A Robust Internet of Drones Security Surveillance Communication Network Based on IOTA

Syeda Mahnoor Gilani[a], Adeel Anjum[b,c], Abid Khan[d], Madiha Haider Syed[b], Syed Atif Moqurrab[e,*] and Gautam Srivastava[f,g,h,*]

[a] *Department of Computer Sciences, COMSATS University, Islamabad, Pakistan*
[b] *Institute of Information Technology, Quaid-i-Azam University Islamabad, Pakistan*
[c] *Southern University of Science and Technology (SUSTECH), Shenzhen, China*
[d] *School of Computing, College of Science and Engineering, University of Derby, Derby, DE221GB, England*
[e] *School of Computing, Gachon University, 1342, Seongnam-daero, Sujeong-gu, Seongnam-si, 13120, Korea*
[f] *Dept. of Math and Computer Science, Brandon University, Canada*
[g] *Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan*
[h] *Dept of Computer Science and Math, Lebanese American University, Beirut 1102, Lebanon*

ARTICLE INFO

Keywords:
Internet of Drones (IoD)
Security surveillance
Secure communication
IOTA
AVISPA
Physical capture attacks
Botnet

ABSTRACT

Drones are increasingly utilized for a variety of purposes, spanning military to civilian applications. The rise in drone usage underscores privacy and security challenges concerning flight boundaries, data collection in public and private domains, and data storage and dissemination. Such issues highlight the drones' capability to communicate and securely store data over potentially insecure channels. Recognizing these challenges and gaps in the research, this paper introduces an efficient and secure security surveillance model for the Internet of Drones (IoD). Our model ensures secure communication between Ground Stations (GS) and Drones, effectively addressing various attack types. Particularly, surveillance drones are vulnerable to physical capture attacks. We delve into a scenario where a network drone is physically apprehended. Leveraging the information stored within the drone, the attacker could potentially access the session. This paper proposes a solution to counter such threats. Through experiments using MATLAB and VScode, we evaluate our network's efficiency and scalability in relation to the surge in transactions. The findings reveal our model's prowess in handling large-scale networks. Specifically, when transactions surpass 1000 per minute, our model achieves approximately a 20% reduction in processing time compared to existing studies. Moreover, our approach facilitates about 80% enhanced communication efficiency relative to the contemporary state-of-the-art frameworks. A security analysis via AVISPA further corroborates the robustness and security of our proposed communication strategy against diverse attack types.

1. Introduction

Rapid technological advancements have brought about significant changes in various industries, and the realm of drones also referred to as Unmanned Aerial Vehicles (UAVs), is no exception. Drones are witnessing a surging demand across numerous sectors, encompassing agriculture, construction, law enforcement, search and emergency rescue, controlled airspace management, and navigation services [1]. They are already actively deployed in a wide range of applications, including military operations [2], delivery services, medical supply transportation, and cinematography.

The Internet of Battlefield Things (IoBT) [3] has emerged as a concept connecting soldiers with smart technologies integrated into their weapons, armor, and radios. This connectivity provides soldiers with enhanced situational awareness, allowing more efficient risk assessments and improved situational understanding. By leveraging interconnected technology and machine intelligence, military operations can achieve higher levels of security capabilities [4]. IoBT plays a crucial role in developing effective security deployment strategies [5]. Furthermore, when tethered drones are integrated into IoBT, they can provide swift and efficient responses in various situations, operating along faster routes and approaching intruders covertly, thereby reducing risks for personnel [6].

[*] Corresponding author

mahagilani111@gmail.com (S.M. Gilani); Aanjum@qau.edu.pk (A. Anjum); a.khan3@derby.ac.uk (A. Khan); Madiha@qau.edu.pk (M.H. Syed); atif@gachon.ac.kr (S.A. Moqurrab); srivastavag@brandonu.ca (G. Srivastava)

ORCID(s): 0000-0003-3284-1755 (S.M. Gilani); 0000-0001-5083-0019 (A. Anjum); 0000-0003-2712-1956 (A. Khan); 0000-0001-5083-0019 (M.H. Syed); 0000-0003-3284-1755 (S.A. Moqurrab); 0000-0001-9851-4103 (G. Srivastava)

The Internet of Things (IoT) ecosystem has adopted a distributed ledger called IOTA [7] (MIOTA) to facilitate secure machine-to-machine and device-to-device transactions. IOTA ensures secure data transactions among different network nodes and exhibits scalability, allowing networks to expand to thousands of nodes. The scalability and resource efficiency offered by IOTA are particularly advantageous for large-scale networks. Additionally, IOTA operates without transaction fees, as it does not rely on traditional miners. It can be implemented across various communication mediums, such as 4G, 5G, and 6G, offering flexibility based on budget and network speed requirements [8].

