西南交通大学学报

第 55 卷 第 2 期
2020 年 4 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol. 55 No. 2
Apr. 2020

ISSN: 0258-2724

DOI：10.35741/issn.0258-2724.55.2.1

Research article

Computer and Information Science

# A HYBRID SECURITY SYSTEM FOR UNMANNED AERIAL VEHICLES
# 无人驾驶飞机的混合安全系统

**Shahad Mahdi Al-Abrez [a], Khattab M. Ali Alheeti [b], Abdul Kareem A. Najem Alaloosy [b]**

[a] Computer Sciences Department, College of Computer and Information Technology, University of Anbar
Anbar, Iraq, shahadmahdi17@uoanbar.edu.iq
[b] Computer Networking Systems Department, College of Computer and Information Technology, University of Anbar, Iraq, co.khattab.alheeti@uoanbar.edu.iq, alaloosy@gmail.com

***Received: January 10, 2020 ▪ Review: February 10, 2020 ▪ Accepted: February 20, 2020***

## Abstract

Autonomous unmanned aerial vehicles are one of the most important applications in modern technology. Otherwise known drones, these vehicles perform a lot of vital missions and sensitive tasks in scientific discoveries and agricultural and military applications. Drones that are in a network possess the freedom to roam in various directions. The security system of drones plays an important role in performing services. In this paper, a hybrid security system is proposed for drones to protect their data. This detection system is designed to protect autonomous drones from any attack. The proposed approach is implemented in a highway environment scenario. Our experimental results for the security system demonstrate that the proposed approach possesses an outstandingly accurate rate for intrusion detection.

**Keywords:** Unmanned Aerial Vehicle, Drone, Intrusion Detection System, Watchdog Technique, Pathrater Technique

**摘要** 自主无人机是现代技术中最重要的应用之一。这些车辆在其他方面也称为无人机，在科学发现，农业和军事应用中执行许多重要任务和敏感任务。网络中的无人机拥有在各个方向漫游的自由。无人机的安全系统在执行服务中起着重要作用。本文针对无人机提出了一种混合安全系统，以保护其数据。该检测系统旨在保护自主无人机免受任何攻击。所提出的方法是在高速公路环境中实施的。我们针对安全系统的实验结果表明，所提出的方法具有出色的入侵检测准确率。

**关键词:** 无人机，无人机，入侵检测系统，看门狗技术，探路者技术

## I. INTRODUCTION

An unmanned aerial vehicle (UAV) is an aircraft that flies without any human interaction onboard [1], [18], [19]. There are two types of flight control in UAVs: autonomous on-board computer systems or remotely via a ground operator. UAVs are officially referred to as drones in modern applications [2]. These vehicles are widely utilized in the civil research field, scientific discoveries, and complex military missions. However, they are primarily utilized in military applications. Device miniaturization, communication systems, and computing boards play an important role in creating a new generation of drones, such as gliders, quad copters, and balloons. This UAV was able to perform many risky missions that would have been to dangerous for human pilots.

Figure 1. Drone

Recently, more civilian applications have been initiated for drones. In addition to inspection and policing, search and rescue operations during natural disasters are considered a very important application. In such instances, drones require an external communication system, whether transmitting, receiving, processing or collecting a wide range of control data and sensitive information.

(UAVs) deal with sensitive data. Depending on the mission, this data needs to be secured and protected from various types of attacks, fraud, and theft in order to achieve integrity, authentication, confidentiality, and availability [1].

These challenges have been introduced in this context:

- Supplemented overhead has been introduced by UAV communications for architecture deployment, reliability, consistency, and design.
- Path planning and UAV deployment must be considered due to the energy efficiency.
- Insufficient integration due to the structural design of UAV communication.
- The suffering from the devoted spectrum sharing [2].
- The mechanisms of security systems can be classified as signature-based [3], specification-based [4], anomaly-based [5], and hybrid-based [6]. The integration of two or more security methods is called the hybrid-based system, which is a robust system that can detect attacks.
- The intent of this research paper is to describe a hybrid security system based on two methods: the watchdog and the path rater techniques. Both provide an intelligent architecture that protects the network by effectively detecting malignant nodes and substituting a counterfeit route with the true one [7].
- This paper begins by presenting a general overview about the UAV in section I, before introducing some challenges concerning UAV communication. Section II presents the background of works related to our subject. Section III presents some abbreviated information about drone communication systems, while section IV explains the methodology of this work. In section VI, we discuss the experimental results of this paper. Section VII continues this discussion. Finally, section VIII offers a conclusion and suggestions for the direction for future work.
-

