International Journal of Engineering & Technology, 7 (1.1) (2018) 371-376

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Secured dynamic path planning and multi-obstacle avoidance model for UAV networks

K. Prathyusha [1] *, A. S. C. S. Sastry [1]

[1] Department of E. C. E, K. L. University, Vaddeswaram, Guntur, A. P, India
**Corresponding author E-mail: prathyushakuncha@gmail.com*

Abstract

As the number of the obstacles are increasing along with the navigation paths, the security of the communication data also increasing exponentially in the dynamic UAV networks. A large number of path planning and obstacle avoidance models have been proposed on the static and dynamic UAV networks for data communication. Most of the traditional obstacle avoidance models are independent of security for communication data or path planning procedures. Since the UAV sensitive data are stored in each sensor along with the path planning information; there exists an unauthorized access or malicious access to the sensitive data from third party applications or users. Also, traditional standard cryptographic algorithms (both symmetric and asymmetric) are not efficient to provide complete security to vast amount of UAV data dynamically due to its high computational memory and time. In this paper, a novel trust based Ant Colony optimization model was proposed to secure the sensitive UAV data against unauthorized access. In this model, a novel cipher text policy based encryption and decryption procedure is used as an extension to KP-ABE for UAV path security. Experimental results proved that the proposed trust based optimization model is better than the traditional UAV security models in terms of computational time and memory.

Keywords: CP-ABE; KP-ABE; UAV; Path Planning; Obstacle Avoidance.

1. Introduction

Unmanned Aerial Vehicle (UAV) operations have essential factors namely safety and reliability. Due to their lower cost and dynamic path planning compared to other aircrafts, UAVs can be remotely controlled or competently programmed. Numerous fields such as scientific research, commercial services, and agriculture have seen the benefits of UAVs. UAVs have been widely applied in numerous disciplines. Prime Air was launched by Amazon in 2013. Prime Air is a new form of packaging and delivering with the help of UAVs. On the other hand, these UAVs are prone to attack as their communication security is not guaranteed since they use wireless networks. A notable amount of effort has been directed at improving and maintaining these features for daily UAV users. Unfortunately, cyber-security has only been recently recognized. An ArduinoLibs Crypto library, Galois embedded Crypto library and an openLRSng open source radio project are used in this project [1]. Some lessons learned during development, implementation, and testing will be made accessible so that users with a desire to utilize their encrypted link can contribute to our work There has been a keen eye on the security of both commercial consumer-grade UAVs and the open source UAVs from the regulators and manufacturers. On the other hand, it is unfortunate that very minor research has been done on software security and prevention of attacks who voluntarily gain control other's drones. This is probably as a result of the reality that most of the known accidents caused by drones owned by man-in-the-middle attacks due to operator error, malfunctioning of drone or by a combination of the two.

Cyber-security has only come to the limelight after contemporary events such as fear of US presidential elections credibility having been interfered with the Russian hackers, hacking of Democratic National Committee (DNC) and the massive denial of service attacks perpetrated by IoT devices. The conflict in Ukraine has been an event of great interest for UAV. Ukrainian military had to expend off the shelf products to fight against the Russian backed separatist's airborne surveillance. This demonstrates how simple it is to compromise operation or take up the control of the commercial UAV product. It is worth to note that the Ukrainian military realized from their mistakes and begun effecting communication security measures gained from military systems like specific operating procedures and encryption into their Do-It-Yourself (DIY) products. This proves the fact that small teams dedicated to hateful intentions can mess up with UAV [2].

It is vital to change the symmetric encryption keys regularly. This is quite possible for the intruder, and also the specific application of AES can have bugs that can be exploited by hackers. The safety link is not encrypted hence making it vulnerable. This has been witnessed after a link attack on a popular DSMx radio protocol. The attacker used a cheap microcontroller and software-defined radio protocol through the specific hardware setting. The other popular RC protocols are also vulnerable due to their similarity, and there are just a few different radio chips operating across the transmitters. A massive amount of time and resources will be required for this attack. This implies that the decryption must be initiated equally to the amount of power traces. In addition to this, the equipment is quite costly and also the software required to scrutinize the produced power traces is expensive. In the future, a lot of focus has to be put in the security of UAV from unauthorized access and external interference [3] [4].

