An Architecture to Secure (UAV) Cluster Communication

Mr Richard Joseph[1], Ms. Sreevidya Iyer[2], Ms. Anjali Nambiar[3], Ms. Purva Badgujar[4], Ms. Dhanashree Shetty[5]

[1]Assistant Professor, Vivekanand Education Society's Institute of Technology (VESIT), Mumbai, India [2]Department of Computer Engineering, Vivekanand Education Society's Institute of Technology (VESIT), Mumbai, India [3]Department of Computer Engineering, Vivekanand Education Society's Institute of Technology (VESIT), Mumbai, India [4]Department of Computer Engineering, Vivekanand Education Society's Institute of Technology (VESIT), Mumbai, India [5]Department of Computer Engineering Vivekanand Education Society's Institute of Technology (VESIT), Mumbai, India

[1]richard.joseph@ves.ac.in [2]2017.sreevidya.iyer@ves.ac.in [3]2017.anjali.nambiar@ves.ac.in [4]2017.purva.badgujar@ves.ac.in [5]2017.dhanashree.shetty@ves.ac.in

***Abstract*—UAVs are being increasingly used in military and commercial areas alike. They often carry sensitive information making them vulnerable to cybersecurity attacks. Potential security vulnerabilities may also exist in the modules used for functioning of the drone, for example, by launching a GPS spoofing attack or WIFI attack, adversaries can get hold of important information. RF signals are used to control UAVs, but this does not work for clusters. Hence, we use wireless networking for UAV clusters. We use the WIFI module for this, but this, too, has vulnerabilities. In this paper, we have attempted to strengthen the security layer for UAV communication by exploring various security threats.**

***Keywords*— drone security, UAV, cluster communication, IBOOS protocol, iot security**

1. Introduction

UAVs (Unmanned Aerial Vehicle) are aircrafts that can fly without the requirement of a human on board. Operators or computer systems remotely control UAV flight both on and off board. With advances in computing, communication, UAVs could also include other flying objects such as quadcopters, balloons, and gliders. Historically, UAVs were used for high-stakes situations such as military operations. Applications of UAVs have been expanded to civilian domains more and more recently. Operations such as search, rescue in human unreachable areas or otherwise are performed by drones. During sensitive missions, UAVs need to collect, process, and transmit a wide range of data which need to be secure. This also opens the UAVs up to cyber attacks, manipulation, and theft.Moreover, wireless sensor networks (WSNs) of UAVs have several potential applications. For all these critical applications, real-time data access is needed by an authorized user (external party) from some designated sensor nodes directly. Thus, user authentication is needed for securing WSNs. To provide a more flexible distributed authentication scheme, we have adapted a clustering heuristic for security requirements and then developed a cluster-based authentication scheme for large adhoc networks. In this framework, there are multiple independent CA services in a network. Different authentication schemes can be separately and locally employed in individual clusters, and independently configured for various factors like the trust relationships among nodes, the membership dynamic, the node density, mobility speed.. Each cluster is like an encapsulated object with some public interfaces like the public key of its own authentication service, the cluster head, and some gateway nodes connecting to other clusters. The certificates locally issued within a cluster may be verified anywhere within the cluster or among clusters and the compromise or failures of any individual CA service does not affect other clusters. Furthermore, because our approach exploits a more utilized flooding-based scheme, this cluster-based framework, which will be more robust and secure, can be efficiently built without depending on ad hoc routing protocols. Referring to a terrorist activity from 2009, unencrypted video recordings from UAVs can be accessed using tools like SkyGrabber. Hence, sensitive UAV information is prone to unauthorized usage. Due to weak security measures in UAV communications legitimate access to necessary services could be blocked by Denial-of-Service (DoS) attacks. In this paper, we have taken into consideration an ad hoc network between UAVs in this paper, which will have a master-slave cluster architecture, with one node acting as master. We focus on enhancing both inter and intra cluster communication security. Here we will give an overview of various attacks that can be performed on swarm of drones (wireless network), their simulation on gns3 software and develop the protocols to secure the communication network.

2. Literature Survey

'*Secure and efficient data transmission for cluster-based wireless sensor networks*' [1]

This paper deals with securing cluster based wireless network sensors. It proposes two protocols (Secure and Efficient data transmission) SET-IBS (Identity based digital signatures), SET-IBOOS (identity based online/offline digital signatures) schemes. These protocols solve the orphan node problem which exists in LEACH protocol.Orphan node problem occurs when a particular node doesn't share its pairwise key with any other node so the node becomes orphan and does not belong to any cluster.