This paper focuses on a security surveillance system based on drones, specifically addressing vulnerabilities arising from physical capture attacks on network drones. We assume that the ground station (GS) and control station (Cr) are authorized and trusted entities. The system consists of four phases that enable scalable communication among multiple entities while providing security against various attacks. In the first phase, the system initializes and registers different entities, with the GS registering the ground stations and drones within their respective zones. The second phase involves session establishment between the GS and each drone, facilitating information transfer. In the third phase, the GS assigns credentials to the drones for a confidence-building scenario. This scenario involves the drones computing a code based on their assigned code and a known formula, which is then sent to the GS for verification. Finally, the fourth phase enables drone-to-drone communication and the creation of ad-hoc networks when necessary. Figure 1 illustrates the network model, with Ground Stations (GS) linked to a Control Station (Cr) and Drones (Dr) divided area-wise, each linked to their respective Ground Station (GS).

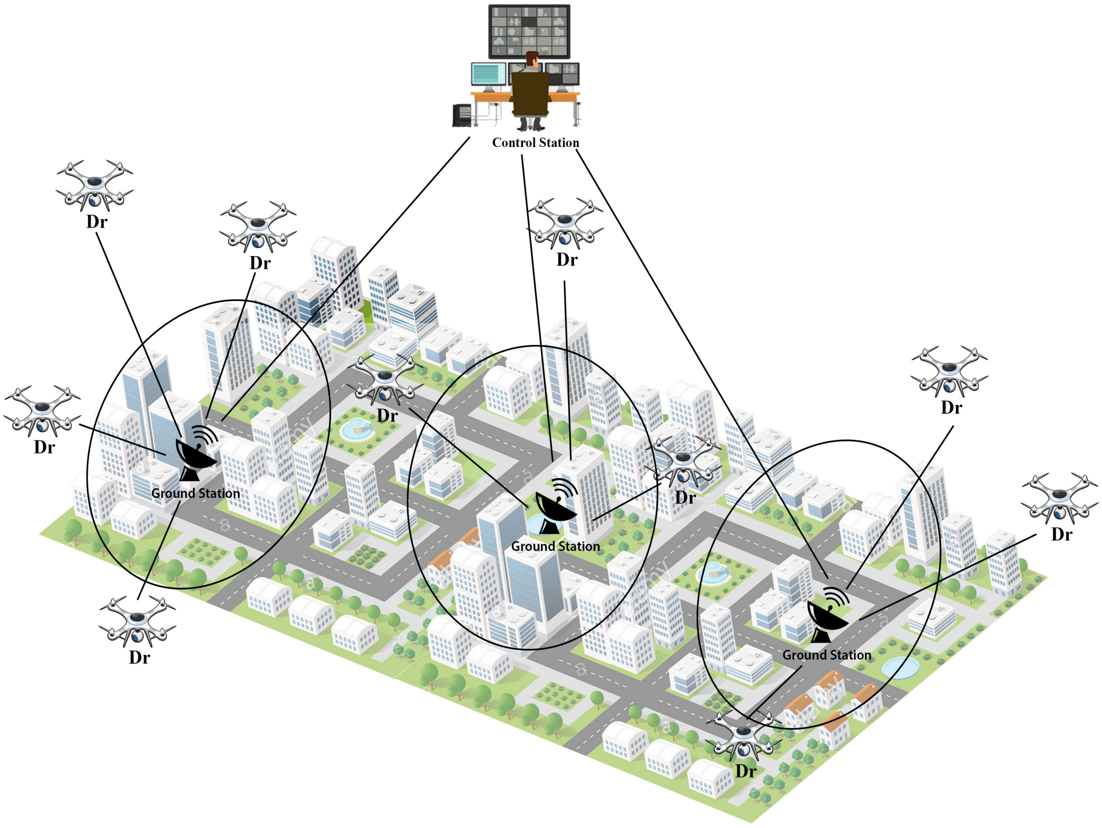


Figure 1: System Model showing surveillance drones network which contains GS and their associated drones, which are monitored by the GS.