## II. Literature Review

- Many researchers focus on the intrusion detection problem by addressing the security aspects of UAVs. Several attacks have been studied, and some of the research is summarized below.
- M. Ali et al. [8] defined the drone identification in which each drone has a special code generated by the spreading method. Because of this system, any drone that does not stratify the Drone Identification (DID) is not allowed to fly as it is an unauthenticated drone. The proposed method is based on various parameters, such as the country code, the date, and the serial number of the drone. The proposed method is useful in the IoT environment with large number of robots.
- M. Ali et al. [10] presented a hybrid intrusion detection system by merging the misuse-based intrusion detection system with the anomaly-based intrusion detection system, resulting in the Network Traffic Anomaly Detection (NETAD) and the Packet Header Anomaly Detection (PHAD). They then use Massachusetts Institute of Technology (MIT) Lincoln Laboratories network traffic data (Intrusion Detection Evaluation dataset (IDEVAL)) to evaluate this system, which can compare the number of attacks detected by the hybrid intrusion detection system to those found by the misuse-based intrusion detection system.

P. Nishant et al. [12] used an attacker node as the initial phase in the ad hoc on-demand distance vector (AODV) routing protocol in the vehicular ad hoc network (VANET) and then evaluated the malignant node using the watchdog intrusion detection system as a second phase. The Bayesian network theory has been used to deny the attacker node any access to communication with other neighbor nodes. The solution has been implemented for the malignant node and some attacks such as the grey hole and the black hole for the AODVs.

N. Soganile et al. [13] studied the weak points of the mobile ad hoc network (MANET) and focused on the black hole attacks, their types, and their effects on the MANET. The authors discuss the detection of the black hole attacks by the radical path rater and the watchdog algorithms. The proposed algorithms are an extension of the watchdog-path rater algorithm, which has been designed to detect the intrusion by finding it and issuing an ultimatum to the next node to make sure that malignant nodes will be determined within the entire MANET.

Z. Ruohao et al. [14] used the robust controller and spectral traffic analysis to create a hybrid method based on the behavior of user datagram protocol and transmission control protocol. The first step in this method involved a statistical signature that tracked down a set of signatures, the model then being selected according to various signatures based on some types of intrusions that were produced in the network. A specific controller is chosen from among a collection of models.

Our work is distinct from that of the others as it depends on artificial intelligence for designing the intrusion detection system in the network layer; this is much easier and also employs the control system at the data link layer.

## III. Drone Communication Systems

Unmanned aerial vehicles (UAVs) consist of different fundamental components that perform specific objectives consistently, but the communication system is the most important component for helping UAVs and their operators to obtain the desired results. It is impossible to collect and transmit communications data without communication systems. Because of their strong communication links, weights, small sizes, and low power consumption, these systems provide the most appropriate solutions for civilian drones. The systems operate on 2.4 GHz and 5.8 GHz frequencies. One frequency has been used by the UAV communication system for controlling drones from the ground; the other frequency is used to shift first-person view (FPV) videos [9].

To obtain real-time data on the UAVs, these systems communicate with the ground control systems wirelessly, which can achieve security and navigation safety for the drones and monitor immediate live videos from drone cameras.

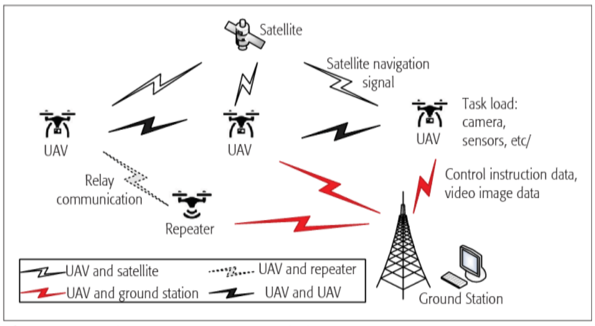

Figure 2. Drone communication system [10]

There are different types of ground control systems (GCS) in smartphones and desktop configurations, and the desktop GCS is better than the smartphone one. An efficient deployment strategy is required for the communication between the drone and the controller, which can be performed by either:

- Networks—initiated bases or ground coordinates
- Host-based or autonomous systems [2].

The transmissions to UAVs are supported directly by communication links; this allows multiple UAVs to share information with a ground system. The traffic is also monitored by these links between the source and the destination.

Wireless communication systems are a possible option for rapid deployment, trusted, and elastic communication links. These systems can be divided into two categories. The first includes short-range communication technologies, which support information that is being transferred from several millimeters to a few hundred meters as follows:

- Bluetooth (IEEE 802.15.1)
- Wi-Fi (IEEE 802.11)
- ZigBee (IEEE 802.15.4).

