A Panacea to Soft Computing Approach for Sinkhole Attack Classification in a Wireless Sensor Networks Environment

Kenneth E. Nwankwo[1], Shafi'i Mohammad Abdulhamid[2], Joseph A. Ojeniyi[3], Sanjay Misra[2(✉)], Jonathan Oluranti[2], and Ravin Ahuja[3]

[1] Federal University of Technology Minna, Minna, Nigeria
[2] Covenant University, Ota, Nigeria
shafii.abdulhamid@futminna.edu.ng, {Sanjay.misra, jonathan.oluranti}@covenantuniversity.edu.ng
[3] Shri Vishwakarma Skill University, Gurgaon, India
ojeniyija@futminna.edu.ng

Abstract. Small sensor nodes with the capability to sense and process data make up a wireless sensor network (WSN). This environment has limitations of low energy, low computational power and simple routing protocols; making is susceptible to attacks such as sinkhole attack. This attack happens when the enemy node in the network camouflages as a genuine node nearest to the base station, thereby have information sent by a source node to another destination node travel through it, giving it chance to alter, drop or delay information from reaching to the base station as intended. In our paper, the research developed a sinkhole detection technique, an enhancement of ant colony optimization by including a hash table in the ant colony optimization technique to advance sinkhole attack detection and reduce fa1se alarm rate in a wireless sensor network. An increase in the detection rate of 96% was achieved and result out performed other related research works when compared and further research discussed.

Keywords: Ant colony optimization · Swarm intelligence · Sinkhole detection · Wireless sensor network

1 Introduction

Wireless sensor network (WSN) contains a varied size of arranged interconnected nodes that forms cells for information dissemination (transceiver). WSN is a profoundly used system with application in numerous territories such as social insurance tracking, territory checking world and it environ sensing its observation likewise. Information received via sensors are managed by the cells. WSN utilization within a domain can either be genuine or rather without assurance [1]. The idea behind WSNs can be said to amount to its defenceless nature against numerous security dangers of various sorts and reason. With the straight forward idea of their directing strategies, security serves as the best test as they are increasingly defenceless to different system threat or exploits, of which

P. K. Singh et al. (Eds.): FTNCT 2020, CCIS 1395, pp. 78–87, 2021.
https://doi.org/10.1007/978-981-16-1480-4_7

can lead to sinkhole exploit in a corporation, priority forwarding, wormhole exploits, hello-distributed attack, Sybil-attack, node replication exploit, as well as black hole [2]. Sinkhole attack is considerable as it can prompt each other attack referenced previously. Figure 1 shows a run of the mill WSN system and all it contains.

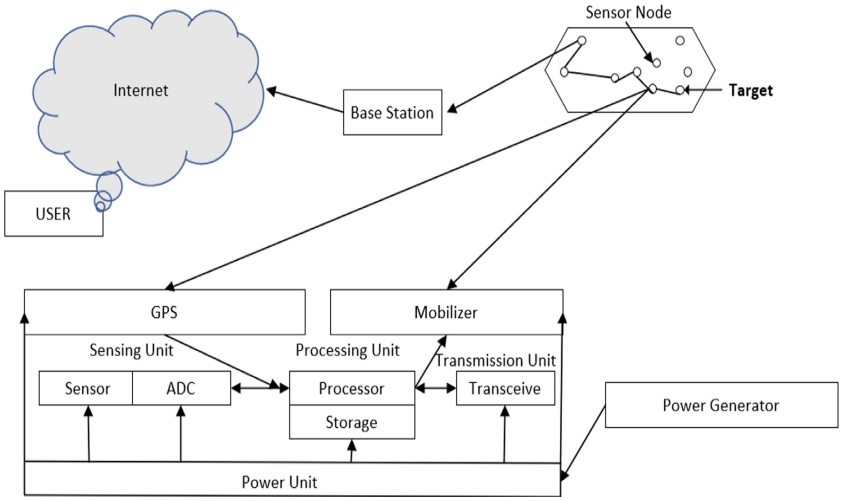

Fig. 1. Node sensor architecture

The military, as well as restorative exploration, are known commonly to utilize the functionality of sensor networks for the evaluation purpose, inclusive are threat tracing, conflict spots-review, as well as trespasser, acknowledge, WSN regularly explores threatening as well as the remote destination. Along these lines, there is a firm prerequisite for guaranteeing the distinguishing of data and recognizing readings. In detached circumstances, an interloper not only can tune in the correspondence, yet besides, the gatecrasher can get or meddle with the exchanged messages. Along these lines, various estimations, and shows don't work in hostile conditions without adequate wellbeing estimates set up. Thusly, security winds up as one of the most significant concerns while organizing security shows in resources constrained to work in WSNs. A piece of the employments of WSNs is for combat area observation, clinical administration applications, nature watching, keen home, and vehicular exceptionally designated frameworks VANETs.