The motivation behind this research is to propose a secure communication network for surveillance systems based on drones (UAVs), which are in high demand across various fields. The proposed system leverages IoBT to provide soldiers with enhanced situational awareness and safeguarding capabilities. It also utilizes IOTA as a distributed ledger for secure data transactions, scalability, and resource efficiency. The goal is to develop a cost-effective, scalable, and secure communication system that protects against various attacks, including botnet attacks, fake node attacks, sinkhole attacks, and black hole attacks.

The research objectives of this study include proposing a security surveillance system for drones using IOTA as a distributed ledger system. Additionally, the study aims to provide scalable communication and security against various attacks. The research also involves implementing a system initialization and registration process for different entities, such as ground stations and drones. Moreover, the study aims to establish secure sessions between ground stations and drones to facilitate secure information transfer. Furthermore, a confidence-building mechanism will be implemented to verify and validate the authenticity of drones within the network. Finally, the proposed system's performance and security will be evaluated against different types of attacks.

The contributions of this research include:

- Utilizing the IOTA tangle network for transactions, showcasing its scalability, efficiency, security, and cost-effectiveness.
- Introducing behavior monitoring of drones by the ground station for detecting malicious activities.
- Employing hash functions for secure communication, enabling identification of fake packets and preventing the transfer of false information between nodes.
- Providing immunity against botnet attacks and fake nodes through a confidence-building scenario.
- Addressing the limitations of previous research by proposing an IOTA-based security surveillance system for drones that offers enhanced security and efficiency.
- Presenting experimental results that demonstrate the efficiency of the proposed network compared to other networks.

The organization of the paper is as follows: Related work has been discussed in Section 2. The preliminaries in security surveillance are discussed in Section 3. The attacker model has been discussed in Section 4. The proposed framework and architecture have been detailed in Section 5. The results and discussion are discussed in Section 6. Moreover, the security analysis of the proposed framework is detailed in Section 7. Conclusion and future work are presented in Section 8.

2. Related Work

Drones, also known as Unmanned Aerial Vehicles (UAVs), have been increasingly utilized in various fields such as agriculture, construction, law enforcement, search and emergency rescue, transportation-controlled airspace, and navigation services. With the integration of the Internet of Battlefield Things (IoBT), drones have the potential to provide soldiers with extra sensory perception through smart technology in weapons, armor, and radios. However, the increasing use of drones also brings about security and privacy concerns that need to be addressed. In this section, current studies relevant to drone security Surveillance Communication networks based on IOTA have been discussed in detail.

The use of drones is tremendously increasing in various fields. They have rising demand in numerous fields including agriculture, construction, law enforcement, search and emergency rescue, transportation-controlled airspace, and providing navigation services. The Internet of Battlefield Things (IoBT) provides soldiers with extra sensory perception by connecting them with smart technology in weapons, armor, and radios. Furthermore, they will be able to get close to the intruders without giving them any clue and it can reduce the risks for the people because tracking any kind of intruder will be less challenging. Different techniques are proposed to mitigate security and privacy issues. But every technique has its drawbacks. We have highlighted some of the major limitations and security negligence which isn't considered by most of the researchers, which mainly includes physical capture attack, session hijacking, and botnet attacks.

Alladi et al. [9] in their paper provided a comprehensive study about all the applications of UAVs. The rapid enhancements in the use of UAVs go hand in hand with industrial advancements. However, with the advancement of UAV networks, their vulnerabilities demand a higher level of security. UAV's security includes verification, secrecy, integrity, and denial services for the transmitted information. UAVs have a very high risk of leakage of data, as they are remotely accessed. Due to the vulnerable communication network, it is important to properly encrypt information to secure it from any attack. For this problem, cryptographic primitives are an essential tool, but it is important to use them accurately. Many researchers are providing their solutions in this regard. UAV networks generally involve communication entities like UAV-to-UAV, UAV-to-GSS, and UAV-to-User. Every entity has its significant role, and it also includes different levels of insecurities. The most common security issues are network jamming, eavesdropping, authentication, mobility management, and many more. As UAVs don't have proper mechanisms and protocols so many attacks are still unknown. Many researchers are working on these things and we get to know about new attacks daily. In this regard, we reviewed some of the papers and their comprehensive study is as follows.

Muskan et al. [10] proposed a secure authentication scheme tailored for the Internet of Drones (IoDs), utilizing physical unclonable functions. Their model boasts a lower storage cost compared to other schemes and effectively mitigates node tampering and cloning attacks. However, it is worth noting that the proposed model incurs higher communication costs.

