SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

VOLUME 2, ISSUE 2
ISSN: 2054 - 7390

A novel Approach to System Security using Derived Odor Keys with Weight Elimination Neural Algorithm (DOK-WENA)

Mahmoud Z. Iskandarani
Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan
m.iskandarani@hotmail.com

ABSTRACT

A novel security technique for network and data communication applications that makes use of odors as password generators is developed and tested. The developed system employs odor keys derived from an original key together with the original key to allow access to systems and networks. The used key combinations are initially unknown to the user, and if detected while in the transmission process, there is no way of being able to be emulated.

The uniqueness of the developed system is that it is not necessary for an odor key to be an exact replica of the original, but to be derived from the original. This is a chemical encryption and encoding as the right key will not be detected by anyone since it is a derived version and not a match. Genetic Algorithm is used to emulate the chemical derivation and to make up for any margin of odor detection error and sensors tolerances.

Keywords: Genetic Algorithm, Olfactory, Odor Sensor, Software, Neural, Algorithm, Security.

1 INTRODUCTIN

The selective application of technological and related procedural safeguards is an important responsibility of every organization in providing adequate security to its electronic data systems. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. Attacks against computer systems and networks are becoming more sophisticated, using new techniques and technologies with increased global interconnectivity, and Internet communication, system security has become a necessity.

Organizations must protect their systems from intruders and other forms of attacks. Such protection must detect anomalous patterns while monitoring normal computer programs and networks. The need for authentication is well understood and is concerned with well-equipped attackers who have access to processes and who merely need a starting point to be considered successful. This conservative approach is now finding its way into standards and specifications.

DOI: 10.14738/tmlai.22.138
Publication Date: 11th April 2014
URL: http://dx.doi.org/10.14738/tmlai.22.138

Network and device security is utilized in various applications and environments. The specific utilization and various implementations will be based on many factors particular to the computer system and its associated components. In general, password security is used to protect data access while it is stored in a medium vulnerable to physical theft or technical intrusion (e.g., hacker attacks, where the key must be maintained and accessible for the duration of the storage period.

A security technique for network data communication applications that makes use of odors as password generators, might adopt both personal and synthetic odors. Such a system not only use such odors as an access control identifier, but also the converted signals obtained from them can be implanted and added randomly to a data file for extra security [1-5].

In this paper, a novel algorithm that employs odors as password and encryption keys is developed within a hierarchical layered architecture, which maps out odor features in a lower (uncertain) and upper (certain) bands, thus resulting in finding the correct access and/or decryption key [6-10].

2 MATERIALS AND METHODS

The used system comprises a combinations of tuned sensors coupled with sophisticated information processing. Each odorant or volatile compound presented to the sensor array produces a signature or characteristic pattern of the odorant.

By presenting many different odorants to the sensor array, a database of signatures is built up. This database of odorant signatures is then used to build odor recognition system. The goal of this process is to configure the recognition system to produce unique classifications or clustering's of each odorant so that an automated identification can be implemented.

When the sensor array is exposed to odor mixtures, containing the molecules to which the devices are sensitive, different response patterns will be created. By detecting odor patterns the system would then be able to classify a vapor mixture and perform security actions as required. Different levels of security exist, depending number of odors required as keys to generate a specific password.

Generally speaking, the odor system collects a sample and routes it through a sensor array where the presence of certain substances are detected. The concentrations of these substances are recorded. The combination of tuned sensors coupled with sophisticated information processing makes the recognition system a powerful instrument for odor applications. Each odorant presented to the sensor array produces a signature or characteristic pattern of the odorant.

Our Multi-Sensor array system employs MOS- based sensors with an SnO_2 metal-oxide semiconducting film coated onto a ceramic substrate Each device also contains a heating element. Oxygen from the air is dissolved in the semiconductors' lattice, setting its electrical resistance to a background level (stable when at equilibrium). During the measurement, the volatile molecules (mainly non-polar) are adsorbed at the surface of the semiconductor where they react (oxidation/reduction) with the dissolved oxygen species causing a further modification of the resistance (or conductivity) of the device. This last change is taken as the response of the system to that particular sample.