An improved Ant Colony Optimization (ACO) proffered in this study through the incorporation of a hash table in the typical ACO order to improve detection rate (DR) as well as decrease false alert rate (FAR) in Sinkhole Attack Detection. The key contributions of this study are hereby highlighted or outlined:

- Design an "Enhanced Ant-Colony Optimization Tech (EACO)" used for sinkhole attack detection.
- Develop an EACO using DR and FAR.
- Evaluate the EACO comparatively with existing results in previous literature.

2 Related Works

For over a decade, research on prevention as well as forestalling Sinkhole Attack have been in steady peace, here is a brief review of some of the recent works. [1] presented a parameter evaluation used by ACS to get high values for throughput, best energy usage as well as a lag period which leads to an optimal process of packet routing was attained.

Authors [2] achieved optimal detection through a detection algorithm opined. This was made possible from the communications obtained by aggregation algorithm data for discovering the exploit that emerges from Body Area Network (BAN) as a result of sinkhole attack. In [3] authors deploy an (ESPO) to modify flocking is associated with a collection of algorithms that functions with cohesion, partitioning as well as alignment that exists in the collection of nodes within WSN deployed in a sizeable instance in order to forestall sinkhole attacker.

Authors [4] applied an enhanced ACS algorithm motivated from an alternate of ACO the remote as well as local update enhancements for discovery as well as exploitation improvement path with effective packet loss depletion while improving the efficiency of sensor edge energy. Authors in [5] employ COOJA as a simulator, with consideration of ACO-pheromone vanishing mechanism and ACO critical protection allocation for the effective balancing of edge interactions as well as speed management. Furthermore, in order to mislead an intruder, enhanced (KMT) method with Ant Colony optimization was explored to state a route in other to achieve safe as well as improve packet transmission ingress the nodes and egressing the cell and vice versa.

Authors [6] presented an enhanced ACO algorithm solving the challenges associated with traffic drop experienced when nodes communication traffic is in excess of its capacity. The research evaluation help in juxtaposing EACS with Cost Aware Ant Routing (SC) algorithm potentials as well as the strength of Efficient Ant Based Routing (EEABR) algorithm of which the presented model was planned for implementation in a WSN that is static.

There are several other works available in the literature on ant colony optimization problem [12–15]. We have not considered them for detailed explanation due to several reasons, including not much related and space issue due to conference paper.

2.1 Findings from Literature

Literature has revealed that different methodology such as the cryptographic, swarm intelligence [7] and machine learning [8] have been employed to address detection of sinkhole attack.

Minimal tradeoff is experienced in swarm intelligence as against all other methods as reviewed in the literature, based on the fact the WSN still remain fragile field that requires lots of attention in terms of energy utilization management, overhead computation management as well as package monitoring. The outperformance of ACO, swarm intelligence algorithm against others of such family algorithm in addressing challenges in various fields like the Travel Salesman Problem (TSP) have proved its prospect for success in its application. Furthermore, the reviewed literature points out gaps such as the need for novel technique, enhancement of existing techniques and addressing false

alarm rate reduction in quest or an improved detection rate as well as reduced FAR in WSN.

3 Research Methodology

This study is composed of two major phases, formulation of the problem, planning as well as design. The implementation was achieved through simulation in NS-3.30.1.

An attacker edge was introduced into the network in order to determine the havoc incurred. Furthermore, an evaluation was carried out based on performance. A flow chart of EACO is Fig. 2.