Berini et al. [11] introduced a hyperelliptic curve-based anonymous lightweight authentication (HCALA) scheme designed for both drones and users. This scheme relies on a combination of hash functions, blockchain technology, XOR operations, and hyperelliptic curve cryptography (HECC). Their solution excels in terms of achieving a balanced trade-off between security and efficiency for drones while maintaining robust security.

Biregani et al. [12] in 2021, proposed a security model of UAVs based on smart agents to resolve security challenges during the communication of different entities in a network. Their method is based on two phases, the first phase identifies and removes malicious nodes using behavior detection and the second phase is based on mobile agents that are used for data transfer and to detect malicious traffic. Mobile agents work with neighboring UAVs for reliable communication. Their proposed system is expensive as it requires extra drones as mobile agents.

Bera et al. [13] 2020, proposed a blockchain-based access control algorithm for IoD to secure the drone to drone and drone-to-GS communication. In their proposed scheme, sensitive data is collected from transactions through GS and converted into blocks, these blocks are then added to the BC via the "Ripple Protocol Consensus Algorithm (RPCA)" using a peer-to-peer cloud server connected to the GS. The transactions containing the data cannot be tampered with or removed once they are added to BC. Bera et al. [14] in 2020 said, that all the drones and the GSS are enrolled with a focal trusted power Control Room (CR) preceding their organization. Since the GSS and the robots convey over an open channel (e.g., remote medium), there are protection and security issues in the IoD climate. The proposed BACS-IoD needs low cost for correspondence during both D2D and D2GSS access control stages when contrasted with all other existing plans. Under the CL-AtSe backend, the simulation investigated 1614 states, and out of those states, 149 states were reachable, and it took the interpretation season of 0.05s and calculation season of 0.18s. In HLSPL execution, the top-most job (climate) determines the worldwide constants alongside a synthesis of at least one meeting. Significantly, none of the current plans give blockchain-based secure arrangements using the entrance control instrument, only BACS-IoD accomplishes blockchain-based arrangements. Tian et al. [15] in 2019, proposed a framework that works for security and privacy issues of IoDs using MEC. The framework is based on privacy-preserving authentication utilizing lightweight online/ offline signatures. The proposed signature scheme works in different phases starting from initial key generation, SK prep. on joining, R-TS key update, offline signature preparation, online signature generation, and signature verification.

Different techniques are proposed although all the authors provided a secure mechanism for mitigating different attacks. All the techniques are good in their own ways. But the major problem is the botnet attack which is missing. Many authors discussed physical capture attacks, but no one discussed if any node of the network is created by the bot, then it can severely damage the network. The latest research like Yahuza et al. [2] and Ko et al. [16], did not focus on these sorts of attacks. But their schemes are good in their ways. They proposed security surveillance schemes of IoDs based on secure communication networks and achieving security from different attacks. Later, Yaacoub et al.[17] proposed a lightweight authentication scheme for IoDs, which used symmetric key cryptography and Alladi et al. [18] proposed ECC based authentication scheme. Later, Bera et al. [14] proposed an authentication scheme in 2020, which was based on temporal credentials and it removed a lot of problems. Furthermore, security and privacy remained a hotline for researchers. Yoon et al. [19], Wazid et al. [20] and Bera et al. [13], provided some protocols in concern with security and privacy aspects. 2020 was the year for blockchain-oriented networks many researchers proposed schemes using blockchain. Li et al. [21] Irshad et al. [16] proposed models based on blockchain which provided secure communication and a low risk of data loss. This paper proposes a security surveillance system based on four phases that provides scalable communication of multiple entities and provides security from numerous attacks like botnet attacks, fake node attacks, sinkhole attacks, black hole attacks, etc [4]. The proposed model uses IOTA which is a distributed ledger technology. IOTA can provide secure transactions of data between different nodes. It