The second category involves long-range communication technologies, which support information that is being transferred and can be classified as follows:

- Long-Term Evolution (LTE)
- WiMAX (IEEE 802.16)
- Satellite Communication (SATCOM)
- Fifth Generation (5G) [11].

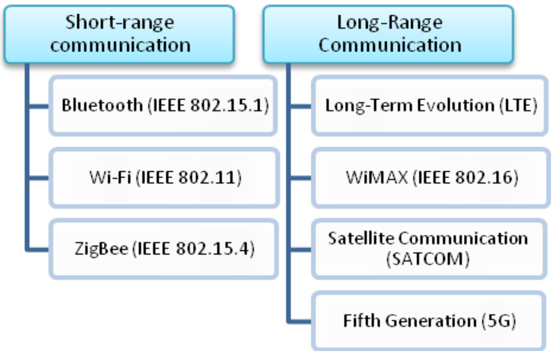
Short-range communication
Bluetooth (IEEE 802.15.1)
Wi-Fi (IEEE 802.11)
ZigBee (IEEE 802.15.4)
Long-Range Communication
Long-Term Evolution (LTE)
WiMAX (IEEE 802.16)
Satellite Communication (SATCOM)
Fifth Generation (5G)

Figure 3. Communication system categories

The most important topics for UAV communication systems are information security and the protection of data links. Such protection can be provided using frequency hopping techniques, smart signal processing, error robust protocols, and spread spectrum methods [11].

### A. Reactive Routing Protocol (AODV)

To apply flying ad hoc network (FANET) tasks, all controlling processes should be carried by UAVs and GCSs. As such, routes between nodes are found using adapted routing protocols, taking into consideration the specific FANET features for ensuring that the communication between GCSs and UAVs is effective [12].

There are two methods that have been proposed for producing routing protocols. The first is creating the protocol from scratch by deciding on the route authenticity or detection and then performing route conservation and packet transportation. The second involves adopting the current routing protocol [13]. This design option has gained more focus because it allows the interoperability to stay among the sensor nodes and land vehicles when using FANETs for improving the communication of the land nodes. As a result, there is no protocol for implementation that is preferable to other protocols [14].

In fact, the protocols that have been mentioned have the same goal because they attempt to increase fertility while decreasing the packet waste and commanding the upper load and end-to-end lateness that result from the same protocol.

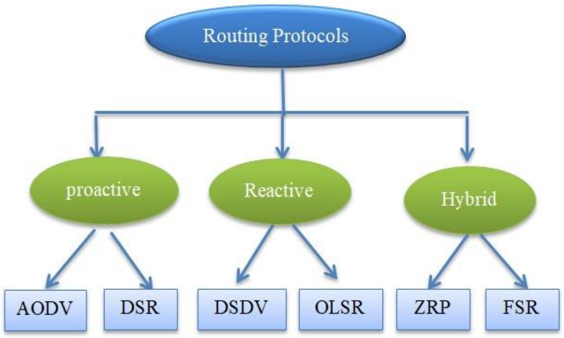

Figure 4. Routing protocols classification

## IV. Methodology

In this section, we describe the watchdog and the path rater techniques that are used for detecting the routing misbehavior and assist routing protocols in averting these nodes by ignoring them and producing a new path to improve throughput [2]. The k-nearest neighbor algorithm will also be described in this section.

### A. Watchdog

The watchdog technique uses a high-confidence, face detection algorithm when it implements the detection system on the misbehaving nodes. The watchdog nodes monitor the local neighbors through messages to reveal black hole nodes. The local monitoring can reveal, through packet drop and intentional packet delay, the modifications on the packet and packet forge. Whenever a node sends a data packet, the watchdog node proves the validity of the following node and then transports the packet. All nodes in the transmission range are evaluated by the watchdog algorithm.

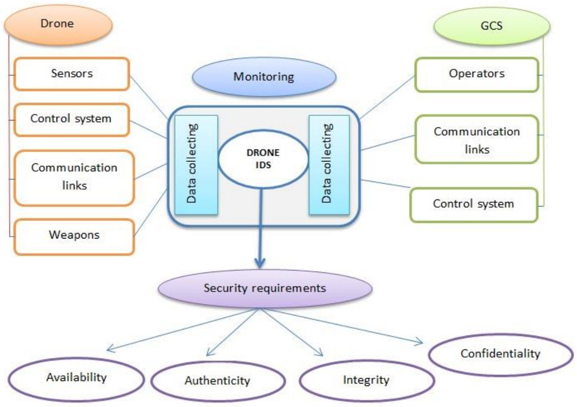

Figure 5. Drone detection system [15]

The watchdog technique counts the delay time of transmitting messages and matches it with the value of the threshold if a received message packet does not get sent by any node. If the threshold value is bigger than the delay time, then the watchdog determines the next node as an alternative, otherwise, the node is determined as a malignant node. Watchdog advertises that the node is a sinkhole node and excludes it from the packet sending path, only if a node only agrees with the watchdog node and does not transmit. The sinkhole node can infinitely send and deliver packets [9].