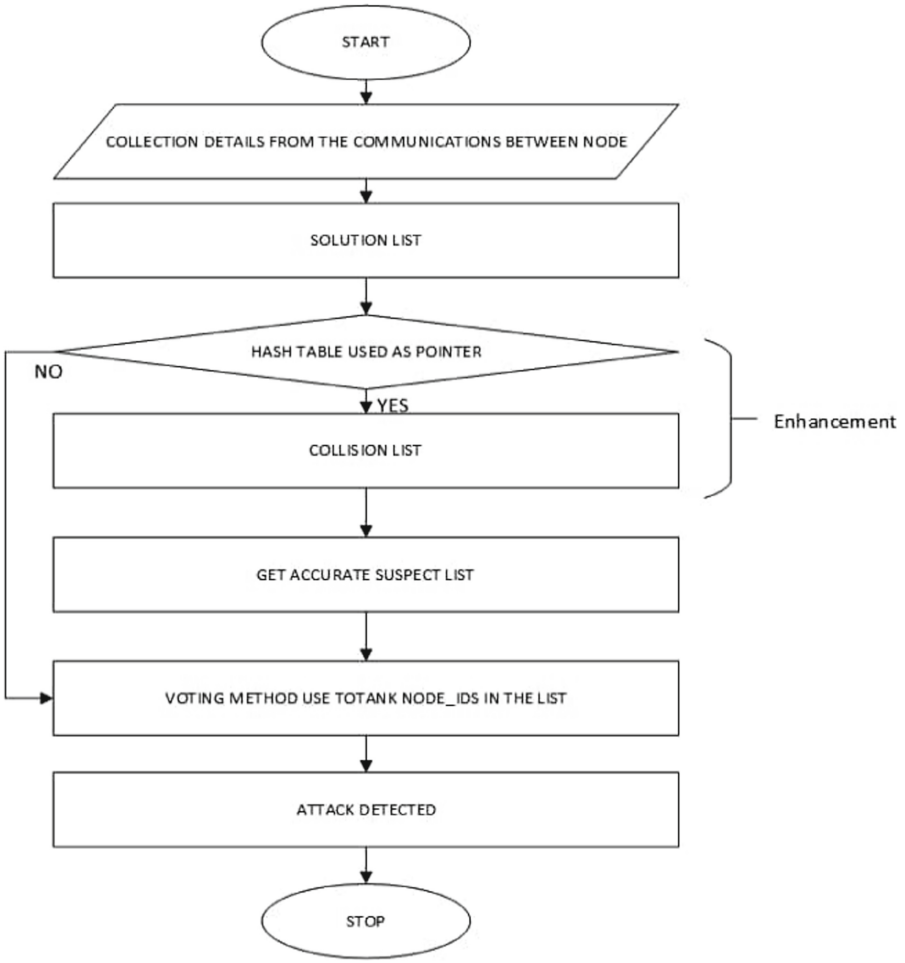

Fig. 2. Flowchart for EACO

A solution list is generated based on the interaction of nodes in a wireless sensor network serving as a pointer In the record is a hash collision is stored as collision list

which builds up as a suspect list circulated between communicating edge to track an attacker after signing and voting against the existing ACO with the functionality of transmitting solution list unto suspect list (Table 1).

Table 1. Pseudo code for EACO

```
Procedure code EACO ( )
{
Input n, α , β , ρ
set  the ant colony configuration
set the initial pheromone and heuristic value
get ant colony optimization system based on the calculated cost matrix
i = 1
while (I <= n)
{              r = 1
While ( r <= i)
{
Reset the ants
Build ant s' solution
Assume d(N)
// hash table implementation
if (h[d(N)]=0) { t=t+1 h[d(N)]=t and SL[t]= N //SL-Solution List
 return TRUE}
if (h[d(N)] ? 0 and SL[h[d(N)] ] = N) then return FALSE if h[d(N)] ? 0 and SL[h[d(N)]
] ? N { if N ? CL {cl = cl+1
//CL-Collision List
CL[cl] = N
return TRUE
}else return FALSE
initiate local search
Update path best for i
Update pheromones
r = r + 1
}
Choose  path best for i
i = i + 1
}
}
```

4 Results and Discussion

Table 2 depicts the various parameters used in simulation with 300 edges.