Copyright © 2018 K. Prathyusha, A. S. C. S. Sastry. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1.1. ABE model

ABE is a method used in cryptography to enhance access control and data confidentiality simultaneously. It was originally proposed by Sahai and Waters [5]. Sahai and waters stated that a private decryption key for a given identity could only be used to decrypt a ciphertext with a matching identity. Its central focus is on the Identity-Based Encryption. In this, the identity is seen as a set of attributes. Collusion resistance is a vital feature of Attribute-Based Encryption. There are several schemes that have been generated as a result of ABE to address various access control problems. Sahai and Goyal improved the ABE scheme to increase efficiency to a finer access control system. Every ciphertext in this scheme is given a label by the encryptor together with an attribute set. Every private decryption key is related to the access structure [5]. The access structure defines the type of ciphertexts the key can decrypt. This scheme is referred to as Key-Policy Attribute-Based Encryption (KP-ABE) [13]. Another scheme is called Ciphertext-Policy Attribute-Based Encryption (CP-ABE). Attributes define user credentials in this scheme, and the encryptor has the right to determine the properties of the decryptor. Computation of the secret key is another issue. The key size can grow larger with an increase in the size of data user's attribute list. The user attribute list grows as the user accesses more services and this enables him to satisfy different access policies. The key size ought to be fixed without considering the size of the attribute list. This is also applicable to lightweight devices as the decryption key can be as small as 672-bits [6].

The public and military can use this fast developing technology of Unmanned Aerial Vehicles (UAVs) in their endeavours. For more than two and a half decades, the military has been making use of UAV for striking and attack, reconnaissance and border surveillance operations. Public utilization of this great technology has been seen in the transportation management, police and general public safety. They can be used for recovery operations in situations where there is a communication breakdown. UAVs can also be used in risky situations such as wildfires, poisonous gases, and wild animal tracking. This saves the human from the hazards of attending to this in person. But, traditional results from the simulations are only appropriate for a specific set of boundary conditions. Due to this, the user has to perform calculations for each possible specific condition.

The network structure of UAV networks is still unsecured due to the number and positions of nodes along with paths. This forces the links to be developed securely. This implies that some features of architectural design will not be inbuilt. The second challenge being posed is that the routing protocol can't be a straightforward realization of a reactive or a proactive scheme. Finally, traditional path planning models are not trusted against Man-in-the-Middle attacks.

In CP-ABE access tree structure is used to encode the data using the user specified gate operators such as AND, OR and NOT with attribute list. Similarly, in KP-ABE data encryption is performed using the user specified attribute list without the access tree structure. Unlike ABE (where both the cipher text and secret key are associated with attributes), in this model only cipher text are associated with attributes and secret keys are merged with monotonic access structures. KP-ABE model can gain access control and flexibility as compared to the conventional ABE model. The major flaw of this model is the algorithm does not control who can decrypt.

2. Related works

Shamir in 1985 came up with the IBE system. Key generation of this system has been an issue. As it stands now, no cryptographic systems can be comfortably changed into an IBE system. This includes the Diffie-Hellman protocol and RSA. Some solutions have been suggested for the system, although the computational requirements are still a headache to implement. There was a success in the year 2001 when a new approach called bilinear map was invented. The bilinear map is effective when generating keys and it is secure and precise.

Some descriptive attributes are used to label ciphertext and users in threshold access control. A user can only decrypt a ciphertext if the user attribute and those of the ciphertext label have over a given level of similarity. This thinking is fetched from Identity-Based Encryption IBE which perceives identities as strings of characters. This threshold provides room to accommodate course-grained access control schemes. It is normally used in biometric systems [7].

Data encryption is a popular way to ensure data security and privacy during data storage. In the CP-ABE, the decryption key is related to an attribute set while the encrypted text is related to the access rules. This means that the data can only be decrypted when the user has characteristics that match the access rules. KP-ABE is the inverse of CP-ABE. The user decryption key is related to the access policy while the encrypted data is related to a set of attributes. This implies that the user can only decrypt data whose set of attributes match the access policy related to the decryption key. Time is considered sensitive in many information processing systems.

For a long time, the security of both consumer grade UAV and the open source UAVs has been under a keen observation by the manufacturers and regulators. Unfortunately, there has been very minimal concentration on the security of the software used and the avoidance of deliberate hacking of drones with intent to cause evil. The results of these are manifested in the number of civilian drone accident being caused by operator error, faulty drones or a combination of the two. There has been a steady improvement of drone security over time. The WPA-2 encryption for Wi-Fi authentication is the one being used currently as opposed to the fail WEP key. An attribute is defined as a descriptive string in the CP-ABE context. An attribute is issued to an entity where every entity has the policy of having many attributes. This enables the encryptors to formulate policies of data access by using logical operators such as OR, AND, NOT etc. For decryption to occur, the attributes of the decryptor need to match with the access rules or policies.