Also these protocols work well against passive, active as well as node compromising attacks, IBS comprises the following operations - set up at the BS(base station), key extraction and signature signing of the data sending nodes and verification of the data receiving nodes. IBOOS comprises offline and online signatures in addition to the operations as in IBS. These protocols have better performers than the existing secure protocols for CWSNs.Considering the effectiveness of these protocols, SET-IBOOS will be incorporated in our proposed system.

'*Design and Analysis of Secure lightweight remote User authentication and key agreement scheme in internet of drones deployment*'[2]

This paper proposes a new signature-based authentication key establishment scheme in Iot environment,where the real time data access from Iot sensing devices by an authorized user is needed.This scheme only uses the efficient one-way cryptographic hash functions and bitwise XOR operations.The following are the phases of the scheme-

1) pre deployment

2) user registration (external)

3)login

4) authentication and key agreement

5) password and biometric update

6) dynamic drone addition

7)drone key management.

This systematic layout has been an influence for the proposed architecture.

'*A secure group of communication architecture for a swarm of autonomous unmanned aerial vehicles*.'[3]

This thesis focuses on securing group communication in an autonomous UAV swarm. This is rendered by incorporating the Hubenko architecture which develops a multicast secure group communication architecture for low earth orbit satellite networks in the global information grid.

Multicast groups are divided into clusters based on the physical location of its members. Using Iolus framework,all the clusters are independent and each cluster has its own group leader and SEK(session encryption key).In case a new member joins or leaves the cluster,only the affected cluster needs to rekey.Each cluster is managed by cluster leader, GSA(group security agent).

The cluster leaders communicate with each other to bridge local multicast traffic.At the top of the hierarchy,the group security controller manages all the cluster leaders and overall security of the group.The basic framework of Hubenko architecture is formed by combining features of spatial clustering and Iolus.

This paper has enabled us to understand the various concepts and technicalities of cluster based systems like GSC(Group Security Controller),Cluster leaders and cluster members and their roles in the system.

3. Proposed Solution

Network Architecture:

- Wireless network between drones.
- Swarm (Cluster of Drones) contains one cluster head (leader) and leaf nodes. There will be one base station which controls the cluster.
- Leaf nodes will transmit data to the base station via cluster head.
- Cluster head performs 2 operations

1. Data Transmission
2. Data Processing

- Data transmission is costlier than processing in terms of energy consumption.

- To avoid quick energy consumption and to balance energy consumption we use LEACH (Low Energy Adaptive Clustering Hierarchy) Protocol.

- LEACH rotates Cluster Head (CH) among all sensor nodes.

❖ Security Threat:

- Since wireless networks have been used, LEACH protocol is quite vulnerable.

- Attackers can attack CH or leaf nodes and pretend to be cluster heads or leaf nodes.

- Attackers can create orphan nodes from the network which will consume even more energy.

- Three type of attacks are possible:

    1. Passive Attack : Attackers are able to perform eavesdropping at any point of the network. Thus they can undertake traffic analysis based on eavesdropped messages.

    2. Active Attack : Attackers can modify the message. They are able to perform attacks like bogus and replayed routing information attack, sybil attack, HELLO Flood attack, wormhole attack, sinkhole attack etc.

    3. Node Compromising Attack : Attackers can hack the nodes and can access secret information like keys. They can even change the inner state and behaviour of a particular node.

ATTACKS	SOLUTION
DDOS	Black Hole Routing, Rate Limiting,Web Application Firewall
MITM	Employ Encryption,Verify TLS/SSL Setups
Sybil attack	Raise the cost to create a new identity,chain of trust,unequal reputation
Wormhole Attack	Reply Count-based Approach,WARP,Guard node based approach
Sinkhole attack	Routing Algorithms,Utilizing an IDS(intrusion Detection System)

- Aim is to protect LEACH protocol from such attacks.

❖ Protocols for secure and efficient message transfer:

- Key distribution is a method of providing security for such networks.

- As no. of orphan nodes increase , no. of CHs increase results into increase in energy consumption.

- Symmetric key distribution is an inadequate method hence we use asymmetric key distribution methods.

- There are two protocols that can secure message transfer between nodes :

1. SET-IBS (Identity Based Digital Signature)[1]

2. SET-IBOOS (Identity Based Online/Offline Digital Signature)[1]

- SET-IBS uses the Diffie Hellman method whereas SET-IBOOS uses a discrete logarithm method for security.