The watchdog method along with the dynamic source routing has an advantage, that is, it can reveal misbehavior at the link level as well as at the sending level. However, the watchdog cannot reveal the mistreated nodes in several cases, such as during collision, partial dropping, transmitter collision, and fault mistreatment. The watchdog works inconveniently if it knows where the data packet must be in the two nodes. As dynamic source routing is a source-routing protocol, the watchdog can know the data packet position. In case that the watchdog does not have the data packet position, the data packet will be broadcasted to a pseudo node if the watchdog was performed on a hop-to-hop routing protocol [20].

### B. Pathrater

Pathrater performs in every node of the network; it is responsible for analyzing the accuracy of the packet exchange paths by selecting the most authentic one. Each node in the network performs the estimation for other nodes. The Pathrater, according to the path metric, simulates the shortest path algorithm when there is no reliable information. The path with the highest metric is selected if there is more than one path for the same destination, contrary to the standard dynamic source routing, wherein the shortest path of the route stash is chosen. A route request would be sent by the Pathrater if it could not get a free path of misbehaving nodes.

Due to everything mentioned, the Watchdog and Pathrater techniques would act best when paired with the source routing protocol [20].

### C. K-Nearest Neighbor Algorithm

KNN is a learning method based on instance type of object classification, depending on the exercising samples in the space of the features. It is the easier machine-learning algorithm that classifies objects according to the superiority polling of their neighbors [21]. It assigns objects to their nearest neighbor class and can be utilized with statistical schemes to classify the proposed intrusion detection system. KNN can also be implemented by simply using local information to produce an extremely adaptive behavior. However, this algorithm requires a great computation cost and major distance calculation amount.

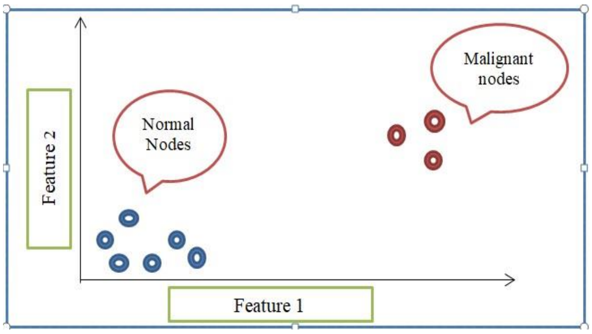

Figure 6. KNN schematic diagram

The mentioned algorithm has two parameters: the first one is the (K) value, which is the number of nearest neighbor nodes; the second parameter is the cutoff value used for the ruling of misbehaving nodes. To choose the correct cutoff and (K) values, we will assume that normal nodes are (N1) and misbehaving nodes are (N2), in which (N1) is bigger than (N2) [16].

K-distance function can be calculated by dividing the summation of all neighbors in Euclidean distance by (K). We can determine the suitable (K) value by keeping the normal node K-distance function as little as possible and the misbehaving node K-distance function as big as possible. The misbehaving nodes can be determined by the difference between the cutoff value and the K-distance function.

