PAPER • OPEN ACCESS

Analysis of the impact of threats to change and block responses of experts in online survey systems

To cite this article: B I Efimov and P S Lozhnikov 2020 *J. Phys.: Conf. Ser.* **1546** 012079

View the article online for updates and enhancements.

Analysis of the impact of threats to change and block responses of experts in online survey systems

B I Efimov and P S Lozhnikov

Omsk State Technical University, 11, Mira ave., 644050, Omsk, Russia
b_efimov@mail.ru

Abstract. The authors of the article analyze the impact of information security threats when conducting online surveys with an uncertain number of respondents. The article discusses threats to change responses of experts and block responses of experts. Finding the probability of making an erroneous decision using the methods of probability theory is a very difficult task. The authors propose using the Monte Carlo method as a solution. A software module that implements this method has been developed. We obtained the dependence of the probability of making an erroneous decision on the probability of changing the answers of experts, the probability of blocking the answers of experts and the number of respondents. The authors showed that there are critical values for the probability of changes in the responses of experts. These values determine the boundaries of ranges with different characteristics of the dependence of the probability of making an erroneous decision. The authors proposed two methods for finding one of the critical values. In conclusion, the authors formulated conditions that reduce the probability of making an erroneous decision.

1. Introduction

When conducting online surveys, in most cases, the list of persons participating in the vote and the number of respondents are not determined in advance. In addition, reliable authentication and digital signature mechanisms are not used. This distinguishes online survey systems from decision-making systems involving experts and electronic voting systems.

The security problems of electronic voting systems are described in detail in [1, 2], the works of Chaum D., Schneier B., Fujioka A., Kohno A., Kremer S., Rubin A., Lifshits Yu., Babenko L. In these works, cryptographic protocols are described as the main security measures.

An analysis of the impact of information security threats on the online voting system can be carried out in terms of assessing the reliability of distributed information systems. Mathematical models of reliability of distributed systems are described in detail in [3, 4], in the works of Pereguda A., Akimova G., Strukov A.

The main task of the information security system during online surveys is to prevent changes in the alternative, for which the majority of respondents voted. Threats to information security are significant only if they lead to the choice of another alternative. Changing the selected alternative may be affected by threats to block or change expert responses.

The most difficult case is the simultaneous impact of threats to change and block expert responses. The purpose of this study is to determine the dependence of the probability of making an erroneous decision on the probability of changing expert responses, the probability of blocking expert responses, and the number of respondents.

2. Determining the probability of making an erroneous decision

We define the following initial positions:

   – a survey of experts is carried out at the choice of one of two alternatives: "0" and "1";

   – the attacker's actions are aimed at changing the answers of experts in favor of the alternative "0";

   – $P(A0)$ – probability of making an erroneous decision;

   – P_{block} – probability of blocking answers of expert ($P_{block\ i} = const$);

   – P_{change} – probability of changes answers of expert ($P_{change\ i} = const$);

   – m – total number of experts (respondents);

   – n – number of experts who voted for alternative "1".

For $P_{block} \neq 0$ & $P_{change} \neq 0$, obtaining an analytical solution to the problem of finding $P(A0)$ using probability theory methods is a rather complicated task. In this regard, the authors proposed to use the method of modeling random variables - the method of statistical tests Monte Carlo.

This method is implemented in the C++programming language. To obtain a reliable result, a large number of statistical tests (10^6) are performed for each set of initial data.

2.1 Dependence of P(A0) on P_{change} for various values of m

We obtained the dependence of $P(A0)$ on P_{change} for various values of m. The calculations were repeated for different values of P_{block} (from 0 to 0.99) and n/m.

Figure 1 shows a graph of the dependence of $P(A0)$ on P_{change} for $m = \{10;\ 20;\ 40\}$ ($P_{block} = 0.8$; $n/m = 0.6$).

As a result of the analysis of this mathematical model, the following results were obtained:

- a decrease in P_{change} leads to a decrease in $P(A0)$;

- for any $P_{block} \geq 0$ there is a certain value P'_{change}, in which the values of $P(A0)$ for different values of m are the same (for $n/m = const$);