The smaller the UAV network, the more the energy limitations. Since the nodes are dynamic, the network will have to frequently organize and reorganize itself raising a specific routing requirement. The routing protocols to be used need to be able to conserve energy to increase the UAV network service time.

2.1. Multi-UAV network

In the Multi-UAV network setup, there used to be a single aerial node and single or numerous ground nodes. It has been proven that multiple UAV systems working in coordination are more effective. A multi-UAV system is also cheaper, smaller and it works in a systematic manner. The communication network must provide security in many multi-UAV systems. The communication between UAVs themselves and between UAVs and ground nodes is paramount. Provision of service co-operatively and extending the network coverage area by relaying is achieved if the UAVs are configured. Differing from this, during UAV application in the agricultural field, they travel across large areas, and the links often break and rebuild in a unsecured way. The dynamic nature of path planning in UAV allows the system to periodically go out of service. This may be the result of power drainage or faulty UAV. Link disruptions are common phenomena in wireless networks. There are several factors that influence the extent of disruption in UAV. The disruption may be relative to the power transmitted, extraneous noise and inter-UAV distances and attack. Unfortunately, dynamic operations in UAV require high mobility with an increased chance of disruptions. Poor data link quality may result in delays in data transmission and path hijacking. Another cause of delayed data transmission could be a single or multiple UAV nodes storing the data are not available [8].

During asymmetric encryption, a public key is required for encryption and a private key is required for decryption. This ar-

rangement will generate a different communication channel between every UAV. There is a need for a secure central area for storing public keys to ensure security. The public keys will have to be centrally stored in a ground station or the UAVs. This asymmetric way of encryption is not suitable for static communications. Symmetric encryption has the advantage of being faster, and it operates perfectly within the swarm communication architecture. In symmetric encryption, the same key will be given to every UAV before a flight. The UAV system will, therefore, use one key to encrypt and decrypt [9].

There is an access structure that has leaf nodes that match with a data attribute. Interior nodes can be used as threshold gates. To explicitly define each user access privilege, the access structure needs to show complex expressions of logic over the attribute. There is a new PKC method referred to as Key-Policy Attribute-Based Encryption (KP-ABE) [13]. To begin with, it is efficient for data computation, storage, and communication operating cost at the sensor node. Ensuring secure data communication through the communication channels is the most crucial one in dynamic UAVs. UAVs frequently communicate with ground control, and this communication needs to be secure. This research proposes to use a system of cryptographic protection of path planning model. The UAV will communicate through encrypted signals [10].

3. Proposed model

In this proposed model, a novel trust based ACO model with encryption algorithm is implemented on dynamic path planning coordinates. Proposed model was implemented in three phases as shown in figure 1. In the first phase, UAV path planning is designed and implemented using A* algorithm [12]. In this phase, a novel multi-UAV's with dynamic path planning procedure is used for obstacle avoidance [11]. In the second phase, dynamic path planning coordinates are used to find the optimized trusted points using the ACO algorithm [10]. In this phase, user access control mechanism and data encryption operations are performed on the path planning coordinates against the Man-in-the-Middle attacks.

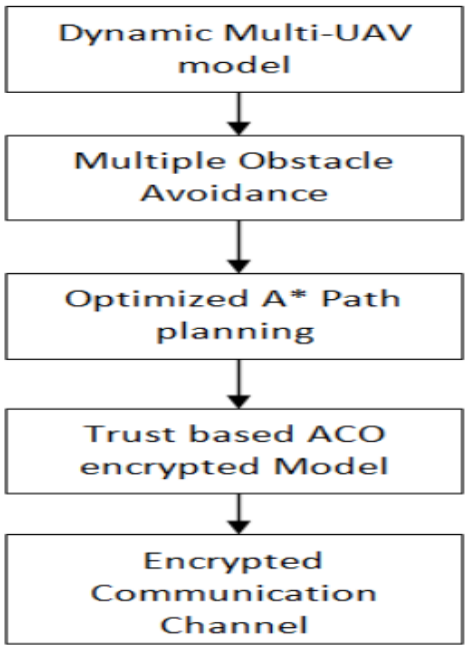

Fig. 1: Proposed Framework.

