Method of secure communication in a group of unmanned aerial vehicles based on credit theory

Iuliia Kim
Faculty of Secure Information Technologies
ITMO University
Saint Petersburg, Russia
yulia1344@gmail.com

Ilya Viksnin
Faculty of Secure Information Technologies
ITMO University
Saint Petersburg, Russia
wixnin@mail.ru

Sergei Chuprov
Faculty of Secure Information Technologies
ITMO University
Saint Petersburg, Russia
drmyscull@gmail.com

Danil Zakoldaev
Faculty of Secure Information Technologies
ITMO University
Saint Petersburg, Russia
d.zakoldaev@mail.ru

***Abstract*—*In this article multi-agent robotic systems are considered in the context of providing information security. Preference is given to decentralized collective strategy of group management due to the opportunity of providing secure and consensual agent interaction with help of common communication channel presence. For the correct and effective functioning of the robotic group there is a necessity in providing security of information transfer via communication channels. In the article the mechanisms of "hard" and "soft" security in robotic systems are described. The emphasis is put on providing pragmatic information integrity, and to avoid violation occurrence in this integrity category the method based on credit theory was developed. The method implies regulation of information volume transferred by agents through establishment of fixed amount for information conventional units per time unit (installment plan). In case of data retention by agent subsequently its payment value is reduced, thus, its indebtedness is increased. In the end of installment plan period agent's level of trust and reputation is calculated. During introduction into the group of a new agent the credit is determined, due to which the new agent gets from other group members not full information but information reduced by the established interest rate. However, this agent must transmit data in accordance with predetermined installment plan conditions. In the end of credit period the decision whether the new agent is accepted or blocked is made. To assess effectiveness of the proposed method the interaction in robotic group consisted of ten agents was modeled. Two new agents were introduced into the group, and one of them was a saboteur. The threshold value of indebtedness for being accepted to the group is the half of established credit size. Series of independent tests were conducted, in the 90,2 % of them the saboteur was blocked.*

Keywords*—*decentralized collective management, multi-agent system, unmanned aerial vehicle, credit theory, pragmatic integrity, information security

I. INTRODUCTION

In the recent time multi-agent systems obtained a widespread recognition due to their resilience in comparison with centralized implementations. Such systems provide users with stronger fault tolerance, higher interaction speed and agent relative self-independence. There is a significant amount of ideas and already existing projects dedicated to ways of multi-agent system implementation in the society life. In the work [1] the contribution of multi-agent approach providing intelligence in the distributed smart grids is discussed. The multi-agent prototype was proposed for production control in water fabs [2]. Relatively to recent projects the demand side management strategy was offered for optimal energy distribution in smart houses [3]. In addition, self-organized multi-agent system consisted of various agent types and provided with possibility of feedback and coordination was suggested for smart factories [4]. In this article multi-agent systems are considered in the context of closed and open space monitoring by group of unmanned aerial vehicles (UAV). The term "monitoring" is considered in this work as regular examination for nonstandard changes.

The classification of group management strategies is presented in the Fig. 1:

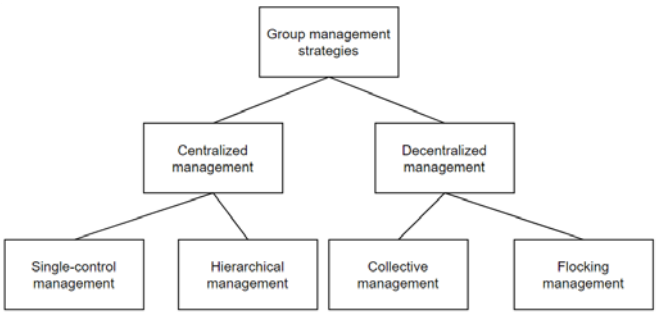

Fig. 1. *Classification of group management strategies.*

Group management strategies can be divided into two types: centralized and decentralized. In its turn centralized management can be single-control and hierarchical. In case of centralized single-control management group has central control unit (commander), which plans and inspects actions of all the group members (agents). Centralized hierarchical management obeys the concept that one commander controls the determined group, whose members, in their turn, control their own subgroups.