Table 1
Limitations in Recent Research Studies

Ref	Publication year	Technique	Methods	Security vulnerabilities/ limitations
[22]	2022	Proposes a hybrid blockchain technique for privacy and security of IoDs	ML, Blockchain	physical capture attack
[12]	2021	Uses a method of smart agents to detect and to eliminate malicious UAVs	HFA, SHA-3, ECDSA	What if any node is hijacked and it shields the surrounding nodes also then it will be difficult to route and to remove the malicious node?
[14]	2021	Blockchain-based secure communication framework for IoDs enabled aerial computing deployment	ECDSA, SHA.256,	Mutual authentication needs to be strong which led to various types of potential attacks.
[16]	2021	Communication scheme based on different phases to authenticate drones.	ECDSA, SHA-256, DHKE	No discussion of attacks such as fake agent inside a valid node and ddos attack.
[13]	2020	Works in phases starting from system initialization, registration, access control, secure data delivery and collection phase, block creation, verification and addition in blockchain center, and dynamic drone addition phase	ECDSA, DHK, SHA-256.	Their proposed scheme is lacking in securing session key and anonymity and untraceability.
[23]	2019	Framework is based on privacy-preserving authentication utilizing lightweight online/ offline signatures.	Asymmetric crypto, signatures, hashing.	Lacking some important security aspects like MITM, impersonation, and credential leakage.
[21]	2019	Proposed a physical layer security mechanism to overcome different security attacks.	none	The robustness between connected UAVs is not considered.

provides the fastest transaction rate which is advantageous for large networks [7]. Additionally, the proposed model uses cryptographic techniques ECDSA, DHKE, and SHA256 to provide secure communication of the network devices.

This paper considers an attacker model to test the robustness of the network. To develop a deep understanding of the attacker model we have provided preliminaries in the next section, which defines important definitions and attacker scenarios. The most relevant and advanced studies along with their limitations are presented in Table. 1.
In this research work, we have elucidated some of the significant limitations and security oversights in current drone technologies. While various techniques have been proposed to mitigate security and privacy issues, they all exhibit their own shortcomings. We conducted an extensive review of relevant literature on this topic, offering a comprehensive overview of the current state of drone security. Despite the challenges, the utilization of drones continues to grow, underscoring the importance of ongoing research and the development of novel methods to enhance their security and privacy.

3. Preliminaries

Unmanned Aerial Vehicles (UAVs) are particularly susceptible to attacks due to their operation in open spaces and reliance on wireless communication channels [24]. They are exposed to various forms of attacks and threats, especially when navigating through open airspace. Some notable attacks include physical capture attacks, botnet attacks, fake nodes, black hole attacks, grey hole attacks, and sinkhole attacks [12]. This paper primarily focuses on the scenario in which a UAV is compromised and turned into a botnet. Below are key definitions used in this paper, along with detailed explanations of these attacks. Additionally, all symbols employed in this paper are defined in Table 2.

Table 2
Symbols and Their Significance

Symbols	Significance
$E_q(u, v)$	A non-singular elliptic curve.
B	A base point in $E_q(u, v)$ of order as large as q.
$K * B$	Elliptic curve point multiplication": $k * B = B + B + ... + B(ktimes)$
$X + Y$	Elliptic curve point addition, $X, Y \in Eq(u, v)$
TS	"Current timestamp"
δT	Maximum transmission delay associated with a message
$h(.)$	Collision-resistant Cryptographic one-way hash function
Sk_i	Session key established for one session.
skv_i	Session key verifier
Ack_n	Acknowledgment.
Cr	control room (trusted authority)
Cr_n	Identity
c_n	secret key
Pb_n	Public key
GS	ground server station
GS_n	GS identity (n number of times)
g_n	GS Secret key
GPb_n	GS Public key by Cr
Ct_{G_S}	Certificates of GS
$TsGS$	Timestamps of GS used while registration process
rsk_n	Random secret key
Pub_{g_n}	Random public key
Dr	Drone
Dr_n	Real identity of Dr (n number of drones in the network)
PID_n	Pseudo-identity of Dr
d_n	Primary Secret key
DPb_n	Primary Public key
k_{d_r}	secret key for signature
Pk_{d_r}	Public key for signature
Ct_{d_r}	Certificate by Cr to Dr
$TsDr$	timestamps

3.1. Botnet Attack

A botnet attack is a type of attack in which an attacker employs legitimate nodes to engage in illicit activities [25]. Botnets are ordinary network devices that have been compromised through malware injection, allowing the attacker to control them for various malicious purposes, such as sending spam or launching Distributed Denial of Service (DDoS) attacks on specific servers [26]. DDoS attacks initiated by bots pose a significant threat because they are nearly indistinguishable from valid users.

3.2. Physical capture attack

This type of attack targets devices that are publicly accessible, such as UAVs. UAVs operate openly in the airspace, making them vulnerable to capture [26]. Attackers can seize UAVs from various networks, including security networks or delivery systems, to gain access to the sensitive data stored within them.