By presenting many different odorants to the sensor array, a database of signatures is built up. This database of odorant signatures is then used to build the odor recognition system. The goal of this process is to train or configure the recognition system to produce unique classifications or clustering's of each odorant so that an automated identification can be implemented. During testing operation, a chemical vapor or odor is blown over the sensor array, the sensor signals are digitized and fed into the computer, with intelligent classification algorithm used to identify the odor and its relation to others odors.

Consider a classification problem where a test pattern is to be assigned to a class label (Odor Class), OC where:

$$OC \in \{OC_1, OC_2, ..., OC_n \} \tag{1}$$

n: Number of possible classes.

Measuring the test pattern is carried out by means of M sensors. Assume that the observations on the test pattern from the ith sensor are represented by the feature vector $S_i \quad (i = 1...m)$, which can be assumed a row vector. The objective now is to map $S_i \quad (i = 1...m)$ to a pattern class OC.

S_i can be considered an estimation of the test pattern's characters using the ith sensor. Different sensors probably give different measurements due to the factors of sensor type, position, sensitivity, while measuring same odor and describing the same test pattern. So there must be some kind of inherent relationship among them.

We define S_0 as the Center-Feature (CF) which is the default and intrinsic response of the test pattern's characters, which is a priori feature. Hence, there is a functional relationship T_i between S_0 and S_i :

$$S_i = T_i(S_0) \tag{2}$$

T_i: Transformation Function (TF).

Using CF and TF, the observation set $\{S_1, ...S_m\}$ can be re-written as:

$$\{T1(S_0), ...T_m(S_0)\} \tag{3}$$

which is the mapping from the observation set to the pattern class label OC.

3 RESULTS AND DISCUSSION

Table 1 shows the obtained results from exposing an odor sensor array unit to six different types of odors where the presence of certain substances is detected. The concentrations of these substances are counted and recorded as digital pulses. Each odorant presented to the sensor array produces a signature or characteristic pattern of the odorant.

Table 1: Sensor Array Pulse Output

Time(Sec)	**Number of Response Pulses (N) for Six Odor Samples**					
t	**k_1**	**k_2**	**k_3**	**k_4**	**k_5**	**k_6**
10	119	19	8	13	13	21
20	145	25	10	18	17	40
30	160	29	11	21	21	50
40	169	30	11	24	22	54
50	174	32	12	26	23	55
60	178	34	13	27	24	56

Each sensor response signal rises from its base as the sensor detects the presence of a particular odor. This means an unstable rising function of signal amplitude for a certain period of time followed by a stable and constant value for a second period of time. Such behavior would not be obvious from the sensor readings and will not show which key is the one derived from the original key that can be used as a password to the intended system [11-15].

For the system to only accepts the correct odor key, which is also encrypted within the signal readings as the main, master odor key is not emulated in an opening key but the opening odorant key is derived from the master key composition, and hence, the output readings for any odorant key will not be equal to the original master key. This is a new way of hiding the key [16-20].

To uncover the correct password odorant key, all represented keys are processed using equations 4 and 5 as part of the mapping process into lower and upper bounding parts as shown in Tables 2-6.

$$Odor_{code\ match}(t) = XOR(k_i, k_j) = const. \dots \qquad (4)$$

$$(k_i, k_j) = (k_n, k_i)\, XOR\, (k_n, k_j) \dots \qquad (5)$$

Table 2: Odor Keys Map1

t	k_1k_2	k_1k_3	k_1k_4	k_1k_5	k_1k_6
Lower Bounded					
10	100	127	122	122	98
20	136	155	131	128	185
30	189	171	181	181	146
Upper Bounded					
40	183	162	177	191	159
50	142	162	180	185	153
60	144	191	169	170	138

Table 3: Odor Keys Map2

t	k_2k_3	k_2k_4	k_2k_5	k_2k_6
Lower Bounded				
10	27	30	30	6
20	19	11	8	49
30	22	8	8	47
Upper bounded				
40	21	6	8	40
50	44	58	55	23
60	47	57	58	26