The advantage of centralized management is its realization simplicity. However, implementation of centralized management is accompanied with a risk of system crashing due to weak fault tolerance: to destroy the functionality of all the system or its significant part it is enough to impact negatively only on the central unit. Furthermore, the central node is responsible for solving complicated optimization tasks relatively to each member

of group or subgroup, which provokes a long-time decision-making. All the mentioned shortcomings are taken into account in the groups with decentralized management strategy. The lack of central unit minimizes time costs for decision-making, and crash of one or several participants will not impact significantly on group productivity.

Decentralized management strategy is divided into two types: collective and flocking. In case of collective decentralized management group agents have a common channel for information exchange. In flocking groups members do not have communication channel and make decisions based on indirect information about environmental changes caused by actions of other agents.

The preference is given to collective management strategy, as presence of common channel provides communication between UAVs in order to find the optimal algorithm for achieving the stated group purposes. The structure of collective management consists in the following: in the group of n members each agent R_i $(i \in [1; n])$ possesses its own management system C_i, which is responsible for actions of this particular agent. These systems are united by common communication channel. Information about actions, chosen by C_i is transmitted to other C_j, $(j \in [1; n], i \neq j)$, and based on obtained data the agents optimize their performance [5]. The strategy of collective decentralized management is depicted in the Fig. 2:

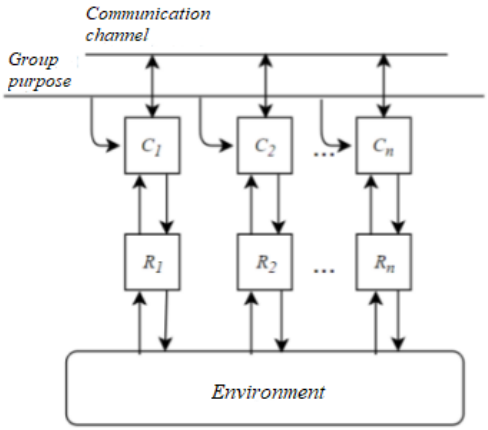

Fig. 2. *Collective group management strategy.*

UAVs give a possibility to cover large territories in a short period of time by small group, and they have already been integrated in such processes as controlling sowing complexes, cartography [7], etc. Wide area of visibility, high speed of UAV make it possible to quickly monitor, predict, prevent emergency situations and prospectively to avoid or reduce fatal consequences and significant material and human losses. In the work [8] use of UAV group for forest restoration was described. In such relevant circumstances it is vital to guarantee correct and effective group functioning. Firstly, it is necessary to provide security of information transmitted through the group common communication channel.

II. Related Work and Theoretical Background

In this article the emphasis is made on providing information integrity of the data transmitted. The message semiotic model has three basic constituents: syntax (rules of encoding, decoding, interpretation), semantics (message content), pragmatics (message usefulness, knowledge) [9]. From these instances it is possible to conclude that syntactic integrity – property of the information presentation form, semantic integrity – property of message content characteristics, pragmatic integrity – property of information utility in the context of environment and own recipient state.

The mechanisms providing information security in multi-agent robotic systems are divided into two fundamental types: mechanisms providing hard security and soft security [10]. Communication channel encryption with public key, use of mobile cryptography, agent authorization can be referenced to the first mechanism type. A demonstrative example of soft security mechanisms is trust and reputation model for objects [11]. However, one of the vulnerabilities of this model is situation, when saboteurs make up half or majority of the group: in this case saboteurs can give each other high trust points discrediting other agents. The measurement of agent reputation during the whole interaction time was implemented as solution method.

The enumerated methods are oriented, basically, to the semantic integrity preservation – content constituent [12] [13]. It should be considered that in order not to undermine their trust level saboteurs can transmit correct data but not in a full size. Due to such actions the group does not possess enough information for task performing. In this case pragmatic integrity violation happens [6]. In this work the most attention is paid to pragmatic information integrity, which is category consisted in reliability and completeness of data that serves as basis for information message.

III. Research Task Statement

There is a group consisted of N UAVs: $R = \{r_1, r_2, \ldots, r_N\}$. Each agent possesses the aggregate of M properties: $S_i = \{r_i \mid s^i_j, j \in [1; M]\}$, $i \in [1; N]$. As an assumption, UAV homogeneity is considered: $\forall r_i, r_j \in R, i \neq j, i, j \in [1; N]$: $S_i = S_j$. It is supposed that hard security mechanisms are realized and perform correctly.