3.3. Attacks on the network

This section briefly describes a game that can lead to session hijacking and botnet attacks inspired by the games used in Bera et al. [13]. Firstly, let us overview games created by Bera et al. [13], considering them according to this paper. Bera in their paper created games that an attacker can play on the network. We assume by playing all those games together attacker can compute the session key and using that session key launch a botnet attack on the network. Following is the detail about how the attacker accesses the session key [27].

This section discusses, the botnet attack on the proposed network. We assume that a drone from the network is physically captured and fabricated as a bot. An attacker can perform this attack by getting access to the session key. Following is the detail about how the attacker accesses the session key [28],[29].

Suppose $Bt_A = Botnet\ Attacker,\ T_{poly} = polynomial\ time,\ U = correct\ bit\ and\ U' = guessed\ bit.$

Let us assume, that Bt_A running in polynomial time (T_{poly}) tries to break the security by brute force technique. It tries different combinations to compute the correct session key (sk_i). To guess the correct bit following equation1 needs to be satisfied.

$$Bt_A(T_{poly}) = |2Pr[U' = U] - 1| \tag{1}$$

To compute the the equation 1. the attacker tries different techniques including different attacks on the network. Suppose an attacker attempts to compute session key ski in polynomial time T_{poly}. Then it needs to compute the equation2 to break the "Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)".

$$Bt_A(T_{poly}) \leq \frac{u^2H}{hash} + 2Bt_A(T_{poly}) \tag{2}$$

Where "uH" denotes the number of [30] "hash queries" and "hash" denotes the "hash function". To reach this number attackers will perform some attacks. Firstly, it will perform an "actual attack" which is basically a brute force attack. It will try to guess random bits U' to guess the correct bit U. It will compute random bits in equation 3as:

$$Bt_{A_1}(T_{poly}) = |2Bt_A(T_{poly}) - 1| \tag{3}$$

An attacker can also do an eavesdropping attack, it will help an attacker to learn more about secret information and about the network processes. It executes a query to perform an eavesdropping attack to learn about session key ski from all the messages communicated. It gets extra information attached with the messages like, $msgs = \left\{Dr_n, DPb_n, Ct_{d_r}, TsDr, Pk_{d_r}, GS_n, pub_{g_n}, Ct_{G_S}, TsGS, Pb_n, Ack_n, skv_i\right\}$. However, receiving this information does not let the session key. A session key is protected by hashing. As a result of this attack, the following property holds (see equation 4):

$$Bt_{A_2}(T_{poly}) = Bt_{A_1}(T_{poly}) \tag{4}$$

Now, the attacker performs an "active attack" [24]. This attack is based on "hash computing" and "physically capturing the drone". The session key for one session can be computed as: $Sk_1 = H(dhk_1||Dr_1||GS_1||d_1||pub_2), wheredhk_1 = rsk'_1.B.$

By capturing the drone, the attacker will get the secret key of drone kdr. Now, the attacker has knowledge of $msgs = \{k_dr, Dr_n, DPb_n, Ct_{d_r}, TsDr, Pk_{d_r}, GS_n, pub_{g_n}, Ct_{G_S}, TsGS, Pb_n, Ack_n, skv_i\}$. To compute $Sk1$ attacker needs dhk_1, and to derive dhk_1 attacker needs a random secret key of the $GS = rsk_1$ and base point B. To drive dhk_1 attacker must solve ECDDHP. And it's hard to compute ECDDHP. To solve ECDDHP it needs to compute "hash collision resistant" and solve with the help of the birthday paradox as explained in equation 5 below:

$$|Bt_{A_2}(T_{poly}) - Bt_{A_3}(T_{poly}) \leq \frac{u^2H}{hash} + Bt_A(T_{poly})| \tag{5}$$

After performing all the attacks, the attacker needs to guess the correct bit U. Therefore, we get the equation 6

$$Bt_{A_3}(T_{poly}) = \frac{1}{2} \tag{6}$$

By solving the equation 6 it formed (see equation 7) as:

$$\frac{1}{2}.Bt_A(T_{poly}) = |Bt_{A_1}(T_{poly}) - \frac{1}{2}| \tag{7}$$

Now, by putting the values of equation 2, 3, and 4 in equation 7 we get equation 8, 9, and 10.