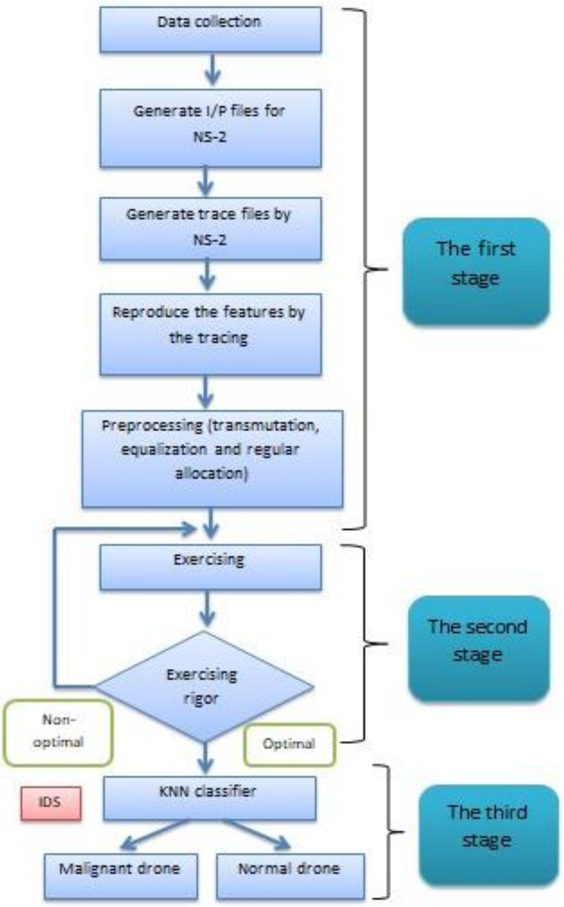
Data collection
Generate I/P files for NS-2
Generate trace files by NS-2
Reproduce the features by the tracing
Preprocessing (transmutation, equalization and regular allocation)
The first stage
Exercising
Exercising rigor
Non-optimal
Optimal
The second stage
IDS
KNN classifier
Malignant drone
Normal drone
The third stage

Figure 7. IDS architecture

### D. Data Normalization

Normalization is a value-regulation process that putting data into tabular form for avoiding data redundancy. Comparing identical values in various data sets is made possible by the normalization process. Without normalization, data can be misclassified and become difficult to compare with other parameters. It has several techniques such as:

- Feature climbing.
- Variation coefficient.

- Standard score.
- Integrated moment.
- Studentized overflow.

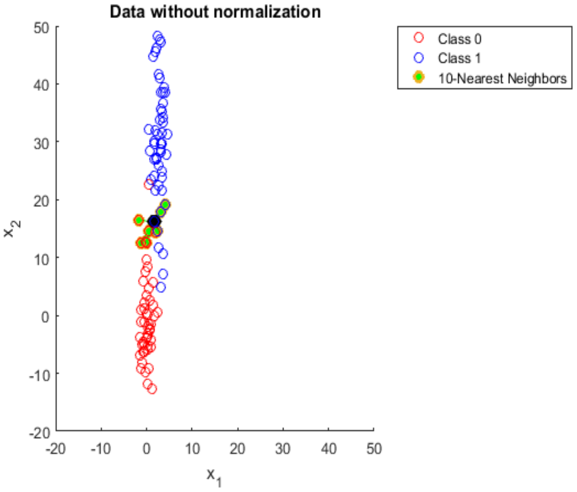

Figure 8. Data without normalization [17]

Normalization has been used in this research to prevent the consequences of misclassification.

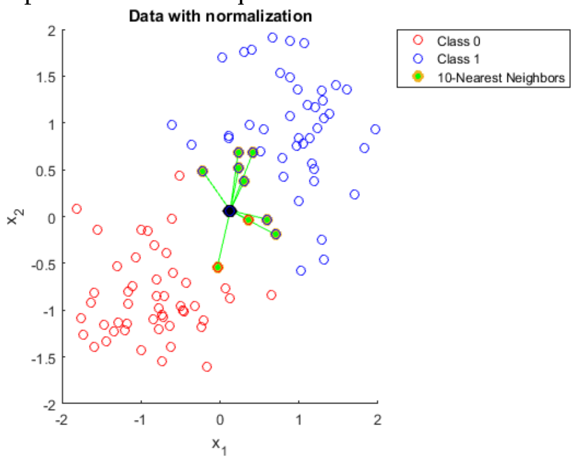

Figure 9. Data with normalization [17]

## V. Experiment Results

The dataset has been used for verifying the proposed detection system performance. The security system can be classified into two behaviors: the first is normal behavior and the second is malignant behavior. The accuracy of the proposed intrusion detection system (IDS) can be measured by the correct data detection among all datasets. We can say that the accuracy rate is high when there is a low error rate and high values of true negative and true positive. The accuracy metric equation (1) is used for determining the IDS feasibility.

$$Accuracy\ Rate = \frac{correct\ classification\ number}{patterns\ synoptic\ number} * 100\ \% \qquad (1)$$

The measurements are calculated as follows:

$$True\ negative\ rate = \frac{true\ negative}{true\ negative + false\ positive} \qquad (2)$$

$$True\ positive\ rate = \frac{true\ positive}{true\ positive + false\ negative} \qquad (3)$$

$$False\ negative\ rate = \frac{false\ negative}{false\ negative + true\ positive} \qquad (4)$$

$$False\ positive\ rate = \frac{false\ positive}{false\ positive + true\ negative} \qquad (5)$$

In which:

- True negative means attack records as attack.
- True positive means normal records as normal.
- False negative means attack records as normal.
- False positive means normal records as attack.