With the increasing numbers of UAVs, there is an essential requirement of both centralized and decentralized solutions in order to add extended path planning and obstacle avoidance solution to the flying objects. These two dimensional shapes can be transformed into a three dimensional shapes. UAV states are responsible for construction of an optimized path in order to map all the obstacles in real time. Horizontal position states have the responsibility to control the UAV while crossing those obstacles. It will in fact gather shape related information of obstacles from all directions. By integrating two vectors which are produced through weighting parameter is responsible for maintaining a safe distance from that obstacle. The heading angle of the UAV is responsible for preventing collision in the same direction of flight because of mapping. Besides this, a new optimized shortest path distance using nearest neighbor based KDTree is used for path optimization. The generated optimized path has the responsibility to map different shapes of complicated obstacles.

The main objective of the proposed model [11] is to increase the probability of arbitrary obstacle detection with optimal path planning procedure. There exist two different quality metrics in order to enhance the probability of path planning issues.

1) According to the search metric, a better path is detected which will increase the Cumulated Conditional Probability.
2) The path must be detected which can achieve better probability with minimum time interval.

The purpose of this model is to find an optimal navigation path against single or multiple dynamics obstacles using the mathematical objective function. As in the traditional models, as the number of static control points increases, the navigation path becomes more difficult and computationally complex to construct an optimal feasible path. In this proposed model, we optimized the dynamic obstacle avoidance mechanism to overcome the path navigational issues in UAV path planning and selection as shown in figure1.

The model has following assumptions.

- All the UAVs have multiple targets in parallel.
- Each source station consists of at least one task in parallel mode.
- All the UAVs have speed v with the different altitude.
- All the UAVs have the maximum flight time.

3.1. Proposed trust based ACO encrypted model

Key Policy Attribute-Based Encryption Model

This is an extended version of traditional model of ABE. Here users are associated with access tree and nodes of these access trees are represented by threshold gates. Attributes are denoted by the leaf nodes. Initially the secret keys of each individual user are defined. Unlike ABE (where both the cipher text and secret key are associated with attributes), in this model only cipher text are associated with attributes and secret keys are merged with monotonic access structures. These components as a whole control the cipher texts in decryption process. The said model is implemented in one-to-many communications.

Trust based ACO Path planning model using improved KPABE

ACO path planning model was used to solve the shortest path planning in multi-UAV dynamic path planning process. Ant Colony Optimization (ACO) was discovered and introduced by M. Dorigo [14] as a Nature-Inspired meta-heuristic for providing optimal solutions to hard combinatorial optimization (CO) problems. Real Ants are highly sophisticated and intelligent swarms to find the shortest path from food source to nest by depositing pheromone on the ground and laying the trails so that other ants can follow. The most important component of ACO Algorithms is the combination of a priori information regarding the structure with a posteriori information about the structure of previously obtained optimal solutions. In order to determine the shortest path, a moving ant lay the pheromone which acts as base for other ants to follow and deciding the high probability to follow it. As a result, it leads to the emergence of collective behaviour and forms a positive feedback loop system through which other ants can follow the path and makes the pheromone more stable and best path for transferring the food back to nest. Pheromone lays the foundation for communication medium for other ants to follow the way and go to the food source. When other ants follow the path, the quantity of pheromone increases on that particular path. The rich the

quantity of pheromone along the path, the more likely is that other ants will detect and follow the path.

Step1: Initialization of ACO parameters Phi ∈ [0,1], rho ∈ [0,1],, alpha, beta, #antnodes, #iterations, source node sn, neighbornode nn, pheromones, MAX_PHEROMONE=1, MIN_PHEROMONE= 0.001, initialize all ant solutions to false.

Step 2: For each node in #antnodes
Do

Build path to the neighbor nodes until best solutions found.

Initialize best ant solutions to true.

Node-pheromone (value) = Math. Min (MAX_ PHEROMONE, Math.max (MIN_ PHEROMONE, value));

Node Heuristic = 1/ distance (sn, nn);

$$distance(sn, nn) = \sqrt{(sn.x - nn.x)^2 + (sn.y - nn.y)^2}$$

$$Newnnode(\alpha, \beta) = \text{currentNode.getPheromone(neighbour)}^{\alpha^2} * \text{currentNode.getHeuristic(neighbour)}^{\beta^2}$$

Compute node trust probability using the following equation to each node as trust initialization.

$$\text{trustprob} = \text{Math.pow(currentNode.getPheromone(neighbour)}, \alpha^2) * \text{Math.pow(currentNode.getHeuristic(neighbour)}, \beta^2);$$

Done

Step 3: Extract all the dynamic paths generated from source node to destination node using improved KNN based A* path planning algorithm [2].