$$\frac{1}{2}.Bt_A(T_{poly}) = |Bt_{A_1}(T_{poly}) - |Bt_{A_3}(T_{poly})| \tag{8}$$

$$= |Bt_{A_2}(T_{poly} - Bt_{A_3}(T_{poly}| \tag{9}$$

$$\leq \frac{u^2 H}{hash} + Bt_A(T_{poly}) \tag{10}$$

Now, multiply 2 on both sides we get the final equation 11.

$$Bt_A(T_{poly}) \leq \frac{u^2 H}{hash} 2Bt_A(ECDDHP)(T_{poly}) \tag{11}$$

In this way, the attacker will succeed in solving ECDDHP and then will compute the session key. Then it will create that drone a botnet Bt-Dr and penetrate the session. It will have all the basic information to become a valid node in the network. Now, it penetrates the established session (session established between drone (***Dr***) and ground station (***GS***)) as shown in Figure 2. It can communicate with GS or other drones. Or it can launch different attacks to access data. It can also create more bots in the network or can perform DDoS attacks and can down the whole network. It is hard to detect botnets in the network or to secure the drone from a physical capture attack [31]. But we can avoid such attacks from prevention and detection models. Our proposed model provides security from such attacks when there is intrusion hidden inside a legal node [32].

4. Attacker Model

This research adopts the widely used DY model as the threat model [33]. According to this model, any two entities communicating over an insecure channel are considered untrustworthy. This includes entities like drones or end-users engaged in communication [34]. In the proposed model, Ground Station (GS) and Control Station (CS) are considered trusted entities, while Drones are categorized as untrusted entities. The weakest and most vulnerable link in the network is the drones, which attackers can exploit to breach the system's security.

Consider a scenario in which attackers utilize drones to infiltrate the network. Figure 2 illustrates an assumption-based scenario in which a valid node in the network falls under attack and is compromised, resulting in the creation of a bot, referred to as Bt-Dr5. GS remains unaware of this attack. Bt-Dr5 utilizes a session key and attempts to establish communication with GS by sending a message containing valid information about Drone Dr5. GS computes its timestamp (TS-Dr5) and verifies the signature. Upon successful verification, GS responds with $Code1$, which initiates a confidence-building scenario. This mechanism aids in detecting such intrusions and prevents attackers from communicating with other entities. However, in this scenario, Bt-Dr5 remains concealed and is unable to compute the necessary response. When GS either does not receive a reply within the TS timestamp or receives an incorrect response, it terminates the session with that drone and marks it as malicious, thereby preventing further communication with the network.

5. Methodology

This section discussed the proposed intelligent drone-based security system in detail. It will be used for security surveillance for societies or cities. The system is based on different surveillance drones which are supervised by ground stations. The proposed framework is a combination of different phases that are depicted in figure 3.

The phases are the Registration Phase, Session Establishment, Exchange of Information, and Drone-to-Drone Communication. The following sections explain the working of these phases.

5.1. Phase 1: System Initialization and Registration

This phase works the same as Bera et al. [13], with slight changes explained in detail below.

Firstly, Cr initializes the system by selecting parameters. Cr picks cryptography primitives as first select points of the elliptic curve as $E_q(u, v) : y^2 = x^3 + ux + v(modq)$.

Where q is a large prime number, and $u, v \in Z *_q = \{1, 2, ...q - 1\}$ such that $4u^3 + 27v^2 \neq 0(modq)$ holds.

