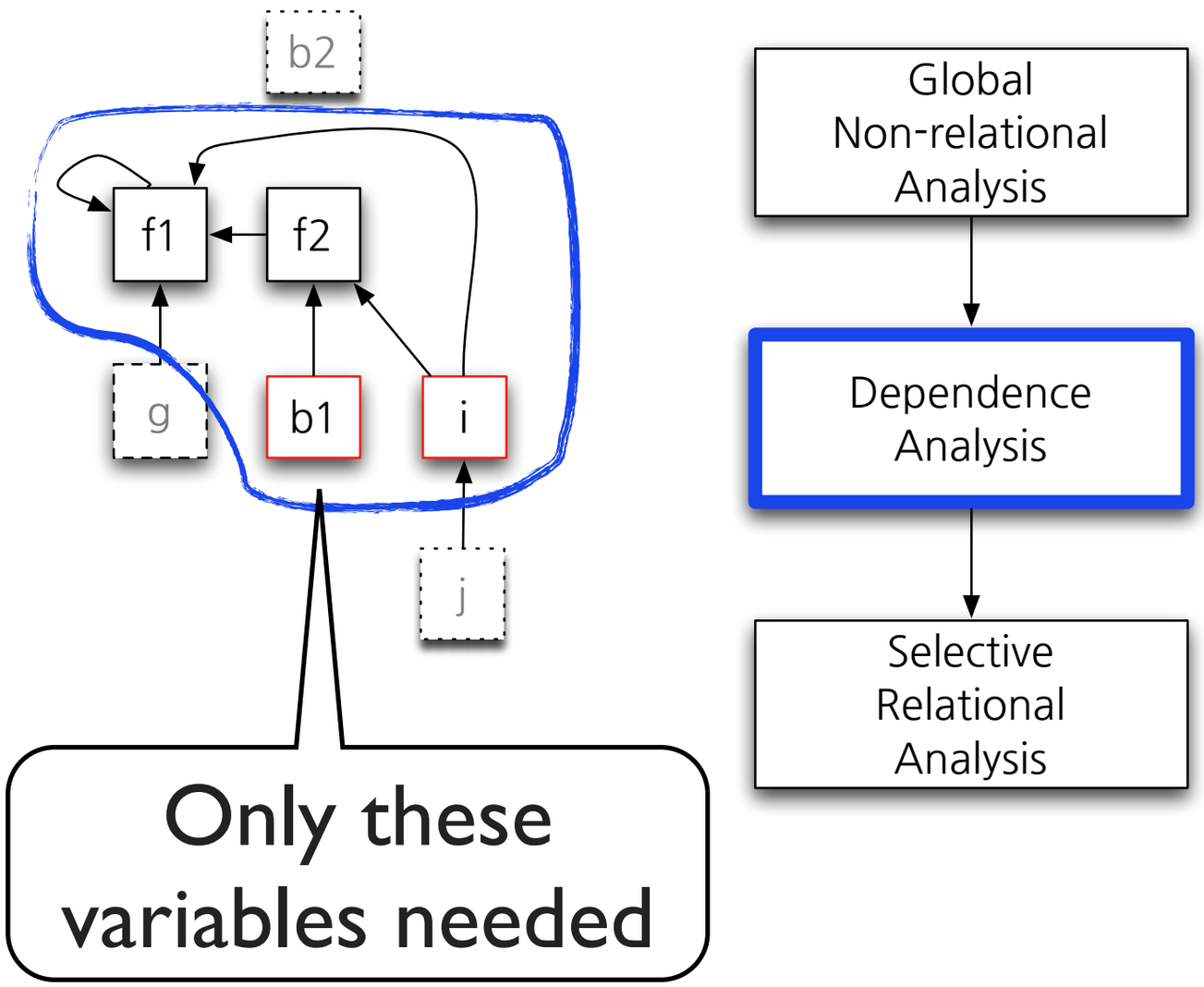
```
b1[20];
b2[100];
f1,f2 := 1,0;
i,j := 0,0;
while(true) {
  if(f1=1) {
      f1:=0;
      f2:=1;
      i:=0;
  }
  g := i + 10;
  if(f2=1) {
    b1[i] :
    i++;
    if(i=7)
      ...
       i:=0;
     ...
  }
```

offset: [0,∞], size: [20,20]



Selective Relational Analysis

```
b1[20];
b2[100];
f1,f2 := 1,0;
i,j := 0,0;
while(true) {
  if(f1==1) {
     f1=0;
     f2=1;
     i=0;
}
g = f1 + 10;
if(f2==1) {
  b1[i]=io();
  i++;
  if(i==7) {
     ...
      j = 0;
    ...
  }
```

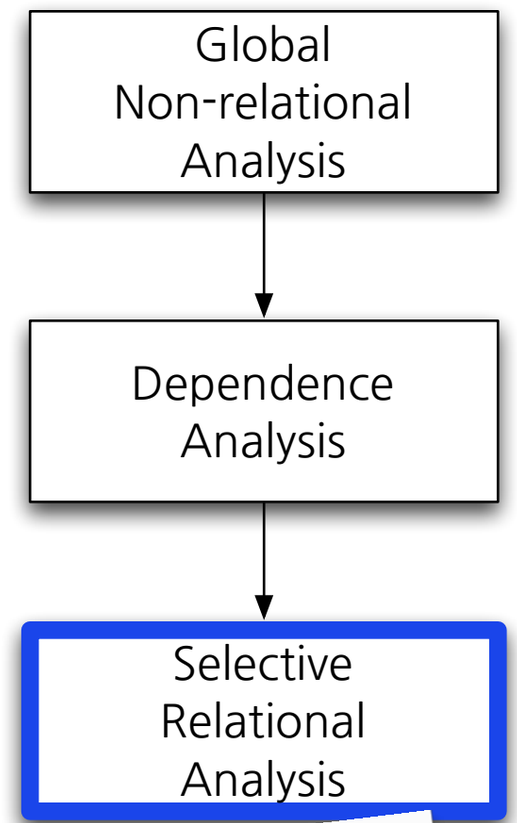


Selective Relational Analysis

Only analyze statements w/ {b1, i, f1, f2}

```
b1[20];
b2[100];
f1,f2 := 1,0;
i,j  := 0,0;
while(true) {
   if(f1==1) {
        f1=0;
        f2=1;
        i=0;
   }
   g = f1 + 10;
   if(f2==1) {
      b1[i]=io();
      i++;
      if(i
         ..
         j = 0;
```

offset: [0,6], size: [20,20]



Result

	Before	Specialized
false/total alarms #	11/27	0/16
false alarm ratio	41%	0%
time(s)*	0.19	14.8

* Intel Core2Duo 2.66Ghz / 4GiB

And more...

- 7 alarms → more precise
  - size : [100,100]
  - offset : [-2, +∞] ➔ [-2,73]

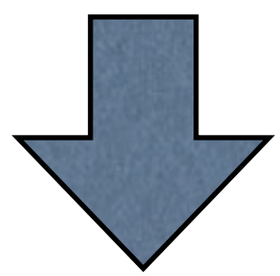
Position Test (Work in Progress) Another UAV Control Software

	Before	Specialized
True alarms	40	40(4 improved)
False / Unknown	3 / 12	0 / 12
Total	55	52
time(s)*	2.7	30.5

* Intel Core2Duo 2.66Ghz / 4GiB

Conclusion

- The Octagon domain
- Delayed widening
- Selective relational analysis
- Variable dependence analysis



UAV Control Software
Zero false-alarm analyzer

Questions
&
Comments