Monte Carlo Simulation Approach to Network Access Control

Patricia Yetunde Omole-Matthew, Gabriel Junior Arome,
Aderonke Favour-Berthy Thompson, Boniface Kayode Alese
Federal University of Technology
Akure, Nigeria

Abstract

Access is an important security platform that restrict access to only authorized entities thereby preventing unauthorized modification, alteration and removal of information. In network environment, there is need to protect the integrity of legitimate users, server providers and the connecting nodes. Thus, network access control secures an organization network such that sensitive data is protected from cyber threats. Network access control encrypts data traffic, control permissions and protects every endpoint on the network. It is therefore to secure the network with a structure that predetermine threats. Monte Carlo Simulation is a heuristic algorithm that predict perfect approach in an unknown circumstance to maximize the decision making of the tool. The simulation uses the state of requesting user's device as parameters for the Monte Carlo Simulation. The requesting user's device include model, registration, certification, access time, location among others. The simulation involves series of iterations that passes through four basic phases of selection, expansion, rollout and updating. Consequently, the decision to grant or deny access to user was achieved by obtaining result from the most rewarding node during iteration.

1. Introduction

The emergence of distributed computing and networking has prompted the necessity of controlling access to information to prevent cyber threats. Threats are impending risks that scan the vulnerability of computer systems and networks to inflict disruption to information [1]. A threat is event that infringe the security of an information by altering the availability, integrity and confidentiality of the computer environment.

Network security creates an environment in which a network environment is serviceable. Network security consists of connecting entities, software, networking hardware, internet services and resources [2]. Network security integrates access control, authentication, confidentiality, integrity, availability and non-repudiation to secure a network environment. Access control provides the identification of a user to define the user. Advance in computing has provided effective access tools [3]. Monte Carlo Simulation takes random samples and builds a search tree to the results [4]. It is statistical algorithm with more computing power for better performance. Monte Carlo Algorithm provides decision capacity with no domain knowledge by distinct selection of sample thereby building a sequential decision and learning from it [5].

2. Related Works

Access control mechanisms are widely used to secure the network resources from attacks such as denial of service, interference to private information among others. Access control verifies and authenticates requests using predefined control models. The control models serve as authorization rules hence Discretionary Access Control and Mandatory Access Control no longer meet the need of real-time access decision. Role Based Access Control introduces roles among the users. Due to the dynamic and stochastic features of users, researchers have proposed User's trust level as determinant of user's behaviour [6, 7, 8]. In [9] addressed a trust game based access control where direct trust, reward punishment and trust risk were proposed for trust evaluation and payoff matrix for analysis of equilibrium strategies of users and providers. Game theory was exploited [10] to realize a robust decentralized trust management to tolerate malicious nodes sending deceitful data. The work is motivated by the need to develop an efficient automated network access control with distinct visibility of all connected users.

3. The Monte Carlo Network Access Control Simulation

The network access control environment consists of several components such as packet, hub, switch, router, IP Address, server, user among others. Figure 1 depicts a typical network access control environment.

3.1. Monte Carlo Simulation Model

The Monte Carlo Simulation as described in Figure 2 aimed at modelling access control between a user and a provider. The user consists of players $P_r = \{benign, malicious\}$ and the

 | DOI: 10.20533/jitst.2046.3723.2021.0088

provider $P_p = \{server\}$. The strategies of the user $\sigma_r = \{forward\ packet, damage\ packet\}$ and the provider's strategies are described as $\sigma_p = \{grant\ packet,\ deny\ packet\}$.

A malicious user will play a strategy that will maximize his chances of accessing the provider's server likewise the provider choice of strategy will protect the server from vulnerability.