Step 4: Build ant best paths using local pheromone updation and global pheromone updation.

$$\omega = (1 + (1\text{-phi})*(1\text{-npheromone})*\text{nheuristic})*\text{npheromone};$$

Local_update (nnode, neighborpheromone, neigbhorheuristic, phi)

$$= (1\text{-phi})*(\text{npheromone}) + (\text{phi}*(\omega))$$

$$\upsilon = (1 + \text{npheromone}*\text{nheuristic}*\text{maxGlobal})*\text{npheromone};$$

global_update (nnode, neighborpheromone, neigbhorheuristic, phi)

$$= (1\text{-rho})*(\text{npheromone}) + (\text{rho}*(\upsilon))$$

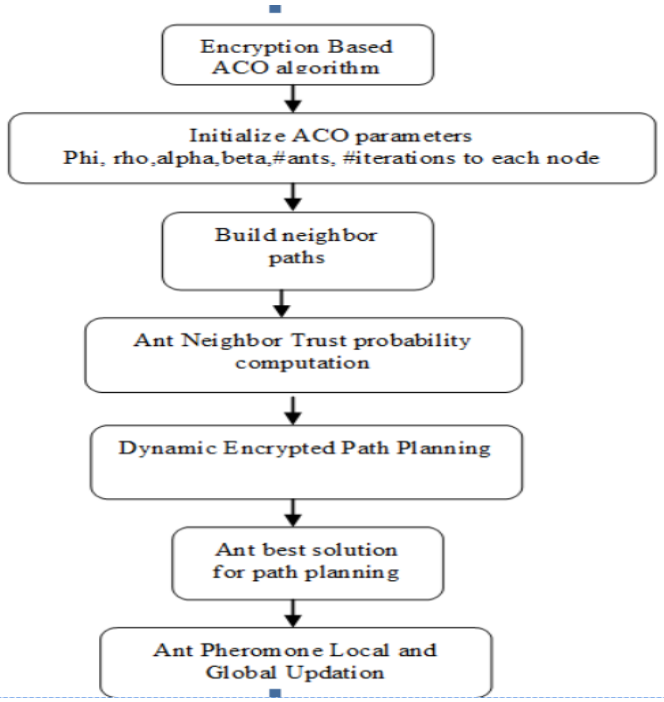

Fig. 2: Encrypted Trust Based ACO Algorithm

Monotonic access structures don't allow the user to give negative attributes while denying particular users decryption rights. Cipher-text policy and key policy are monotonic access structures. Non-monotonic access structures allow the addition of NOT term to better the correctness of the access structure and manage flexibility. The downside of this being, there may be so many negative attributes hence making server get overpowered
Definitions:
The elementary model is derived from KPABE that has KeyGen, setup, encrypt and decrypt algorithms. These are the four common modules in most ABE schemes although each one of them has its formula.
Setup:
Bilinear mapping is first stated. A security parameter k that shows the magnitude of the attribute set as input. It then comes up with a Master key (MK) and a public key (PK) at the end of the processing.
Let G be the bilinear group with prime order p and generator k, which satisfies bilinear property and non-degeneracy property such that θ_1, $\theta_2 \in G_p$ which are relative large primes to MD5 (path[i])/i $\in$ i^{th} optimal path.
The public key and master key can be generated as

$$PublicKey\ (Pk) = \{\text{MD5(trustprob(path))}, G_p, \text{k}, \text{m} = k^{\theta_2}, n = k^{1/\theta_2}, e(\text{k},\text{k})^{\theta_1}\}$$
$$MasterKey\ (Mk) = \{\theta_2, \text{k}^{\theta_1}\}$$

Encrypt:
In threshold policy, the input comprises the plain text M which is given to the encryption algorithm together with attributes S' and the algorithm outputs ciphertext . For ciphertext policy, the input comprises the message M, the PK, and the access tree T, where C is the cipher text.

$$CipherText\ (C) = \{\text{C}^1 = M\ e(\text{k},\text{k})^{\theta_1 \cdot r}, T, C^2 = m^r,$$
$$forall\ \text{x} \in \text{X}: \text{C}_x = k^{q(x,0)}, C^1_x = H(A(\text{x}))^{q(x,0)}$$

KeyGen:
A secret key is generated by a threshold access policy. The key comprises of concepts of user's attribute set S. The KeyGen takes the access tree AT, and MK as input for features key policy. It then generates the user's secret key (SK).