The (K) value was 4, the testing sample size was 3000 records, and the training sample size was 5000 records with no misclassification.

Table 1.
The classification accuracy

| Behavior | Real data | KNN data | Accuracy rate | Error rate |
|---|---|---|---|---|
| Normal | 2676 | 2676 | 100 % | 0 % |
| Malignant | 324 | 324 | 100 % | 0 % |

Table 2.
The recognition rate

| Alarm type | Accuracy | Alarm Rate |
|---|---|---|
| True positive | 100 % | 2676 |
| True negative | 100 % | 324 |
| False-negative | 0 % | 0 |
| False-positive | 0 % | 0 |

The Elapsed time:

- First time: 77.355358 seconds.
- Second time: 81.5329936 seconds.
- Third time: 75.994409 seconds.
- Fourth time: 75.650683 seconds.

## VI. Discussion

The security techniques such as the digital signature and the encryption are not enough for safeguarding systems against many types of attacks, for this reason, we proposed our intelligent intrusion detection system for protecting drones from black hole attacks and other types of attacks. The proposed system is implementing the following phases: simulation, data collection, preprocessing, feature extraction, normalization, training, and testing. The results show that the system is accurate and efficient by defining the normal and malignant nodes with an accuracy rate of 100% and an error rate of 0%.

The use of the normalization supplies depends on flexibility for detecting attacks by increasing the detection ratio from 89.20% to 100% and decreasing the false alarms from 10.80% to 0% within 77.355358 seconds. Due to the mentioned results, the proposed system plays an important role in identifying and blocking the attacks.

We compared our system's accuracy and error rates with the rates given in [16] for evaluating the performance of the proposed system.

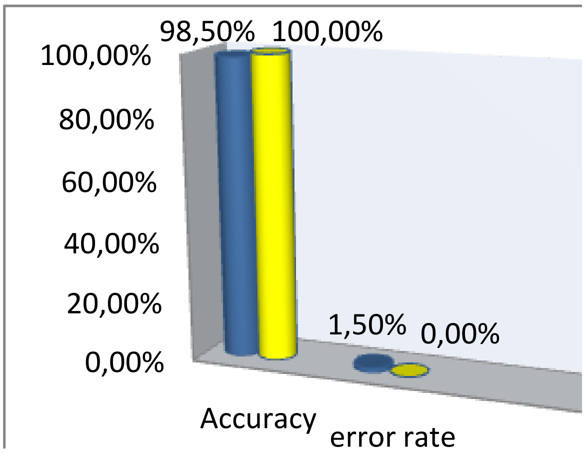

Figure 10. Performance metrics

## VII. Conclusion and Future Works

In this research, we proposed an intelligent intrusion detection system based on watchdog and pathrater techniques for detecting different types of attacks. The K-nearest neighbor algorithm is used to design this system for training and examining the parameters with the extracting features from drones. The experimental results show the system is effective and accurate by defining the normal and malignant behaviors with an accuracy rate of 100%, which is perfect. In future work we can utilize another technique for designing an intelligent detection system or perhaps use another dataset for evaluating the proposed system.

## References

[1] HE, D., CHAN, S., and GUIZANI, M. (2016) Communication security of unmanned aerial vehicles. *IEEE Wireless Communications*, 24 (4), pp. 134-139.

[2] CHOUDHARY, G., SHARMA, V., YOU, I., YIM, K., CHEN, I.R., and CHO, J.H. (2018) Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey. In: *Proceedings of the 14th International Wireless Communications and Mobile Computing Conference, Limassol, June 2018*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 560-565.

[3] VAIDYA, V. (2001) *Dynamic signature inspection-based network intrusion detection*. Google Patents.

[4] TSENG, C.-Y., BALASUBRAMANYAM, P., KO, C., LIMPRASITTIPORN, R., ROWE, J., and LEVITT, K. (2003) A specification-based intrusion detection system for AODV. In: *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, Virginia, October 2003*. New York: Association for Computing Machinery, pp. 125-134.

[5] PATCHA, A. and PARK, J.-M. (2007) An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51 (12), pp. 3448-3470.

[6] AYDIN, M.A., ZAIM, A.H., and CEYLAN, K.G. (2009) A hybrid intrusion detection system design for computer network security. *Computers & Electrical Engineering*, 35 (3), pp. 517-526.