Agents interact with each other during the period T. The given group functions in the territory F, which consists of f equal sectors. The UAVs check these determined regions during equal intervals (discretes) of time. At the end of check process the agents exchange with the collected data. Information I_i, which is possessed by each i^{th} UAV at the expiration of discrete $[t_{k-1}; t_k] \in T$, before the data exchange process, is divided into own and acquired. Own information is data about agent's own technical state at the current moment and technical state of the whole group for the previous time discrete. Acquired information is information collected by ith agent about environment for the period $[t_{k-1}; t_k] \in T$. This relation is represented in (1)-(3):

$$I_{own_i} = I_{cts_{[t_{k-1};t_k]_i}} \cup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}} \right), \quad (1)$$

where I_{own_i} *is* i^{th} agent's own information, $I_{cts_{[t_{k-1};t_k]_i}}$ – i^{th} agent's information about its technical state for the current moment, $I_{cts_{[t_{k-2};t_{k-1}]_j}}$ – j^{th} agent's information about its technical state for the previous time discrete.

$$I_{acquired_i} = I_{es_{[t_{k-1};t_k]_i}}, \quad (2)$$

where $I_{acquired_i}$ *is* i^{th} agent's own information, $I_{es_{[t_{k-1};t_k]_i}}$ – i^{th} agent's data about current environment state.

$$I_i = I_{own_i} \bigcup I_{acquired_i}, \quad (3)$$

After the group data exchange each agent has in the acquired information composition data about the current technical state of other group members and information about environment state collected by the rest of the group. Data structure possessed by agents after the information exchange with area check results for the period $[t_{k-1}; t_k] \in T$ is illustrated by (4)-(6):

$$I_{own_i} = I_{cts_{[t_{k-1};t_k]}} \bigcup \left(\bigcup_{j=1}^{N} I_{cts_{[t_{k-2};t_{k-1}]_j}} \right) \quad (4)$$

$$I_{acquired_i} = I_{es_{[t_{k-1};t_k]_i}} \bigcup \left(\bigcup_{j=1}^{N, i \neq j} \left(I_{es_{[t_{k-1};t_k]_j}} \bigcup I_{cts_{[t_{k-1};t_k]_j}} \right) \right) \quad (5)$$

$$I_i = I_{own_i} \bigcup I_{acquired_i} \quad (6)$$

Thus, information obtained by joinder of data transmitted by all the agents, has to tend to the ability of full group and environment state reflection. This statement is expressed in (7) and (8):

$$I = \bigcup_{i \in [1;N]} I_i \quad (7)$$

$$I \to U, \quad (8)$$

where U is full information about group and environment for the current moment.

The scheme of UAV information possession during a single time discrete is represented in the Fig. 3.

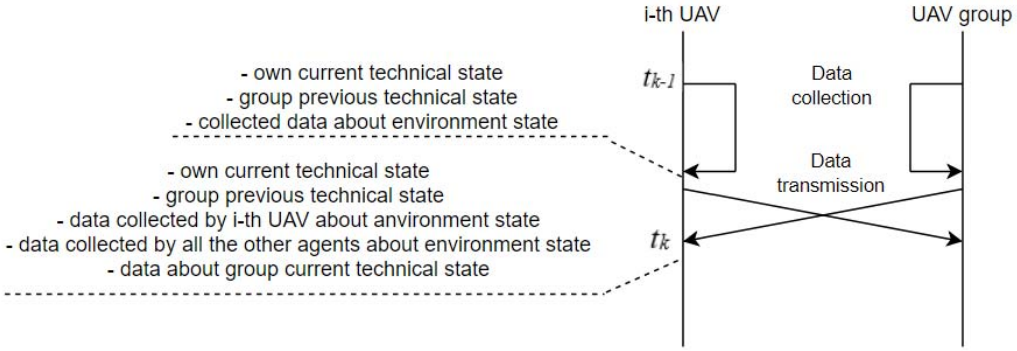

Fig. 3. *Group information interaction scheme in the single time discrete relatively to the* i^{th} *agent in assumption of destructive information influence absence.*