Table 2. Parameters of simulation

Parameter	Description
Platform	Mac OS Catalina
Deployment area	700×300 m^2
Network topology	tree
Network size	250 nodes
Attacker node numbers	50
Simulation total time	1900 s
Traffic type	CBR/UDP
Packet size	512 bytes
Packet transmission rate	25 Kbps
Routing protocol	AODV
Medium access control type	IEEE 802.11
Communication range of sensor node	25 m
Communication range of cluster head	50 m

4.1 Simulation

The simulation was based on a normal flow, sinkhole attackers and EACO technique as outlined in the described scenario of WSN:

- Normal flow scenario: comprising 300 edges sending to and from the base station as well as negligible latency in packet ratio and communication of end-to-end node.
- Sinkhole attack scenario: variation in parameter was tracked, in this scenario which comprise of 200 edges as well as 50 attacker edges.
- EACO Implementation scenario: parameter variation was noted under WSN attack based on the simulation. The following were computed; An end to end latency (in ns), detection rate (DR), Packet delivery ratio (PDR), through put (in kps) as well as FA/FPR.

Figure 3 depicts influence on end to end latency which defines the period of packet getting to the base station for a normal flow, at point a sinkhole is compromised and after the implementation of EACO given as 70.06 ms, 736.66 and 153.46 ms respectively.

- Figure 4 depicts influence of packet delivery ratio which defines ratio to packet value ingress base station and origination from a remote edge. The output of normal flow

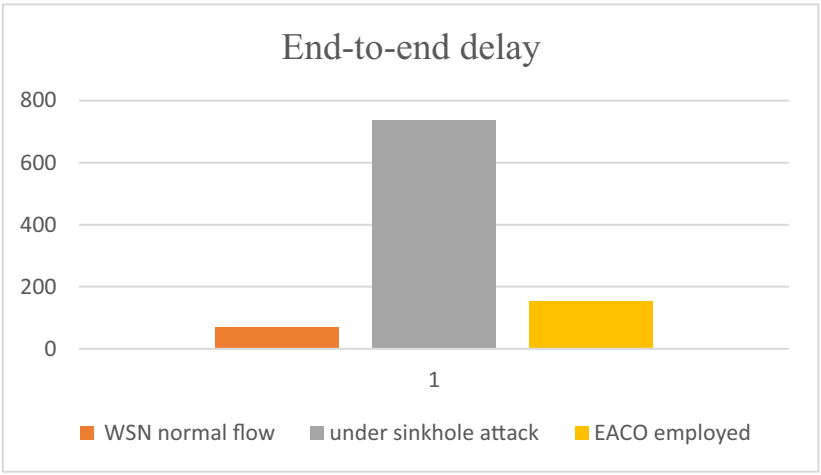

Fig. 3. End to end delay(latency) performance

WSN PDR ratio, sinkhole under attack and EACO implement method are 0.93, 0.46 and 0.9 respectively with a clearly notable performance in regards to PDR.

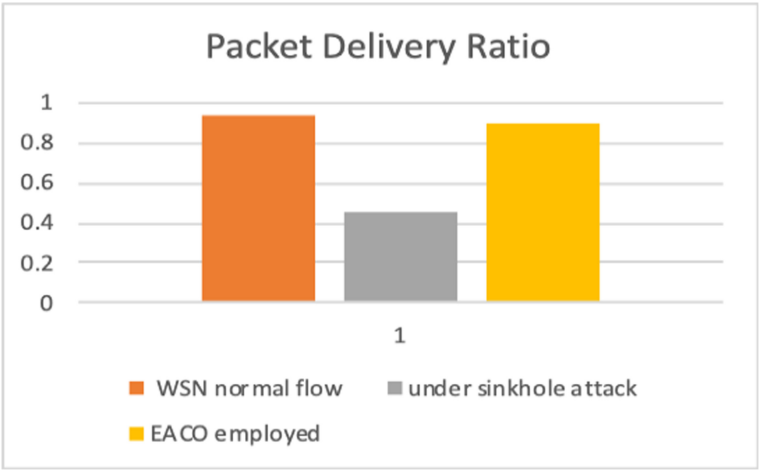

Fig. 4. Packet delivery performance

- Figure 5 depicts impact of throughput which defines transmitted bits value in unit time with a network expressed in (kps), the WSN normal flow, sinkhole under attack and EACO implementation results are 9.2 kps, 4.25 kps and 8.72 kps respectively with 94.32% improvement experienced under EACO.