[7] SAIFUDDIN, K.M., BIN ALI, A.J., AHMED, A.S., ALAM, S.S., and AHMAD, A.S. (2018) Watchdog and Pathrater Based Intrusion Detection System for MANET. In: *Proceedings of the 4th International Conference on Electrical Engineering and Information & Communication Technology, Dhaka, September 2018*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 168-173.

[8] ALI ALHEETI, K.M., AL-ANI, M.S., and MCDONALD-MAIER, K. (2019) Spreading Code Identification of Legal Drones in IoT Environment. In: *Proceedings of the 8th International Conference on Emerging Security Technologies, Colchester, July 2019*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 1-6.

[9] BATS (2019) *Ground-to-Air Tracking*. [Online] Available from: http://www.extendingbroadband.com/aerial-tracking/ground-to-air-tracking/ [Accessed 05/09/19].

[10] HE, D., QIAO, Y., CHAN, S., and

GUIZANI, N. (2018) Flight Security and Safety of Drones in Airborne Fog Computing Systems. *IEEE Communications Magazine*, 56 (5), pp. 66-71.

[11] DIMC, F. and MAGISTER, T. (2006) Mini UAV communication link systems. In: *Proceedings of the International Conference on Traffic Science*.

[12] OUBBATI, O.S., LAKAS, A., ZHOU, F., GÜNEŞ, M., LAGRAA, N., and YAGOUBI, M.B. (2017) Intelligent UAV-assisted routing protocol for urban VANETs. *Computer Communications*, 107, pp. 93-111.

[13] ASHA, G.R., VAIDHEHI, V., CEDRIC, T., and BALAJI, S. (2015) A Review of Routing Protocols for Airborne Networks. *International Journal of Innovative Research in Advanced Engineering*, 2 (3), pp. 5-10.

[14] HAYAT, S., YANMAZ, E., and MUZAFFAR, R. (2016) Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Communications Surveys & Tutorials*, 18 (4), pp. 2624-2661.

[15] MNS LABORATORY (n.d.) *Drone Detection Project*. [Online] Available from: http://mns.ucdenver.edu/DroneDetectionProject.html [Accessed 11/10/19].

[16] LI, W., YI, P., WU, Y., PAN, L., and LI, J. (2014) A new intrusion detection system based on KNN classification algorithm in wireless sensor network. *Journal of Electrical and Computer Engineering*, 2014, 240217.

[17] STACK EXCHANGE (2020) *Why do you need to scale data in KNN*. [Online] Available from: https://stats.stackexchange.com/questions/287425/why-do-you-need-to-scale-data-in-knn [Accessed 23/12/19].

[18] MOSTAFA, S.A., MUSTAPHA, A., RAMLI, A.A., DARMAN, R., ZEEBAREE, S.R.M., MOHAMMED, M.A., GUNASEKARAN, S.S., and IBRAHIM, D.A. (2019) Applying Trajectory Tracking and Positioning Techniques for Real-time Autonomous Flight Performance Assessment of UAV Systems. *Journal of Southwest Jiaotong University*, 54 (3). Available from http://jsju.org/index.php/journal/article/view/285.

[19] OUBBATI, O.S., LAKAS, A., ZHOU, F., GÜNEŞ, M., LAGRAA, N., and YAGOUBI, M.B. (2017) Intelligent UAV-assisted routing protocol for urban VANETs. *Computer Communications*, 107, pp. 93-111.

[20] MARTI, S., GIULI, T.J., LAI, K., and BAKER, M. (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, New York, August 2000*. New York: Association for Computing Machinery, pp. 255-265.

[21] ASAJU, L.B., SHOLA, P.B., FRANKLIN, N., and ABIOLA, H.M. (2017) Intrusion Detection System on a Computer Network Using an Ensemble of Randomizable Filtered Classifier, K-Nearest Neighbor Algorithm. *FUW Trends in Science & Technology Journal*, 2 (1), pp. 550-553.

## 参考文:

[1] D. D.，CHAN。S. 和 GUIZANI，M.（2016）无人机的通信安全。电气工程师学会无线通信，24（4），第 134-139 页。

[2] CHOUDHARY，G.，SHARMA，V.，您，I.，YIM，K.，CHEN，I.R. 和 CHO，J.H.（2018）网络无人飞行器入侵检测系统：一项调查。于：2018年6月在利马索尔举行的第14届国际无线通信和移动计算会议论文集。新泽西州皮斯卡塔维：电气与电子工程师协会，第 560-565 页。