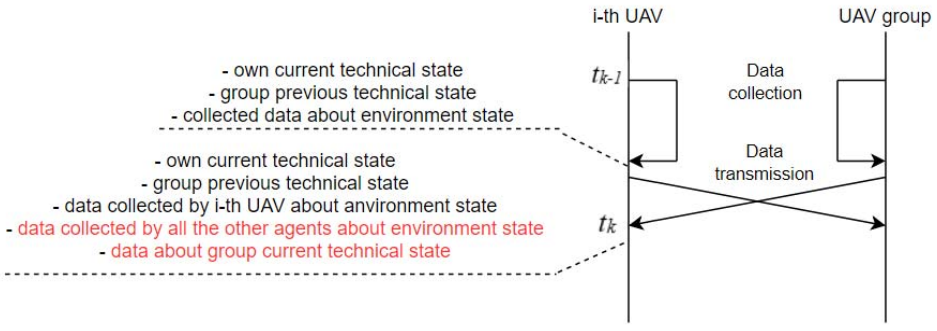

Fig. 4. *Group information interaction scheme in the single time discrete relatively to the* i^{th} *correct agent in assumption of destructive information influence presence*

However, saboteurs pursuing the purpose of work sabotage can be present in the group. In order not to deteriorate its own reputation with spurious data transmission, the saboteur can retain information while getting information from other agents in full. In such way the saboteur hinders from making a complete view about group and environment and can slow down work productivity of all the group. The saboteurs can retain information from other agents about:

a) their own technical state on case of insignificant malfunctions;

b) environment state;

c) both their own technical state and environment state.

Situations (a) and (b) at the end moment of the group data exchange for the discrete $[t_{k-1}; t_k]$ are represented by (9) and (10), respectively:

$$I_{cts_d} \in \tilde{I}_{acquired_i} < I_{cts_i} \in I_{acquired_d}, \quad (9)$$

where I_{cts_d} is information about saboteur's current technical state, $d \in [1; N]$; I_{cts_i} – information about current technical state of the i^{th} correct agent, $i \neq d$; $\tilde{I}_{acquired_i}$ – acquired information of the i^{th} correct agent in case of saboteurs' destructive information influence.

$$I_{es_{[t_{k-1};t_k]_d}} \in \tilde{I}_{acquired_i} < I_{es_{[t_{k-1};t_k]_i}} \in I_{acquired_d}, \quad (10)$$

where $I_{es_{[t_{k-1};t_k]_d}}$ is information about current environment state transmitted by saboteur, $d \in [1; N]$; $I_{es_{[t_{k-1};t_k]_i}}$ – data about current environment state transmitted by i^{th} correct agent, $i \neq d$.

The situation (c) is resumptive for cases enumerated before, and it is illustrated by (11):

$$\tilde{I}_{acquired_i} < I_{acquired_d}, i \neq d, \quad (11)$$

Thus, saboteur impact on other agents' formation of $I_{acquired}$. This is reflected by (12):

$$\tilde{I}_{acquired_i} < I_d \setminus I_{own_d}, i \neq d, \quad (12)$$

The Fig. 4 depicts situations with information retain respectively to the correct UAV in a single time interval, where data pieces marked in red color are at risk of being reduced by saboteurs.

The research task consists in searching of effective methods allowing to minimize the risk of destructive information influence on the group from the saboteur side and in providing pragmatic integrity preservation of transmitted information: $\forall i \in [1; N]$ $\tilde{I}_{acquired_i} = I_{acquired_d} + \varepsilon, \varepsilon \to 0, I \to U$.

IV. Pragmatic Integrity Preservation of Transmitted Information Based on Credit Theory

To prevent information retention by agents it is proposed to integrate into the trust and reputation model a method based on credit theory. The term "credit" is understood as level of trust, which creditor expresses relatively to debtor [14] [15], and this term suitable for soft security mechanisms. Capital credit theory [16] [17] affirms that crediting process contributes to the increase of population wealth level. In the context of information security credit leads to the security raise of data transmitted within the group.

A debtor is given with a credit of D for the period PP (full credit term) with the annual interest rate p. At the end of the term debtor with considering of interest rate must pay the sum equal to θ. During the full credit term after each time discrete U debtor must make fixed annuity payment A, which consists of credit body and credit interest. Proportions of these two categories can be modified preserving fixed payment size. The calculation of annuity payment size is performed according to (13):

$$A = K \cdot D, \quad (13)$$

where K is annuity coefficient.