Table 4: Odor Keys Map3

t	k_3k_4	k_3k_5	k_3k_6
Lower Bounded			
10	5	5	29
20	24	27	34
30	30	30	57
Upper Bounded			
40	19	29	61
50	22	27	59
60	22	21	53

Table 5: Odor Keys Map4

t	k_4k_5	k_4k_6
Lower Bounded		
10	0	24
20	3	58
30	0	39
Upper Bounded		
40	14	46
50	13	45
60	3	35

Table 6: Odor Keys Map5

t	k_5k_6
Lower Bounded	
10	24
20	57
30	39
Upper Bounded	
40	32
50	32
60	32

Careful analysis of the odorant feature maps in Tables 2-6, results in the following observations:

1. The lower bounding encloses the unstable part of the sensor's response to odor keys, while the upper bounding encloses the stable and certain part of the sensor's response.
2. As the number of equity features increases in the lower and unstable bounding, the probability of such a key to be derived from the master one decreases.
3. As the number of equity features increases in the upper and stable bounding, the probability of such a key to be derived from the master one increases.

From the features maps in the tables, semi-final feature map is constructed by the algorithm based on sequential correlation of occurring features per main key per same location over succession of keys. This is illustrated in Table 7.

Table 7: Lower Bounded Final Feature Map

Testing Key	Number of Identical Features {Lower, Upper}	Bounded Features {lower, Upper}
k1	{0, 0}	{15, 15}
k2	{2, 0}	{12, 12}
k3	{0, 2}	{9, 9}
k4	{0, 0}	{6, 6}
k5	{0, 3}	{3, 3}

From table 7, it is clear that k_5 is the correct key as it has zero equity features in the lower bounding and three out of three equity features in the upper bounding. This gives a matching of %100, while k3 has two out of nine features with matching of only %22, with the rest of the keys k_1, k_2, k_4 having %0 matching.

Considering the keys data for k_5 and k_6 and the resulted pairing of (k_5, k_6), which is shown in Figure 1, the following is deduced from the plot:

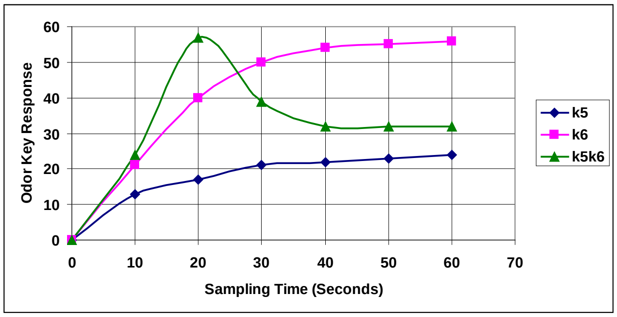

Figure 1: Master and Derived key Responses.

1. k_5k_6 response is consistent with the typical sensor response as it rises when the sensor is exposed to the odorant, reaching a maximum value, then decaying over time to a stable equity and constant region.
2. The observed response for k_5k_6 differs from the conventional response in that it settles at a constant value over the upper bounding part for the rest of the sampling time, instead of decaying towards zero.
3. The observed constant value, which is derived from both k_5 and k_6 responses proved that k_5 is the derived key and can be used to access the system.

For k_3 as a testing key and as it has two equity features in the upper bound, is not a derived key from k_6, as it shows unstable curve with no constant region, as illustrated in Figure 2.

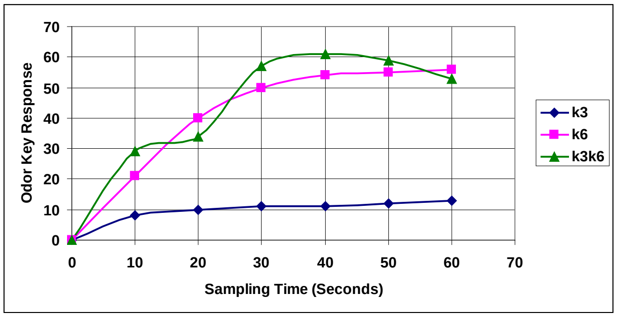

Figure 2: Relationship between k_3 and k_6.