$$\mathbf{SecretKey}(\mathbf{Sk}) = \{D^{'} = k^{(\theta_i + rand)/\theta_2}, D(j) = k^{rand*H(j),rand_j}, D^{'}(j) = \mathrm{k}^{rand_j}\}$$

Decrypt:
The decryption function takes the ciphertext CT, and the user's SK as input, and generates a message M or null if it is not granted access.
To decentralize authority schemes to guide all authorities for a global environment, another algorithm Global Setup is required. It shares a setup algorithm structure with the one in centralized authority scheme. It is utilized in authority set up. With the addition of at least one parameter into the system as a result of each additional feature, makes the system multifaceted hence loss of performance features.

4. Experimental results

The main objective of every access control mechanism is to restrict the actions of users or programs run on behalf of users. The process of access control generally depends on other security measures of a computer system. Access policies are enforced by a reference monitor that considers all attempted access of a user. In the UAV path planning, each path is encrypted against third party attacks using the public key cryptography. Traditional Public-key approaches generally depends upon computationally hard problems like integer factorization, discrete logarithm, and elliptic curve relationships. Attribute based encryption models are computationally easy for dynamic data in order to construct their own policies and access control keys. These keys are generally used in the process of encryption and decryption.
In this section, we present the experimental results behind our dynamic path planning UAV model for polygon obstacle avoidance. First, we represent the experiment results, then we show the performance analysis. The proposed results are all simulated in Java IDE, on an Intel Core i5-4210U with 2.40GHz, 8GB RAM.

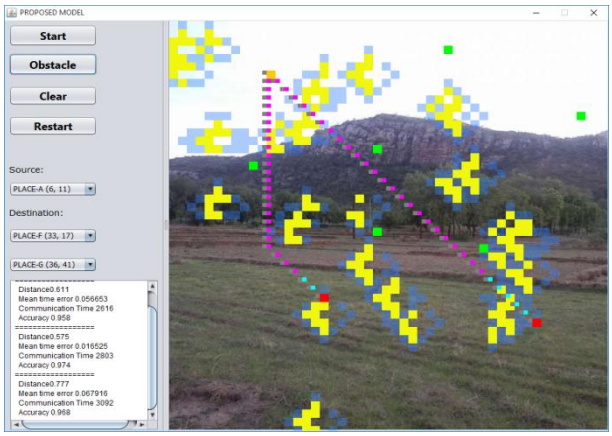

Fig. 3: Proposed Path Planning Model with Dynamic Multi-Source Uavs.

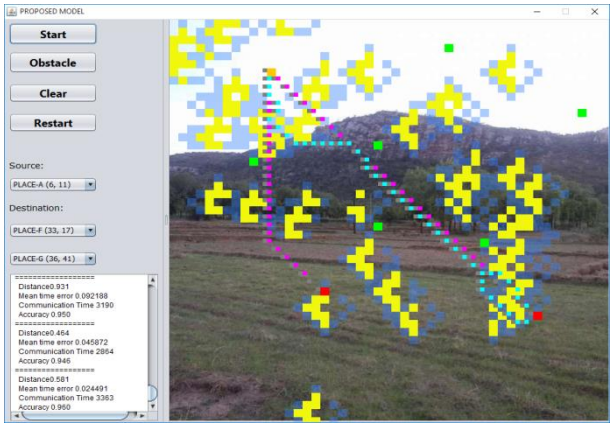

Fig. 4: Different Arbitrary Shaped Obstacles and Path Reconstruction Process.

[{19, 22}, {18, 22}, {17, 23}, {17, 24}, {18, 25}, {19, 25}, {20, 25}, {21, 25}, {22, 25}, {23, 25}, {24, 24}, {25, 23}] Final list.