Annuity coefficient is represented in (14):

$$K = \frac{h \cdot (1+h)^U}{(1+h)^U - 1}, \quad (14)$$

where $h = p / 12$ – monthly interest rate.

In this way, credit payout results can be expressed by (15):

$$\sum_{u=1}^{U} A_u = \theta \quad (15)$$

In the context of UAV group interaction it is suggested introducing terms:

a) installment plan;

b) credit.

a) Interaction time T is divided into U installment plan intervals of the determined length. For the installment plan interval $[t_{u-1}; t_u] \in T$ each agent has to transmit fixed information amount I. In its turn, interaction period $[t_{u-1}; t_u]$ is split into V equal time intervals, at the end of which all the agents must transmit information amount equal to I / V, as it is represented in (16):

$$\sum_{v=1}^{V} payment_v^u = I, U \in T, \quad (16)$$

where *payment* is information amount made by agent in a single installment plan interval.

In case if the UAV retains any information, it violates fixed payment, and a fine is imposed as a sanction, which reduces the value of this agent's future payments. Thus, the agent has indebtednesses. As installment plan period is over, debts of each agent are calculated, and agents with larger debt will have lower trust index and consequently – reputation index. Payment check is performed in the group by regularly randomly reelected responsible agent. Trust and reputation level of the agent in the group are represented with the dependencies (17) and (18), respectively:

$$TRUST_i = f\left(\sum_{v=1}^{V} payment_v^{u\,+}\right), U \in T, \quad (17)$$

$$REPUTATION_i = f\left(\sum_{u=1}^{U}\sum_{v=1}^{V} payment_v^{u\,+}\right), U \in T, \quad (18)$$

b) In case of integration of a new UAV at the moment t_0 it is necessary to perform its crediting relatively to transmitted information amount. Crediting process consists in the following steps:

- planning of interaction *T* for the new UAV and the group;
- calculation of full credit term: $t < PP < T$, where *t* is durability of installment plan period;
- setting of initial size of the interest rate *p*;
- calculation of installment plan size *payment* for the period *PP*.

During the term *PP* the integrated UAV must transmit fixed information amount, which is declared in the group by the installment plan conditions. However, this new agent gets from other UAVs information about group and environment minus the given interest rate, i.e. during credit term for the time discrete $[t_{k-1}; t_k]$ after data exchange with other agents the j^{th} integrated agent's acquired information is expressed by (19):

$$I_{acquired_j} = I_{es_{[t_{k-1};t_k]_j}} \cup (1-p)\cdot\left(\bigcup_{i=1}^{N, i\neq j}\left(I_{es_{[t_{k-1};t_k]_i}} \cup I_{cts_{[t_{k-1};t_k]_i}}\right)\right), \quad (19)$$

During interaction process the interest rate is reduced by a certain value, at the end of the full credit term the interest rate reaches zero. As the full credit term is finished, the checked UAV becomes a full member of the group, updates installment plan conditions, gets full information from other UAVs during monitoring and has a right to be elected as a responsible agent for payment checking.

The check of integrated agents is fulfilled by the enumerated procedures:

1) comparison of the stated credit size $payment_{must}$ and factual $payment_{got}$ at the end of *PP*;

2) comparison of information amount $payment_{must_{u[t_{v-1};t_v]}}$, which have to be transmitted in a single time discrete within the framework of installment plan period, and factual $payment_{got_{u[t_{v-1};t_v]}}$, $u \in [1; U]$, $[t_{v-1}; t_v] \in [t_{u-1}; t_u]$.

3) calculation of discrepancies of $payment_{must_{u[t_{v-1};t_v]}}$ and $payment_{got_{u[t_{v-1};t_v]}}$ at the end of *PP*.

The decision about blocking or accepting of the new UAV is made by the responsible agent.

Temporal crediting process scheme is represented in the Fig. 5.