The stability and instability of odor keys and the checking of matching with the master key is further checked by the algorithm using slide-XOR mapping as shown in Table 8.

Table 8: Slide-XOR for k_5k_6

k_6/k_5	13	17	21	22	23	24
21	24	4	0	3	2	13
40	37	57	61	62	63	48
50	53	35	39	36	37	42
54	59	39	35	32	33	46
55	58	38	34	33	32	47
56	53	41	45	46	47	32

Table 8 is divided into two main areas:

1. Unstable, lower bounded characterized by the line matrix [24, 57, 39].
2. Stable, upper bounded area characterized by the line matrix [32, 32, 32].

From the Mapping of data in Table 8, the following is observed:

1. In the stable, upper bounded area, the result of XORing any diagonally based values around the center value of 32 is 0. This indicates validity of k_5 as derived from k_6. The pairs are: {33,33}, {46,46}, {47,47}, {32,32}.
2. In the stable, upper bounded area, the result of XORing any diagonally unequal values around the center value of 32 is constant and equal to 14. The pairs are: {46,32}, {47,33}.

The table which represents a multi-level filtered map shows clearly which odor key fits to unlock and access the required system.

The overall decision making using the DOK classification algorithm can be described by equation 6.

$$Odor_{code\ match}\left(t,_{x+i}\right) = XOR\left(k_m, k_{m+1}\right) = 0 \quad \ldots \qquad (6)$$

The overall DOK algorithm is simulated using Weight Elimination Neural Algorithm (WENA) as shown in Figure 3.

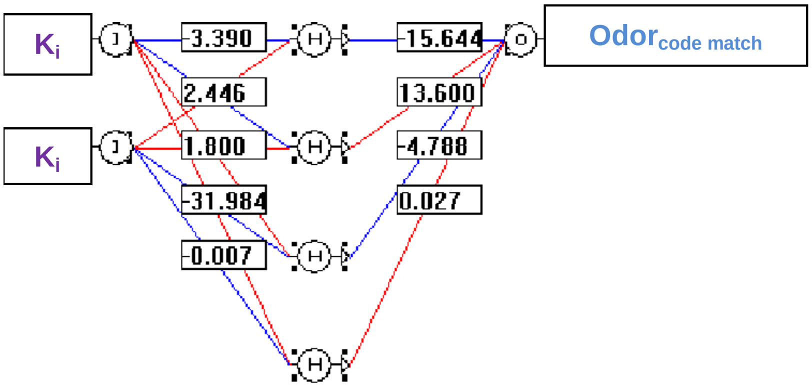

Figure 3: WENA Structure (Alpha: 0.9, LRate: 0.1, dL: 2.5)

Training of the Neural Network was carried out using Weight Elimination Neural Algorithm (WENA), which is a bidirectional Bottom-Up, Top-Down pruning algorithm. It starts with a simple, then complex network and drives unnecessary weights during training towards zero.

The WENA makes use of a liability function that is based on the error function. By reducing the number of connection weights and hence the model's complexity using the weight-elimination liability term, it is expected that network's classification performance to improve.

The weight-elimination overhead function is shown in equation 7. The liability term in weight-elimination minimizes the sum of performance error and the number of weights using standard back propagation technique.

$$E_{Total}(W) = E_{Sum\,Squared}(W) + E_{Liability}(W) \ldots \qquad (7)$$

$E_{Total}(W)$ is the combined overhead function that includes the initial overhead function, $E_{Sum\,Squared}(W)$ and the weight-elimination term $E_{Liability}(W)$.

$$E_{Sum\,Squared}(W) = \frac{1}{2}\sum_k (T_k - O_k)^2 \ldots \qquad (8)$$

Where:

T_k : Target Output

O_k : Actual Output

$$E_{Liability}(W) = \xi \left(\sum_{jk} \frac{\left(\frac{w_{jk}}{w_{epochs-n}} \right)^{2}}{1 + \left(\frac{w_{jk}}{w_{epochs-n}} \right)^{2}} \right) \ldots \qquad (9)$$

Hence;

$$\Delta W = \left(-\eta \frac{\partial E_{Sum\,Squared}}{\partial W} \right) - \left(\xi \frac{\partial E_{Liability}}{\partial W} \right) \ldots \qquad (10)$$

Where

η: Learning Rate (between 0 and 1)

W represents the weight vector, ξ is the weight-reduction factor, and w_{jk} represents the individual weight of the neural network model.