- an increase in m leads to a decrease in $P(A0)$ only for $P_{change} < P'_{change}$.
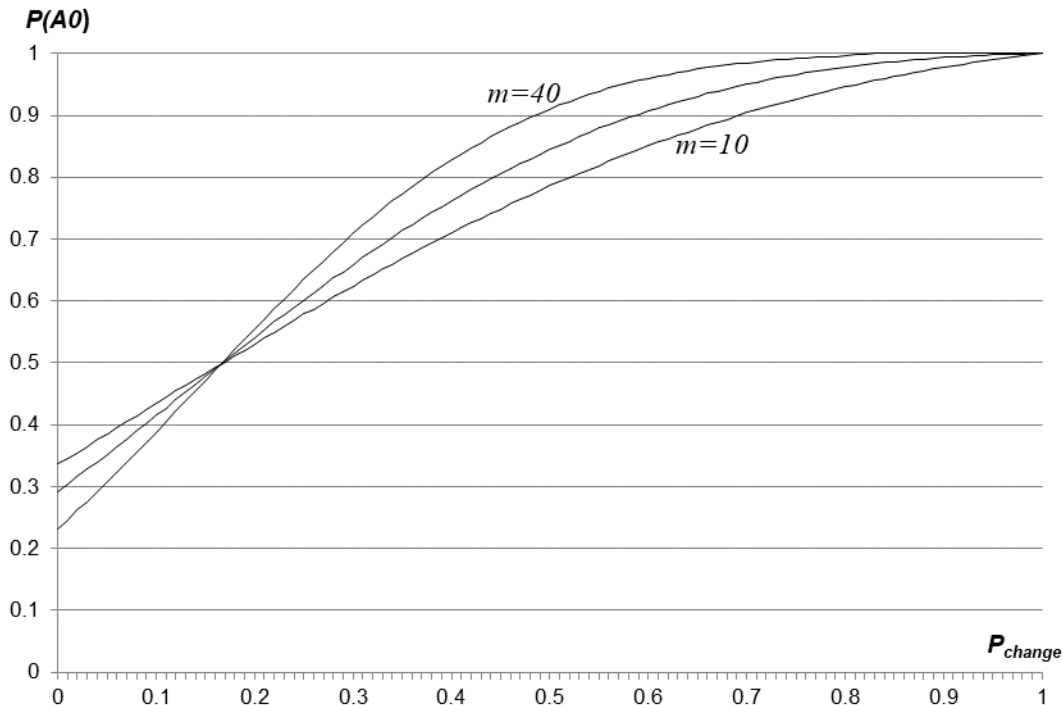

Figure 1. Graph of the dependence of the probability $P(A0)$ on the probability P_{change} for different values of m (for $n/m = 0.6$).

2.2 Dependence of P(A0) on P_{change} for various values of P_{block}

We obtained the dependence of $P(A0)$ on P_{change} for different values of P_{block}. The calculations were repeated for different values of m and n/m.

Figure 2 shows a graph of the dependence of $P(A0)$ on P_{change} for different values of P_{block} ($P_{block} = \{0; 0,2; 0,4; 0,6; 0,8; 0,99\}$, $m = 20$, $n/m = 0.6$). The value $P_{block} = 0.99$ is taken to illustrate the behavior of the system when $P_{block} \rightarrow 1$.

As a result of the analysis of this mathematical model, the following results were obtained:

– a decrease in P_{change} leads to a decrease in $P(A0)$;

– there is a certain value P'_{change}, in which the values of $P(A0)$ for different values of m are the same (for $n/m = const$);

– a decrease in P_{block} leads to a decrease in $P(A0)$ only for $P_{change} < P'_{change}$.
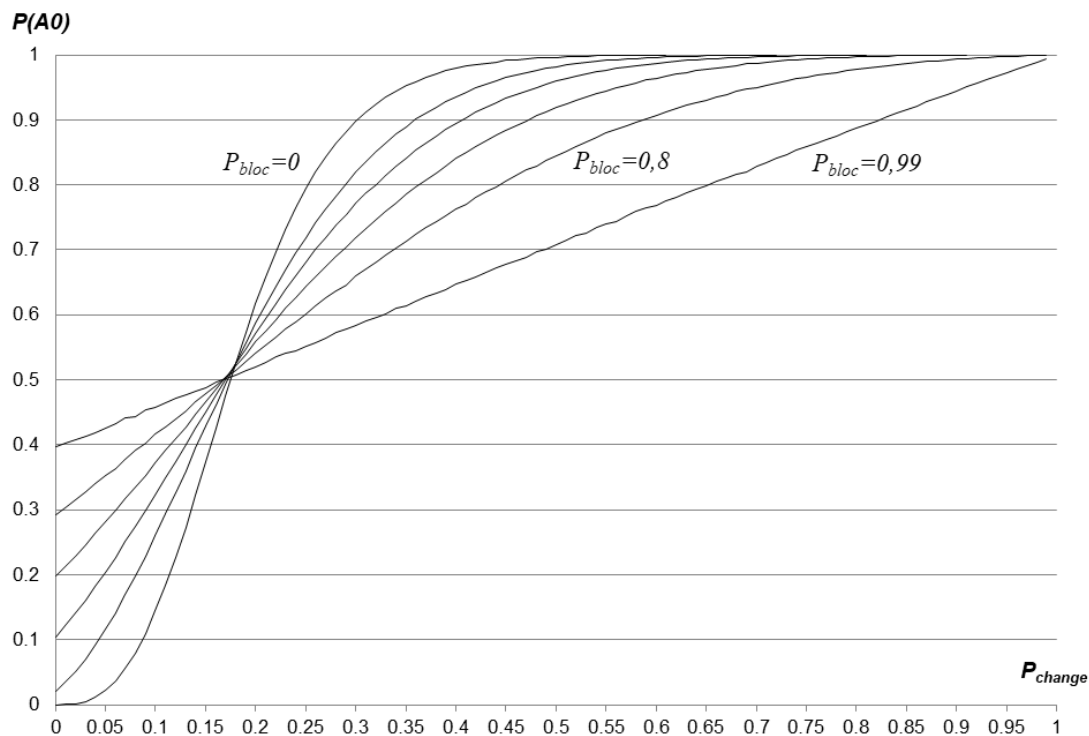