UAV Path

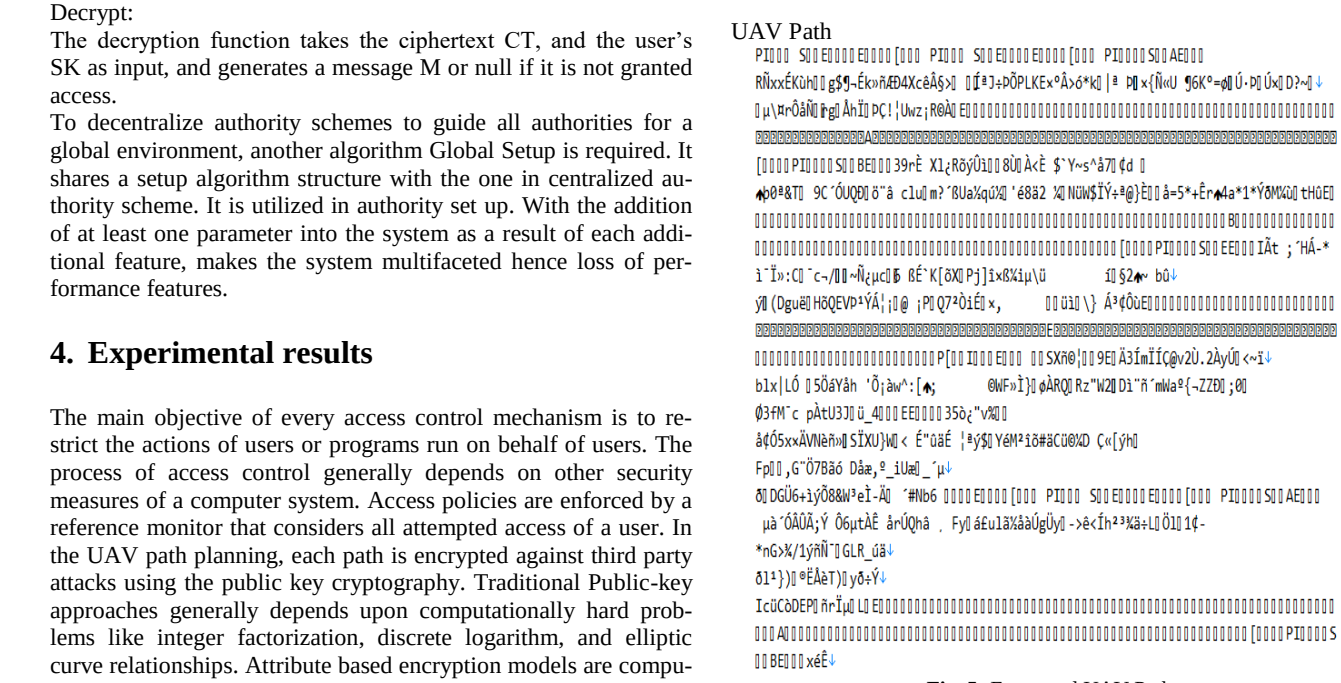

Fig. 5: Encrypted UAV Path.

Table 1: Computational Time of the Proposed Model to the Existing Models in Dynamic UAV Networks

Path Size(Bytes)	PSOABE(ms)	ACOABE(ms)	ACOKPABE(ms))
#200.0	1126.275	1029.969	903.718
#400.0	2122.248	1909.029	1710.897
#600.0	3104.469	2881.353	2477.658
#800.0	3455.351	3338.581	2772.473
#1000.0	4703.512	4358.171	4116.425
#1200.0	6100.984	5617.482	5006.427
#1400.0	6464.452	5971.704	4962.607
#1600.0	7568.933	6820.921	5850.339
#1800.0	8219.665	7817.188	6894.13
#2000.0	9354.092	8541.363	7439.246
#2200.0	9893.062	9303.667	8345.502
#2400.0	11371.586	10288.477	9393.282
#2600.0	12191.181	11321.393	9812.91
#2800.0	12707.367	11355.941	10497.402
#3000.0	12905.019	12508.575	10562.052
#3200.0	14084.897	13234.111	11712.498
#3400.0	14570.503	13800.584	11714.397
#3600.0	15942.461	15132.31	13968.631
#3800.0	16327.583	15911.543	14771.38
#4000.0	17671.673	16674.593	15515.529
#4200.0	18547.951	18217.657	14822.885
#4400.0	19886.806	17792.155	15722.084
#4600.0	20922.115	19110.817	18216.396
#4800.0	21071.717	19702.794	17972.343
#5000.0	21549.237	20037.163	18630.536

Table 1, illustrates the performance of the proposed model to the traditional security algorithms on UAV networks. From the table, it is observed that proposed model has less time computation compared to the traditional models. Using statistical P value and test statistics, null hypothesis is rejected and alternative hypothesis is accepted in all the cases, we can conclude that proposed model is better than traditional ABE models in terms of data encryption and decryption average time.