The role of the weight-reduction factor is to determine the relative importance of the weight-elimination term. Larger values of ξ pushes small weights to further reduce their size. Small values of ξ will not affect the network.

The scale parameter, $w_{epochs-n}$, is a scale parameter computed by the WENA, and chosen to be the smallest weigh from the last epoch or set of epochs to force small weights to zero.

The Neural engine is tested with another odor (k_7) derived from odor k_6. The ratios of chemical concentration derivation are k_7=0.67K_6 and k_5=0.33K_6. The results are shown in Table 9:

Table 9: Neural Networks Testing Results

k7	k6	k5	k7k6-Odor code match	k5k6-Odor code match
25.000	21.000	13.000	3.000	24.000
40.000	40.0000	17.000	42.000	57.000
50.000	50.000	21.000	30.000	39.000
55.000	54.000	22.000	26.000	32.000
55.000	55.000	23.000	26.000	32.000
60.000	56.000	24.000	26.000	32.000

It is clear that both codes have similar upper and lower bound characteristics with similar patterns that indicate that they originated from the same odor source (master key), hence both keys can be used as passwords and encryption keys. It also indicates that the unlocking key and password can be changed by deriving another key from the original with the ability to use multi-level passwords and public and private keys, with the advantage of hiding the keys inside the master key.

4 CONCLUSION

The implemented intelligent algorithm within the designed sensing system proved to be able to detect and classify different odor combinations. Such an approach combined with neural engine forms an excellent platform for further development of odor keys as security and data encryption keys. Such keys can be an array of metal oxide sensors or any custom designed chemiresistors together with an electronic system that is controlled by specially developed software, which extract sequences and subsequence and place them in a feature map before applying the proposed algorithm. The system makes decisions about the odorant at certain concentrations using detection and recognition levels for the odorants. Such security system can replace traditional biometric systems like fingerprint or iris. It also replaces traditional door and safe keys with odor keys that are randomly selected and combined with impossibility of hacking.

REFERENCES

[1]. E. Kim 1, S. Lee, J. Kim, C. Kim, Y. Tae Byun, H. Kim, T. Lee, Pattern Recognition for Selective Odor Detection with Gas Sensor Arrays. Sensors. 2012. 12(12): p.16262-16273. doi:10.3390/s121216262.

[2]. Y. Tian, X. Kang, Y. Li, W. Li, A. Zhang, J. Yu, Y. Li, Identifying Rhodamine Dye Plume Sources in Near-Shore Oceanic Environments by Integration of Chemical and Visual Sensors, Sensors. 2013. 13(13): p.3776-3798. doi:10.3390/s130303776.

[3]. T. Dymerski, J. Gębicki, P. Wiśniewska , M. Śliwińska, W. Wardencki, J. Namieśnik, Application of the Electronic Nose Technique to Differentiation between Model Mixtures with COPD Markers, Sensors. 2013. 13(4): p.5008-5027. doi:10.3390/s130405008.

[4]. K. Fujioka, E. Arakawa, J. Kita, Y. Aoyama, Y. Manome, K. Ikeda, K. Yamamoto, Detection of Aeromonas hydrophila in Liquid Media by Volatile Production Similarity Patterns, Using a FF-2A Electronic Nose, Sensors. 2013. 13(1): p.736-745. doi:10.3390/s130100736.

[5]. W. Yu, S. Wang, Key pre-distribution using combinatorial designs for wireless sensor networks, nodes have the same capabilities and constraints, WSEAS Transactions on Mathematics, 2013. 12(1): p.32-41. doi:10.1109/TNET.2007.892879.