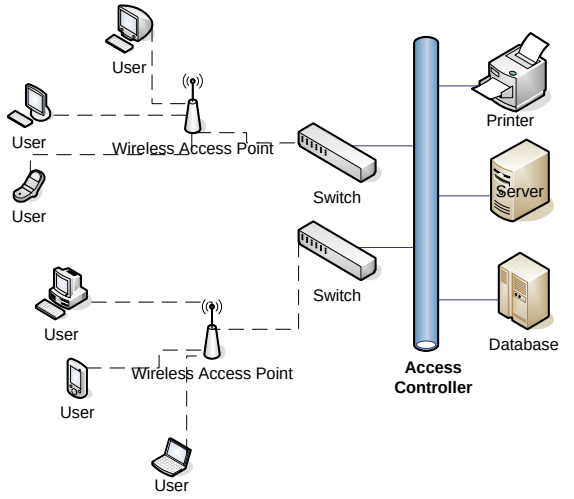

Figure 1. A typical cyber access control environment

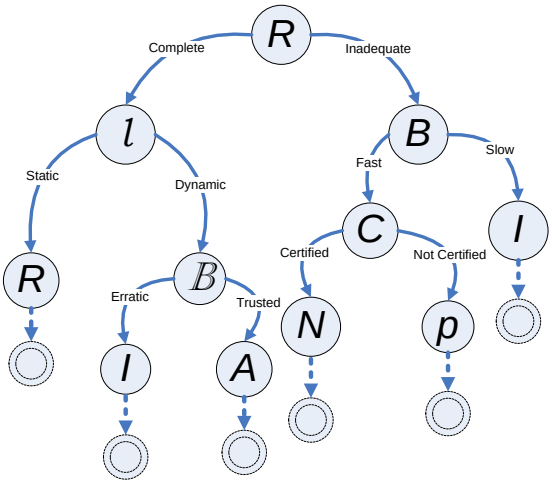

Figure 2. Sample Monte Carlo simulation

The Monte Carlo simulation expanded the sequential entities, every sampling was processed as the selected most useful entity for reward and moves were chosen randomly. At the decision point, the upper confidence bound determined the balance between the exploitation and exploration of the entities. The simulation progressed through entities with high values as described in equation 1,

$$UCB = \frac{u_i}{n_i} + c\sqrt{\frac{\ln t}{n_i}} \quad (1)$$

where

u_i is the cumulative utility after i moves

n_i is the number of simulation performed after i moves

c is the exploration parameter

t is the number of simulation in a given node $t = \sum_i n_i$

The Monte Carlo Simulation entities consist of the followings:

- Patch: The patch rating assesses the quality of device accessing the network resources.
- Registration Status: The registration status of the device discovers a registered user or a guest.
- Location: The IP address of the communicating device indicates the location of the users.
- Behaviour: The behavioural parameter gathers the user's visibility, events, and trends.
- History: The user history is validated by the Monte-Carlo cyber access control model at every point in time the user attempts to gain access to the cyber resources.
- Credentials: The credential of the user is used in authenticating the digital documents.
- Access Time: The user time of access gives the pattern of access by the user.

And the Monte Carlo Tree Search (MCTS) consists of four phases:

a) Selection: Algorithm starts at root node, then moves down the tree by selecting optimal child node until a leaf node is reached.

b) Expansion: If the leaf node is not a terminal node then creates one or more child nodes according to available actions at the current state, then selects the first of these new nodes.

c) Simulation: Runs a simulated rollout from the new nodes until a terminal state is found. The terminal state contains a result that will be returned in backpropagation phase.

d) Backpropagation: After simulation phase, a result is returned. All nodes from simulation up to the root node will be updated by adding the result to their value and increase the count of visits at each

 | DOI: 10.20533/jitst.2046.3723.2021.0088

node. Table I described the classified the various level of vulnerabilities of the entities.

Table 1. Monte Carlo simulation entities

Name	**Entity**	**Utility for Monte Carlo Simulation**
		Level of vulnerability: crucial (0 - 0.5), low (0.6 – 1.0)
Patch	p	0 - 0.5
		0.6 – 1.0
Registration Status	R	0 - 0.5
		0.6 – 1.0
Location	l	0 - 0.5
		0.6 – 1.0
Behaviour	$\mathbb{B}$	0 - 0.5
		0.6 – 1.0
History	H	0 - 0.5
		0.6 – 1.0
Credential	C	0 - 0.5
		0.6 – 1.0
IP Element	I	0 - 0.5
		0.6 – 1.0
Access Time	A	0 - 0.5
		0.6 – 1.0
Bandwidth Account	B	0 - 0.5
		0.6 – 1.0
Network Node	N	0 - 0.5
		0.6 – 1.0

4. Results and Discussions

The Monte Carlo simulation network access control model simulated 52241 instances of interaction between the users and provider. The Patch had the total number of 51188 instances characterized with low vulnerability which amounted to 97.98% of the 52241 instances modeled and 1053 instances were identified as crucial, this depicted 2.01% of the users. The Registration Status showed the result of the strategies identified by the model for users' registration status. Complete registration of users requesting access were 42389 which described 81.14% of the users and 9852 (18.86%) users' registration status were considered incomplete.

The location analysis showed the users' requesting access to network resources, the strategy was classified as 50788 (97.22%) instances of dynamic nature and 1453 (2.78%) instances as static. The behavioural analysis showed the 47311 steady users' behavioural strategy which accounts for 90.56% of the users and 4930 (9.44%) erratic users' behavioural strategy. The user history was validated by the Monte-Carlo cyber access control model. Users were classified as hostile and trusted users. The analysis showed 52015 users were trusted which approximately 99.57% instances and 226 instances were not trusted which accounts for 0.43% of the users.

The information of the users included the users' credentials. The analysis showed the model classified users' request with certified information as 32011 instances which was an equivalent of 61.28% and discredited 20230 instances an equivalent of 38.72%. The model classified users into same domain and neighbouring domain. The analysis showed users in the same domain class of IP information was 37038 (70.90%) instances and neighbouring domain was 15203 (29.10%). Monte Carlo Game Access Control classified 43419 (83.11%) users frequently requested access and 8822 (16.89%) users rarely requested access.