Table 2: Average Trust Probability of the Proposed Model to the Existing Models

Obstacles	PSOUAV	GeneticUAV	ABCUAV	ACOUAV
5	0.87	0.91	0.945	0.987
10	0.889	0.932	0.935	0.9882
15	0.83	0.918	0.952	0.9794
20	0.908	0.932	0.9423	0.9792
25	0.86	0.912	0.9524	0.9814

5. Conclusion

In this paper, a novel security based ACO path planning model was implemented on dynamic UAV networks against third party attacks. Since the UAV sensitive data are stored in each sensor along with the planning path information; there exists an unauthorized access or malicious access to the sensitive data from third party applications or users. Also, traditional standard cryptographic algorithms (both symmetric and asymmetric) are not efficient to provide complete security to vast amount of UAV data dynamically due to its high computational memory and time. In this paper, a novel trust based Ant Colony optimization model was proposed to secure the sensitive UAV data against unauthorized access. Experimental results proved that the proposed trust based optimization model is better than the traditional UAV security models in terms of computational time and memory.

References

[1] Podhradsky, M., Coopmans, C. and Hoffer, N. (2017). "Improving communication security of open source UAVs: Encrypting radio control link", International Conference on Unmanned Aircraft Systems (ICUAS), (2017). https://doi.org/10.1109/ICUAS.2017.7991460.

[2] P.M. Dames, M. Schwager, D. Rus, V. Kumar, "Active magnetic anomaly detection using multiple micro aerial vehicles", IEEE Robot. Autom. Lett. 1 (1) (2016), pp.153–160, https://doi.org/10.1109/LRA.2015.2511444.

[3] J.V. Carroll, "Vulnerability assessment of the US transportation infrastructure that relies on the global positioning system", J. Navig. Vol.56, no.2, (2003), pp.185–193, https://doi.org/10.1017/S0373463303002273.

[4] K.Prathyusha, A.S.C.S.Sastry, K. Sreenivasa Ravi, "UAV Shortest Path Planning& Collision-Free Path: A Review", Journal of Advanced Research in Dynamical and Control Systems, Special Issue – 2,(2017), pp.72-83.

[5] Q. Huang, Y. Yang and M. Shenc, "Secure and efficient data collaboration with hierarchical attribute based encryption in cloud computing ", Future Generation Computer Systems, (2016), pp.1-28, https://doi.org/10.1016/j.future.2016.09.021.

[6] X. Liu, Q. Liu, T. Peng and J. Wu, "Dynamic Access Policy in Cloud- Based Personal Health Record (PHR) Systems", Preprin submitted to Information Sciences, (2016), pp. 1-39, https://doi.org/10.1016/j.ins.2016.06.035.

[7] V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, K. R. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment", Preprint submitted to Elsevier, (2016), pp.1-10,

[8] D. McCallie, J. Butts, R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system", Int. J. Crit. Infrastruct. Prot, Vol. 4, no.2, (2011),pp: 78–87, https://doi.org/10.1016/j.ijcip.2011.06.001.

[9] Kumar, P., Vijay, S. and Devaraj, D. "A hybrid colony fuzzy system for analyzing diabetes microarray data". IEEE Symposium on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB), Singapore, (April 2013), https://doi.org/10.1109/CIBCB.2013.6595395.

[10] Y. Kuwata, M.T. Wolf, D. Zarzhitsky, T.L. Huntsberger, "Safe maritime navigation with COLREGS using velocity obstacles, in: Intelligent Robots and Systems (IROS)", IEEE/RSJ International Conference, (2011), pp. 4728–4734, https://doi.org/10.1109/IROS.2011.6094677.

[11] K.Prathyusha, A.S.C.S.Sastry, M.Chaitanya Suman, "Dynamic Route Planning and Obstacle Avoidance Model for Unmanned Aerial Vehicles", International Journal of Pure and Applied Mathematics, Vol. 116, No. 24, (2017), pp: 315-329.

[12] K.Prathyusha, A.S.C.S.Sastry, M.Chaitanya Suman, "Dynamic Constraint Based Multi-Route Planning And Multi-Obstacle Avoidance Model For Unmanned Aerial Vehicles", Journal of Advanced Research in Dynamical and Control Systems Vol. 9, no. 1, (2017), pp: 348-361.

[13] Parmar Vipul Kumar J , RajaniKanth Aluvalu "Key Policy Attribute Based Encryption (KP-ABE): A Review", International Journal of Innovative and Emerging Research in Engineering, Vol. 2, no. 2, (2015),pp:49-52.

[14] Dorigo, M., Maniezzo, V., & Colorni, A. "Ant system: Optimization by a colony of cooperating agents". IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), Vol. 26,no.1, (1996), pp: 29-41, https://doi.org/10.1109/3477.484436.