[3] VAIDYA，V.（2001）基于动态签名检查的网络入侵检测。谷歌专利。

[4] TSENG，C.-Y.，BALASUBRAMANYAM，P.，KO，C. LIMPRASITTIPORN，R.，ROWE，J. 和 LEVITT，K.（2003）一种基于规范的AODV入侵检测系统。在：2003年10月在弗吉尼亚州费尔法克斯举行的第一届ACM临时和传感器网络安全性ACM研讨会论文集。纽约：计算机协会，第 125-134 页。

[5] PATCHA，A。和 PARK，J.-M。（2007）异常检测技术概述：现有解决方案和最新技术趋势。计算机网络，51（12），第 3448-3470 页。

[6] AYDIN，MA。，ZAIM，A.H。和

CEYLAN，K.G。（2009）一种用于计算机网络安全的混合入侵检测系统设计。计算机与电气工程，35（3），第 517-526 页。

[7] SAIFUDDIN，K.M.，BIN ALI，A.J.，AHMED，A.S.，ALAM，S.S。和 AHMAD，A.S。（2018）用于移动网的基于看门狗和卑鄙者的入侵检测系统。在：第四届国际电气工程与信息与通信技术国际会议论文集，达卡，2018年9月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 168-173 页。

[8] ALI ALHEETI，K.M.，AL-ANI，M.S。和 MCDONALD-MAIER，K。（2019）物联网环境中合法无人机的代码识别。在：第八届新兴安全技术国际会议论文集，科尔切斯特，2019年7月。新泽西州皮斯卡塔维：电气和电子工程师协会，第 1-6 页。

[9] 打击（2019）地空跟踪。[在线]可从以下网站获得：http://www.extendingbroadband.com/aerial-tracking/ground-to-air-tracking/ [访问时间：19/05/09]。

[10] D. D.，QIAO。Y.，CHAN。S. 和 GUIZANI N.（2018）机载雾计算系统中无人机的飞行安全性和安全性。电气工程师学会通信杂志，56（5），第 66-71 页。

[11] DIMC，F. 和 MAGISTER，T.（2006）微型无人机通信链路系统。在：国际交通科学会议论文集。

[12] O.S. OUBBATI，A。LAKAS，周F.，M。GÜNEŞ，N. LAGRAA 和 M.B. YAGOUBI。（2017）适用于城市网络的智能无人机辅助路由协议。计算机通信，107，第 93-111 页。

[13] ASHA，G.R.，VAIDHEHI，V.，CEDRIC，T. 和 BALAJI，S.（2015）机载网络路由协议综述。国际先进工程创新研究杂志，2（3），第 5-10 页。

[14] HAYAT，S.，YANMAZ，E. 和 MUZAFFAR，R.（2016）民用无人机网络调查：一种传播观点。电气工程师学会通信调查与指南，18（4），第 2624-2661 页。

[15] MNS实验室（无注明）无人机检测项目。[在线]可从以下网站获得：http://mns.ucdenver.edu/DroneDetectionProject.html [已访问19/10/19]。

[16] LI，W.，YI，P.，WU，Y.，PAN，L. 和 LI，J.（2014）一种基于无线传感器网络中知识网络分类算法的新型入侵检测系统。电气与计算机工程学报，2014，240217。

[17] 堆栈交换（2020）为什么需要在知识网络中缩放数据。 [在线]可从以下网站获得：https://stats.stackexchange.com/questions/287425/why-do-you-need-to-scale-data-in-knn [访问日期：19/12/23]。

[18] S.A. MOSTAFA，A。MUSTAPHA，RAMLI，A.A.，DARMAN，R.，ZEEBAREE，S.R.M.，MOHAMMED，MA。，GUNASEKARAN，S.S。和 IBRAHIM，D.A。（2019）将轨迹跟踪和定位技术应用于无人机系统的实时自主飞行性能评估。西南交通大学学报，54（3）。可从 http://jsju.org/index.php/journal/article/view/285获得。

[19] O.S. OUBBATI，A。LAKAS，ZHOU F.，M。GÜNEŞ，N.LAGRAA 和 M.B. YAGOUBI。（2017）适用于城市网络的智能无人机辅助路由协议。计算机通信，107，第 93-111 页。

[20] MARTI，S.，GIULI，T.J.，LAI，K. 和 BAKER，M.（2000）缓解移动自组织网络中的路由异常。于：2000年8月在纽约举行的第六届年度移动计算和网络国际会议论文集。纽约：计算机械协会，第 255-265页。

[21] ASAJU，L.B.，SHOLA，P.B.，FRANKLIN，N. 和 ABIOLA，H.M.（2017）计算机网络上的入侵检测系统，使用可随机化的分类器组合，K最近邻算法。FUW科技趋势，2（1），第 550-553 页。