Figure 2. Graph of the dependence of the probability $P(A0)$ on the probability P_{change} for different values of P_{block}.

3. Methods for determining the probability P''_{change}

The authors propose two methods for determining the value of P''_{change}.

3.1 Method 1

For two different values of P_{block} (for example, 0 and 0.99), the dependencies $P_1(A0)$ and $P_2(A0)$ on P_{change} are found. For a series of all values of P_{change}, $\Delta = \left| P_1(A0) - P_2(A0) \right|$ is calculated. There is a value of P_{change} at which Δ is minimal ($\Delta \rightarrow 0$); the found value of P_{change} will be the value of P''_{change} for the given n/m and m.

The results of P''_{change} calculations depending on n/m ($0.51 \leq n/m \leq 1$) with the number of respondents $m = 100$ are shown in figure 3.

Using other values of m ($m = \{10, 20, 50\}$) it was established that P''_{change} depends only on n/m and does not depend on m.
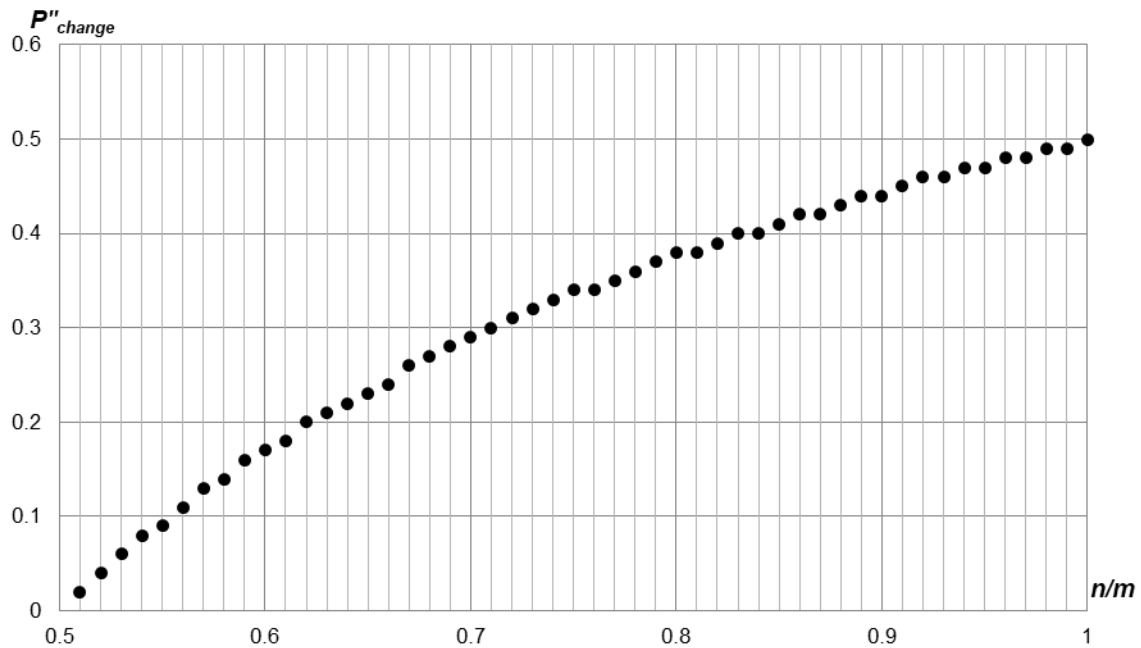
Figure 3. Graph of the dependence of P''_{change} on the ratio n/m (for $m = 100$).