- Since SET-IBOOS uses a discrete logarithm method it reduces computational overload. Hence we prefer this protocol over SET-IBS.

- We authenticate the encrypted sensed data by applying digital signature.

- Following steps are performed in SET-IBOOS Protocol:

  1. Set Up : Base station generates a master key and public parameter for private key generation for leaf nodes.

  2. Extraction : Sensor nodes generate private keys.

  3. Offline signing : from

     Public key and timestamp , cluster head creates

     offline signature and shares it with all the leaf nodes.

  4. Online Signing :

     From private key , message and offline signature sender generates online signatures.

  5. Verification : At the receiver's end , it accepts or rejects the message from given ID and online signature.

- This is how SET-IBOOS protocol can perform secure transmission of messages.

❖ Advantages :

I. Network Lifetime

II. No. of Alive nodes

III. Total system energy consumption

In our proposed architecture,we plan to include the SET-IBOOS protocol. The main idea of the SET-IBOOS protocol is to authenticate the encrypted sensed data, by applying digital signatures. To enhance the security, the architecture includes various phases as shown in Fig.1:

❖ Pre-deployment phase-

In the pre-deployment phase, the Ground Control Station is responsible for registering each drone DRj prior to its deployment in the IoD environment.

❖ Authentication and Key agreement-

For the authentication and key agreement phase, SET-IBOOS [Ref 1] protocol will be implemented.

❖ Dynamic Drone Addition-

For Dynamic Drone Addition, rekeying of only that subgroup will be performed where a drone is joining or leaving, thus reducing the overall energy consumed for rekeying the entire cluster.

❖ Drone Key Management system-

In the drone key management system, a drone may want to share its information with some other drone. In that situation, we need a secure communication link between these drones. For this purpose, we need a pairwise key establishment between two neighbouring communicating drones [2].

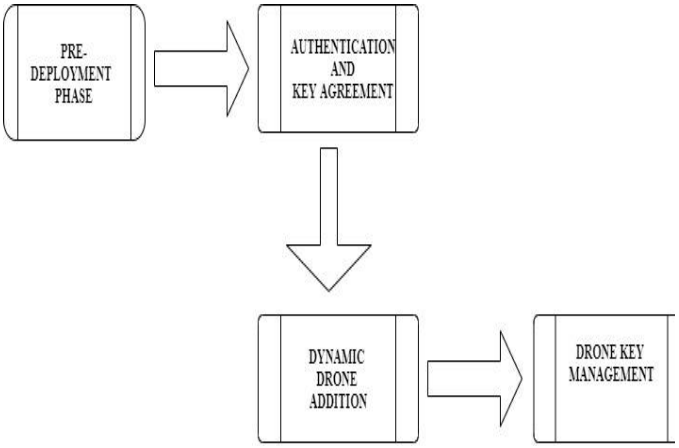

Fig.1

Conclusion:

Wireless network communication is required to work with clusters, but it is not secure enough. To achieve security, in this paper, we have proposed an architecture which includes the SET-IBOOS protocol for authentication & key agreement, pre-registration of drones before deployment, pairwise key establishment for drone communication and other methods to avoid unnecessary energy consumption such as rekeying subgroups instead of the cluster entirely in case of dynamic drone addition.

We chose the SET-IBOOS protocol owing to the following factors-

- Asymmetric key management - providing better security
- Low storage cost compared to the previous protocols
- Better neighbourhood authentication
- Smaller message size (46 Bytes - compared to 64 bytes in SET-IBS)

References:

[1]. Huang Lu, Jie Li and Mohsen Guizani ,"Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks",IEEE Transactions on Parallel and Distributed Systems,vol. 25,no. 3,March ,pp. 750-761,2014.

[2]. Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V. Vasilakos and Joel J. P. C. Rodrigues,,"Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment" IEEE Internet of Things Journal , vol. 6,no. 2 , April ,pp. 3572-3584 ,2019.

[3]. Air Force Institute of Technology, “A secure Group Communication Architecture For a Swarm of Autonomous Unmanned Aerial Vehicles”, DC. Department of Air Force of the United State, 2008

[4]. Ahmad Y. Javaid,Weiqing Sun,Vijay K. Devabhaktuni,Mansoor Alam,”Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System”,

[5]. Navneet Verma, Suman Sangwan, Sukhdeep Sangwan, Devender Parsad,”IoT Security Challenges and Counters Measures”,International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878, Volume-8 Issue-3, September 2019.

[6]. Leela Krishna C. G. and Robin R. Murphy,”A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles ”,2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)Shanghai, China, October 11-13, 2017.