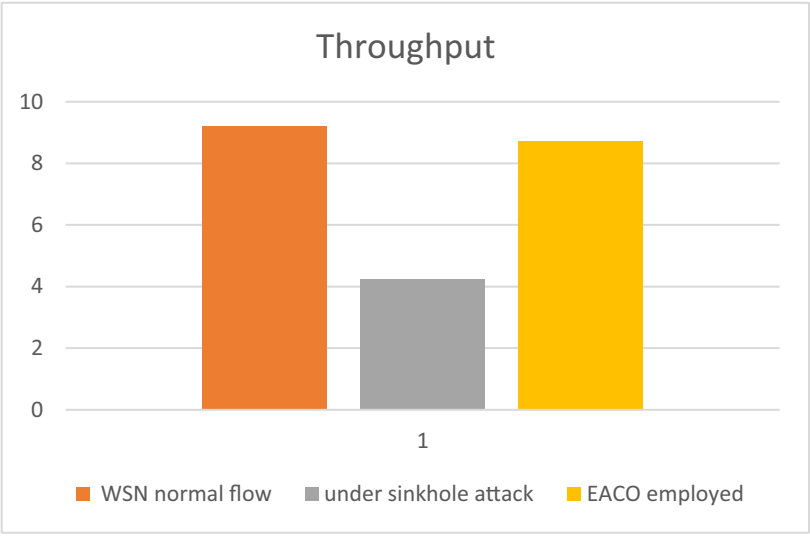

Fig. 5. Network performance

Furthermore, the simulation achieved the following: in our detection technique

I. 48 TP real attacks (attacker nodes) legitimate node (false positive) node of 2, legitimate nodes (True Negative) 198 and false negative (attacker mistaken as legitimate node) 2.
II. A total 200 legitimate node, 50 sinkhole attack node that was deployed in our study simulation achieved 96% and 1.0% respectively for DR and FPR

4.2 Performance Evaluation

A benchmark analysis in terms of performance comparison against some related literature was carried out as presented in Table 3 as well as Fig. 6 with an indication of distinct performance of our study against benchmark technique.

Table 3. Accuracy comparison

Authors	DR (%)	Fa1se alarm (%)
[10]	95	1.25
[11]	87.062	10.648
[9]	53	18
[2]	90	10
Our technique	96	1.0