[6]. Y. Lan, X. Zheng, J. Westbrook, J. Lopez, R. Lacey, W. Hoffmann, Identification of Stink Bugs Using an Electronic Nose. Journal of Bionic Engineering, 2008. 5(1): p.172-180. doi:10.1016/S1672-6529(08)60090-6.

[7]. M. Zarzo, Effect of Functional Group and Carbon Chain Length on the Odor Detection Threshold of Aliphatic Compounds, Sensors, 2012. 12(1): p.4105-4112. doi:10.3390/s120404105.

[8]. Puligundla, J. Jung, S. Ko, Carbon dioxide sensors for intelligent food packaging applications, Food Control, 2012. 25(1): p.328-333. doi.org/10.1016/j.foodcont.2011.10.043.

[9]. M. Mannoor, H. Tao, J. Clayton, A. Sengupta, D. Kaplan, R. Naik, N. Verma, F. Omenetto, M. McAlpine, Graphene-based wireless bacteria detection on tooth enamel. Nature Communications, 2012. 763(3): p.1-8. Doi:10.1038/ncomms1767.

[10]. F. Benrekia, M. Attari, M. Bouhedda, Gas Sensors Characterization and Multi-layer Perceptron (MLP) Hardware Implementation for Gas Identification Using a Field Programmable Gate Array (FPGA), Sensors, 2013. 13(1): p.2967-2985, 2013 doi:10.3390/s130302967.

[11]. B. Zhou, J. Wang, Detection of Insect Infestations in Paddy Field using an Electronic Nose, International Journal Of Agriculture & Biology, 2011. 13(5): p.708-712. doi:11–058/SAE/2011/13–5–707–712.

[12]. C. Wongchoosuk, M. Lutz, T. Kerd-charoen, Detection and Classification of Human Body Odor Using an Electronic Nose, Sensors, 2009. 9(1): p. 7234-7249. doi:10.3390/s90907234.

[13]. H. Lee, W.Yang, N. Choi, S. Moon, Encapsulation of Semiconductor Gas Sensors with Gas Barrier Films for USN Application, ETRI Journal, 2012. 34(5): p.713-718. doi:10.4218/etrij.12.0112.0266.

[14]. A. Lotfi, S. Coradeschi, Odor Recognition for Intelligent Systems, IEEE intelligent Systems, 2008. 23(1): p.41-48. doi: 10.1109/MIS.2008.11.

[15]. M. Ke, M. Lee, C. Lee, L. Fu, A MEMS-based Benzene Gas Sensor with a Self-heating WO3 Sensing Layer, Sensors, 2009. 9(4): p.2895-2906. doi:10.3390/s90402895.

[16]. M. Iskandarani, Low Pass Filter Model for Chemical Sensors in Response to Gases and Odors, American Journal of Applied Sciences, 2012. 9(4): p.605-608. doi: 10.3844/ajassp.2012.605.608.

[17]. M. Iskandarani, Inheritance based Intelligent Technique Employing Nested-XOR with Recursion for Recognition and Classification of Odors using Multi-Sensor Nose System, American Journal of Applied Sciences, 2011. 8(9): p.910-917. 10.3844/ajassp.2011.910.917.

[18]. M. Iskandarani, A Novel Odor Key Technique for Security Applications Using Electronic Nose System, American Journal of Applied Sciences, 2010, 7(8): p.1118-1122. doi:10.3844/ajassp.2010.1118.1122.

[19]. M. Iskandarani, A Novel Approach to Signal Detection of Sensor Array Units Using 5-3-1 Rule Based Matched Filter Algorithm with Intelligent Identifiers, American Journal of Engineering and Applied Sciences, 2010. 3(2): p.427-432. doi: 10.3844/ajeassp.2010.427.432.

[20]. M. Iskandarani, Mathematical Modeling and Characterization of Thin Film, Narrow Gap Sensor Array Units (SAU), American Journal of Applied Sciences, 7(9): p.1277-1284. doi: 10.3844/ajassp.2010.1277.1284.