4.1 Method 2
The method is based on the following features of the system under consideration: when $P_{change} \rightarrow P''_{change}$ in a series of many trials, the number of times a repeat vote should be assigned reaches the maximum value. Repeated voting is appointed when, after exposure to threats, the number of votes for alternatives "0" and "1" is the same.

Figure 3 shows the dependence of the relative number of repeat vote assignments C_{half} on the probability of changing expert responses P_{change} at $n/m = 0.6$.
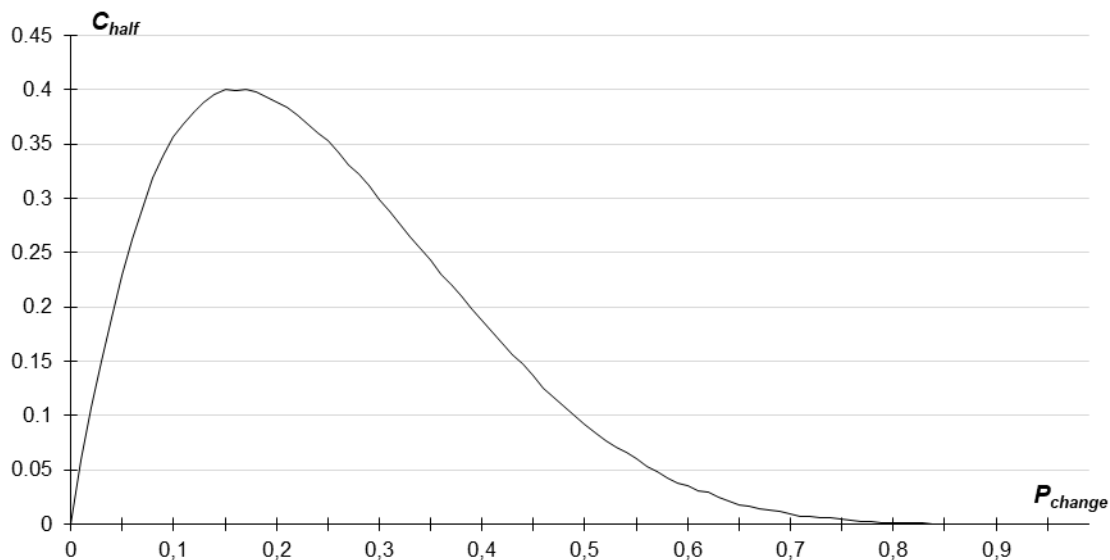

Figure 4. Graph of the dependence of C_{half} on the probability P_{change} (for $n/m = 0.6$).

The values of P''_{change} calculated by the two methods above are the same. For example, for the ratio $n/m = 0.6$, the C_{half} index reaches its maximum value at $P_{change} \approx 0.16$ (the maximum of the function in

graph 4). The value of P''_{change} calculated by the first method is also approximately *0.16* (in graph 3, the value of the function at *n/m = 0.6*).

4. Conclusion

The authors of the article obtained the following main results:

– there is a certain value P''_{change}, where *P(A0)* for different values of P_{block} (for *n/m = const*) are the same. A decrease in P_{block} leads to a decrease in *P(A0)* only with $P_{change} < P''_{change}$;

– for any $P_{block} \geq 0$ there is a critical value P'_{change}, in which the values of *P(A0)* for different *m* are the same. An increase in *m* leads to a decrease in *P(A0)* only at $P_{change} < P'_{change}$.

Thus, an increase in the number of respondents *m* and a decrease in the probability of blocking answers of experts P_{block} are not always justified.

We can formulate the conditions for reducing the probability of making an erroneous decision *P(A0)* under the influence of threats to change and block the answers of experts:

– reducing the probability of changing the responses of experts P_{change};

– increasing the number of experts *m* (if $P_{change} < P'_{change}$ for the assumed value of *n/m*);

– reducing the probability of P_{block} (if $P_{change} < P''_{change}$ for the assumed value of *n/m*).

References

[1]   Gibson J P, Krimmer R, Teague V and Pomares J 2016 A review of E-voting: the past, present and future *Annals of Telecommunications* **71** 279-86

[2]   Neumann Stephan & Volkamer Melanie & Budurushi, Jurlind & Prandini Marco (2016). SecIVo: a quantitative security evaluation framework for internet voting schemes *Annals of Telecommunications* **71** 337-52.

[3]   Rausand M 2014 *Reliability of Safety-Critical Systems: Theory and Applications* (New Jersey: Wiley)

[4]   Kenneth B 2006 *Reliable Distributed Systems: Technologies, Web Services, and Applications* (New York: Springer)