Bandwidth describes the maximum data transfer rate of a network. The model classified 51320 (98.24%) instances of fast strategy and 921 (1.76%) of slow strategy. The network nodes of the users were categorized as Secured strategy and Not secured strategy. The analysis showed 42139 (80.66%) users were classified with secured information and 10102 (19.34%) users were not secured network nodes. The overview of the result described the characteristics of the packet information of users.

The Monte Carlo built the decision tree on every request. The distribution of the iterations as described in Table II with range from 0 to 10,000 and the interval is categorized into frequency of thousand as shown in Figure 3.

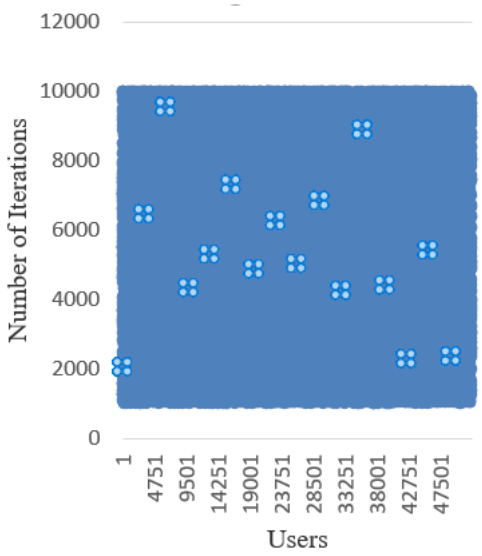

Figure 3. Monte Carlo iterations

Table 2. Distribution of iterations

Range of MCTS Iterations	Number of Users
0-1000	7
1001-1500	2932

 | DOI: 10.20533/jitst.2046.3723.2021.0088

1501-2000	2860
2001-2500	2911
2501-3000	2882
3001-3500	2862
3501-4000	2903
4001-4500	2947
4501-5000	2916
5001-5500	2935
5501-6000	2884
6001-6500	2940
6501-7000	2922
7001-7500	2887
7501-8000	2901
8001-8500	2944
8501-9000	2866
9001-9500	2946
9501-10000	2796

The Monte Carlo Simulation decision result is described in Table 3.

Table 3 Distribution of Iterations

State	Strategy (User and Provider)	Number of Instances	Percentage
S1	Forward - Grant	51186	97.98%
S2	Forward - Deny	1007	1.92%
S3	Damage - Grant	37	0.07%
S4	Damage - Deny	11	0.02%

5. Conclusion

The gaps in the literature reviewed include non-automated network access control, need for visibility of all connected users and need real-time network access control model. Therefore, the result from the study proves the efficiency of Monte Carlo Game Theory technique for network access control mechanism. The study has also established the fact that Monte Carlo Game Theory technique is better than Trust evaluation technique in decision making. The study has further revealed the visibility of requesting users of network environment and established Monte Carlo technique and game theory cyber access model to protect network resources from malicious attacks by limiting access to only authorized users.

6. References

[1] Ciza T. (2020). Computer Security Threats. IntechOpen Publisher.

[2] Xiao M. and Guo M. (2020). Computer Network Security and Preventive Measures in the Age of Big Data. Procedia Computer Science 166, 438-442.

[3] Atlam H. F., Azad M. A., Alassafi M. O., Alshdadi A. A., Alenezi A. (2020). Risk-Based Access Control Model. A Systematic Literature Review. Future Internet.

[4] James S., Konidaris, G. and Rosman, B. (2017). An analysis of Monte Carlo Tree Search. Association for the Advancement of Artificial Intelligence.

[5] Swiechowski M., Godlewski K., Sawicki B. and Mandziuk J. (2021). Monte Carlo Tree Search: A Review of Recent Modifications and Applications. arXiv 210.04931v2, Mar.

[6] Manshaei M., Zhu Q. and Alpcan T. (2013). Game Theory meets Network Security and Privacy. ACM Computing Surveys (CSUR). 45 (3), 1-39, 2013.

[7] Jingsha H., Shunan M. and Bin Z. (2013). Analysis of Trust based Access Control Using Game Theory. International Journal of Multimedia and Ubiquitous Engineering. Vol. 8, No 4, July 2013.

[8] Thejas G.S., Pramod T.C., Iyenas S.S. and Sunith N.R. (2018), "Intelligent Access Control: A Self-Adaptable Trust –Based Access Control (SATBAC) Framework using Game Theory Strategy" Proceeding of International Symposium on Sensor Networks, Systems and Security (2018) pp 97- 111.

[9] Sun, Pan and Jun (2020). A Trust-Game-Based Access Control Model for Cloud Service. Hindawi Mobile Information Systems. Vol. 2020, Article ID 4651205, DOI: 10.1155/2020/4651205.

[10] Esposito C., Tamburis O., Su X. and Choi C. (2020). Robust Dencentralised Trust Management for the Internet of Things by Using Game Theory. Information Processing and Management, Volume 57, Issue 6, Nov.

 | DOI: 10.20533/jitst.2046.3723.2021.0088