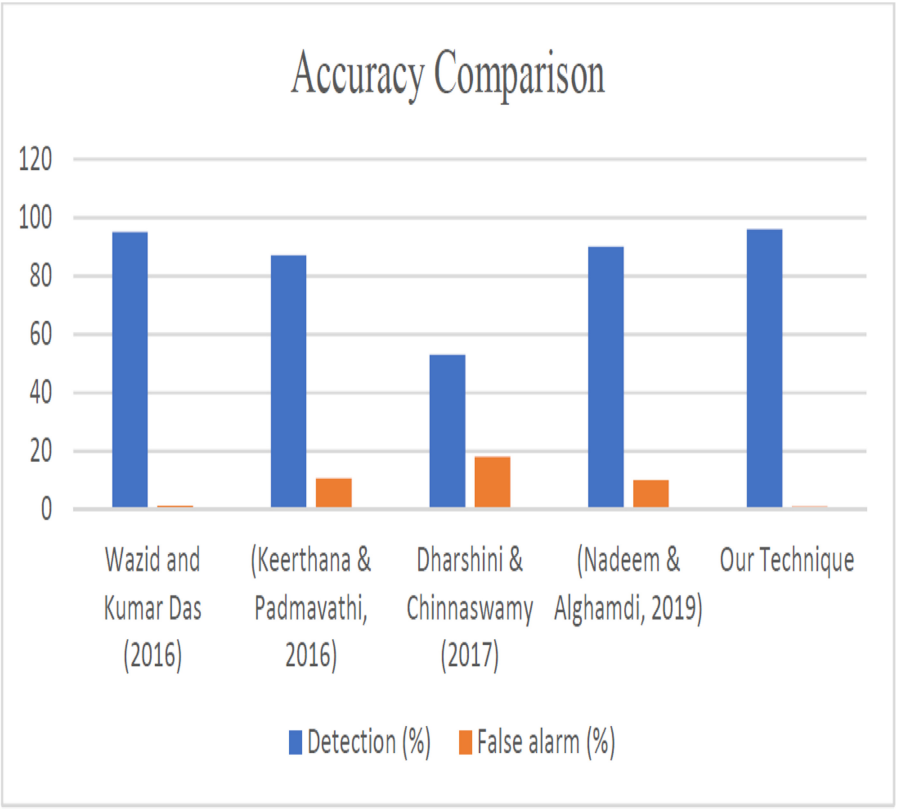

Fig. 6. Accuracy comparison

5 Conclusion and Future Work

A hash table was integrated into Ant Colony Optimization technique which serves as our design in enhancing performance in terms of time reduction in addressing an attacker alongside indexing which builds an accurate suspect list thereby addressing also false alarm associated with detection of the attacker. Secondly an optimal detection rate of 96% was achieved in our enhanced ant colony optimization method in regards to WSN. Furthermore, future research will look into security enhancement based on encryption of sensors as security protocols are given preference in WSN to aid addressing energy depletion, operational period lagging as well as detection enhancement.

References

1. Nasir, H.J.A., Ku-Mahamud, K.R., Kamioka, E.: Parameter adaptation for ant colony system in wireless sensor network. J. Inf. Commun. Technol. **18**(2), 167–182 (2019)
2. Nadeem, A., Alghamdi, T.G.: Detection algorithm for sinkhole attack in body area sensor networks using local information. IJ Netw. Secur. **21**(4), 670–679 (2019)

3. Nithiyanandam, N., Latha, P.: Artificial bee colony based sinkhole detection in wireless sensor networks. J. Ambient Intell. Humaniz. Comput. 0123456789 (2019)
4. Nasir, H.J.A., Ku-Mahamud, K.R., Kamioka, E.: Enhanced ant colony system for reducing packet loss in wireless sensor network. Int. J. Grid Distrib. Comput. **11**(1), 81–88 (2018)
5. Iwendi, C., Zhang, Z., Du, X.: ACO based key management routing mechanism for WSN security and data collection. In: Proceedings of IEEE International Conference on Industrial Technology, vol. 2018, pp. 1935–1939 (2018)
6. Abdul, N.H.J., Ku-Mahamud, K.R., Kamioka, E.: Enhanced ant-based routing for improving performance of wireless sensor network. Int. J. Commun. Netw. Inf. Secur. **9**(3), 386–392 (2017)
7. Kasliwal, B., Bhatia, S., Saini, S., Thaseen, I.S., Kumar, C.A.: A hybrid anomaly detection model using G-LDA. In: Souvenir 2014 IEEE International Advance Computing Conference, IACC 2014, pp. 288–293 (2014)
8. Sun, X., Yan, B., Zhang, X., Rong, C.: An integrated intrusion detection model of cluster-based wireless sensor network. PLoS ONE **10**(10), 1–6 (2015)
9. Dharshini, Y.N., Chinnaswamy, C.N.: Swarm Intelligence Technique for Sinkhole Attack Detection in Wireless Sensor Network - Performance Comparison of the Algorithms, no. 4, pp. 647–656 (2017)
10. Wazid, M., Das, A.K., Kumari, S., Khan, M.K.: Design of sinkhole node detection mechanism for hierarchical wireless sensor networks. Secur. Commun. Netw. **9**(17), 4596–4614 (2016)
11. Keerthana, G., Padmavathi, G.: Detecting sinkhole attack in wireless sensor network using enhanced particle swarm optimization technique. Int. J. Secur. Appl. **10**(3), 41–54 (2016)
12. Alfa, A., Misra, S., Ahmed, K., Arogundade, O., Ahuja, R.: Metaheuristic-based intelligent solutions searching algorithms of ant colony optimization and back. In: Singh, P.K., Pawłowski, W., Tanwar, S., Kumar, N., Rodrigues, J.J.P.C., Obaidat, M.S. (eds.) gation in Neural Networks. In *Proceedings of First International Conference on Computing, Communications,*. LNNS, vol. 121, pp. 95–106. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3369-3_8
13. Crawford, B., Soto, R., Johnson, F., Misra, S., Paredes, F., Olguín, E.: Software project scheduling using the hyper-cube ant colony optimization algorithm. Tech. Gaz. **22**(5), 1171–1178 (2015)
14. Adubi, S.A., Misra, S.: A comparative study on the ant colony optimization algorithms. In: 2014 11th International Conference on Electronics, Computer and Computation (ICECCO), pp. 1–4. IEEE, September 2014
15. Soto, R., et al.: Autonomous tuning for constraint programming via arti. In: Gervasi, O., et al. (eds.) ICCSA 2015. LNCS, vol. 9155, pp. 159–171. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21404-7_12