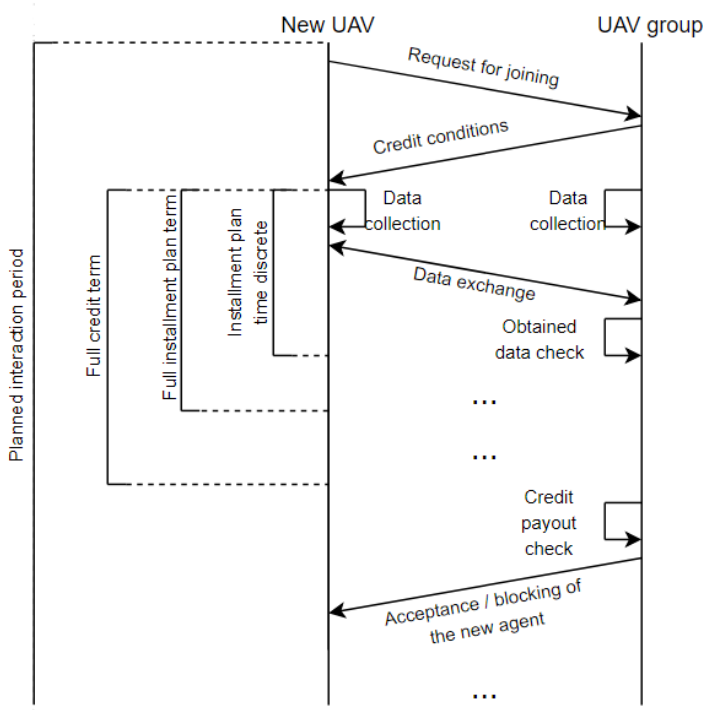

Fig. 5. *Temporal crediting process schem*

The proposed method of pragmatic integrity preservation minimizes risk of destructive information influence on the group. It is not profitable for saboteurs to be integrated into the group with high interest rate, long credit term and short installment plan period: big amount of checks does not give a possibility to retain much information, and costs (energetic, temporal, informational) during the credit exceed incomes, which can be acquired after credit repayment. The example of the described situation is depicted by Fig. 6 and (20):

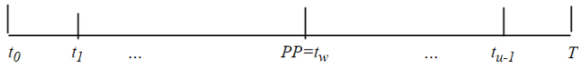

Fig. 6. *Temporal interaction scale of group and integrated UAV.*

$$I^{sent}_{[t_0;PP]} > I^{got}_{[PP;t_{w+1}]}, w \in [1;U-1], \qquad (20)$$

where $I^{sent}_{[t_0;PP]}$ is information transmitted by the new UAV for the credit period, $I^{got}_{[PP;t_{w+1}]}$ – information received in the next installment plan discrete right after credit period is over.

V. Experiment

The proposed method of pragmatic information integrity preservation was tested on a specially programmed simulator for effectiveness in the context of risk minimization of destructive information influence on pragmatic information constituent.

Initial parameters and work sequence of the experiment:

- group consisted of 10 UAVs;
- territory consisted of 10 equal sectors and monitored by the group;
- 1 conditional time unit, during which the group examines 1 sector;
- Integration of 2 new UAVs: one of them is saboteur;
- full credit term is ten conditional time units;
- initial interest is 50 %, at the end of each installment plan period the given interest rate is reduced by 10 %;
- the marginal indebtedness size, with which a new agent can become a full group member is half from the stated credit sum;
- saboteurs depending on situations can either transmit the information in full or retain a part of it;
- correct UAVs can retain information due to technical malfunctions, malfunction emergence probability is considered equal to 10 %.

Series of independent tests was conducted. Debt size distribution of saboteur and correct UAV is represented in Fig. 7 and Fig. 8, respectively:

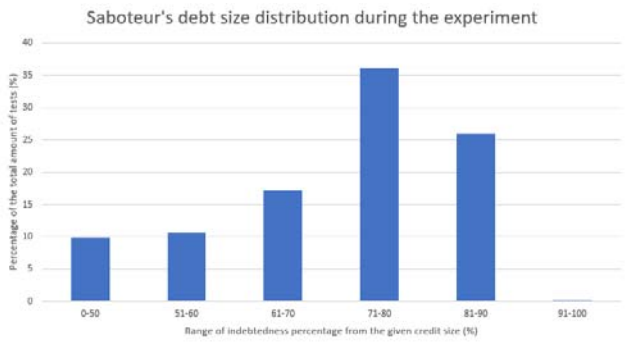

Fig. 7. *Histogram of saboteur's indebtedness size during the experiment.*

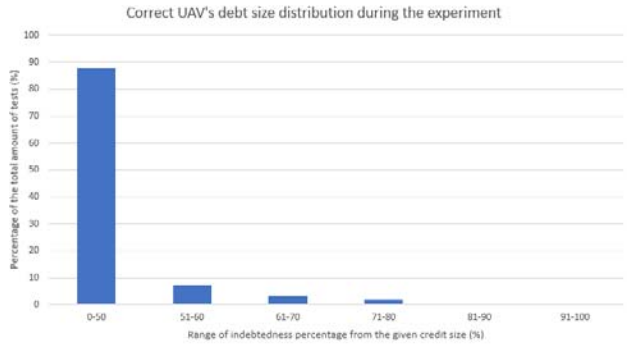

Fig. 8. *Histogram of correct UAV's indebtedness size during the experiment.*

VI. Conclusion

The stated research task was performed. By dint of the method based on theory credit it becomes possible to minimize destructive information influence of UAVs-saboteurs on the group and provide preservation of pragmatic integrity in transmitted data.

Information crediting makes unprofitable group work sabotage, as it significantly slows down the sabotage process and requires large costs from the saboteur side. Prospectively it is planned to implement the proposed method in a real UAV group, and consequently to develop UAV monitoring system providing transmitted data security.

References

[1] *M. Pipattanasomporn, H. Feroze. and S. Rahman, "Multi-agent systems in a distributed smart grid: Design and implementation," 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, 2009, pp. 1-8.*

[2] *L. Mönch, M. Stehli, J. Zimmermann, and I. Habenicht, "The FABMAS multi-agent-system prototype for production control of water fabs: design, implementation and performance assessment," in Production Planning & Control, vol. 17, pp. 701-716, 2006.*

[3] *W. Li, T. Logenthiran, W. L. Woo, V. Phan and D. Srinivasan, "Implementation of demand side management of a smart home using multi-agent system," 2016 IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, 2016, pp. 2028-2035.*

[4] *S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, "Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination," in Computer Networks, vol. 101, pp. 158-168, June 2016.*

[5] *I. Kaliaev, A. Gaiduk, and S.G. Kapustyan, "Models and Algorithms of Collective Management in Groups of Robots," Fizmatlit, 2009.*

[6] *I. Komarov, A. Drannik, and R. Yurieva, "Multiagent information security problem's simulation," In the World of Scientific Discoveries, vol. 52, pp. 61-71, 2014.*

[7] *V. Zhuravlev, and P. Zhuravlev, "UAV implementation in economic spheres: state and prospects," in Civil Aviation High TECHNOLOGIES, vol. 226, pp. 156-164, April 2016.*

[8] *S. Denisov, A. Domrachev, and A. Elsukov, "Experience of application of quadrocopter for monitoring of restoration of forests," in Vestnik of Volga State University of Technology. Series: Forest. Ecology. Nature Management, vol. 4, pp. 34-45, 2016.*

[9] *I. Tsvetkov, "Semantics of messages in telecommunicationsystems," Russian competitive selection of review-analytical articles on the priority area "Information and Telecommunication Systems"*, 2008.

[10] *I. Zikratov, T. Zikratova, I. Lebedev, and A. Gurtov, "Trust and reputation model design for objects of multi-agent robotics systems with decentralized control," in Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 91, pp. 30-38, 2014.*

[11] *A. Beshta, and M. Kirpo, "Building a model of trust in the objects of an automated information system to prevent destructive impacts on systems" in Bulletin of the Tomsk Polytechnic University, vol. 5, pp. 104-108, 2013.*

[12] *I. Jovanov, and M. Pajic, "Sporadic data integrity for secure state estimation," 2017 IEEE 56th Annual Conference on Decision and Control (CDC), 2017. pp. 163-169.*

[13] *P. Santra, A. Roy, and K. Majumder, "Comparative Analysis of Cloud Forensic Techniques in IaaS," in Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol. 554, pp. 207-215, September 2017.*

[14] *O. Lavrushin, "The theory of the credit basis and its use in modern economy," in Journal of economic regulation, vol. 8, pp. 6-15, 2017.*

[15] *A. Evtukh. "The theory of credit: the socio-economic aspect," in Finance and credit, vol. 25, pp. 21-27, 2006.*

[16] *L. Gurnakova, "Essence, theoretical foundations of the credit market concept," in Problems of modern economics, vol. 2, pp. 83-85, 2011.*

[17] *T. Kosterina, and T. Panova, "Methodological foundations for the analysis of credit borders," in Finance and credit, vol. 32, pp. 26-38, 2015.*