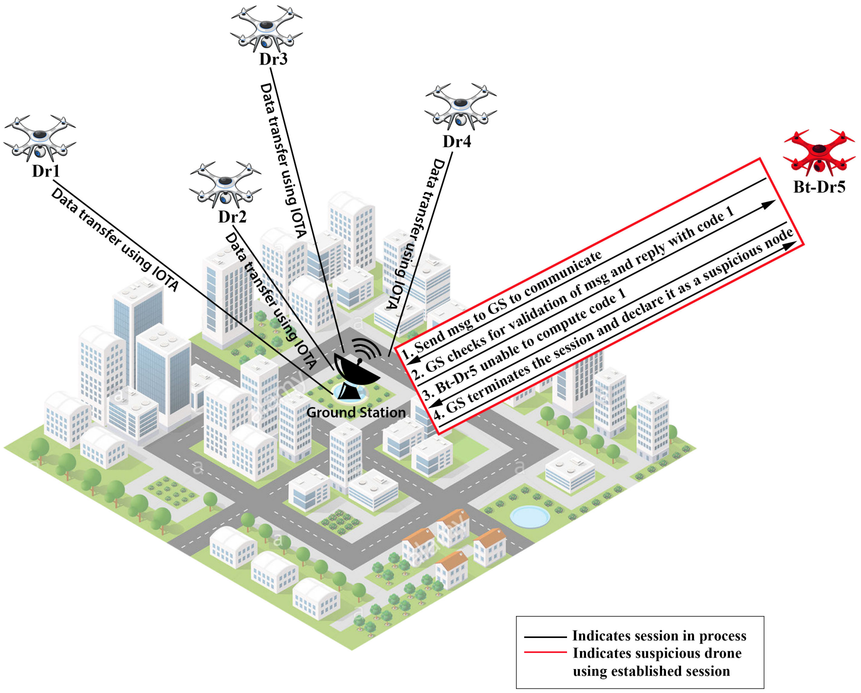

Dr3
Dr4
Dr1
Dr2
Bt-Dr5
Data transfer using IOTA
Data transfer using IOTA
Data transfer using IOTA
Data transfer using IOTA
Ground Station
1. Send msg to GS to communicate
2. GS checks for validation of msg and reply with code 1
3. Bt-Dr5 unable to compute code 1
4. GS terminates the session and declare it as a suspicious node
Indicates session in process
Indicates suspicious drone using established session

Figure 2: Scenario: One of the Network Drone is Created a Bot (named BT-Dr5), Penetrating the Session and Communicating with GS.

Cr then picks a base point $B \in E_q(u,v)$ as large as $q.Cr$, also picks hash function $H(.)$ such as SHA-256. After that Cr picks its own identity as Cr_n and then the secret key as: $c_n \in Z *_q$. Then it computes its public key as: $Pb_n = c_n.B$. The parameters $E_q(u,v)$, B, $H(.)$, Pb_n are public, and c_n is private. After that Cr registers other entities like GS and Dr as shown in Figure 4. The further registration process is as follows.

Cr registers GS: Cr firstly register GS by picking its unique identity as GS_n. GS_n which can be a combination of numbers. Then Cr picks secret key for GS as $g_n \in Z *_q$. Then it computes its public key as $GPb_n = g_n.B \in Z *_q$. Then Cr creates a certificate for GS to make it a valid entity. The certificate is computed as $Ct_{G_S} = g_n + h(Cr_n||GS_n||Pb_n||GPb_n||TsGS) * c_n(modq)$. Parameters $\{Pb_n, GPb_2, Eq(u.v), H(.), B\}$ are public. Cr stores $\{Cr_n, c_n, Pb_n, GS_n, g_n, GPb_n\}$ parameters in its database. And Cr sends $\{Cr_n, GS_n, Ct_{G_S}, Pb_n, GPb_n, E_q(u.v), H(.), B\}$ to GS.

After Receiving parameters GS store them in its database and pick its Random secret key as $rsk_n \in Z *_q$. Then corresponding to it computes the public key as $Pub_{g_n} = rsk_n.B$. Which GS will be used for further communication? After completion of GS registration Cr registers Dr. In this section, we explain the registration of one Dr, there could be more than one Drs in a single Flying Zone, but the process is the same for all.

Cr registers Dr: Cr selects a unique identity for the Dr as Dr_n, then Cr selects its pseudo-identity as $PID_n = H(Dr_n||Cr_n||TsDr)$ then Cr picks the secret key $d_n \in Z *_q$ and computes the public key as: $DPb_n = d_n.B \in Z *_q$. Then Cr pick instant signature key for Dr as $k_{d_r} \in Z *_q$ and compute its corresponding public key for signatures $Pk_{d_r} = k_{d_r}.B$. Then Cr creates certificate for Dr as $Ct_{d_r} = k_{d_r} + H(Dr_n||Pb_n||GPb_n||DPb_n) * c_n(modq)$. After that Cr stores secret credentials $\{d_n, Dr_n\}$ in its database so that in the future it could recognize its drones. Cr creates a table in its database where it stores the identity of Drs and GS for future use. Then Cr sends drone secondary credentials to the GS $\{Dr_n, k_{d_r}, Pk_{d_r}, Ct_{d_r}\}$. Then Cr sends credentials to Dr as $\{Dr_n, Ct_{d_r}(k_{d_r}, Pk_{d_r}), pub_{g_n}, E_q(u,v), H(.), B\}$. Dr receives the data and stores them for later use. The process of registration is repeated every time the system is initialized to avoid any sort of leakage of credentials.

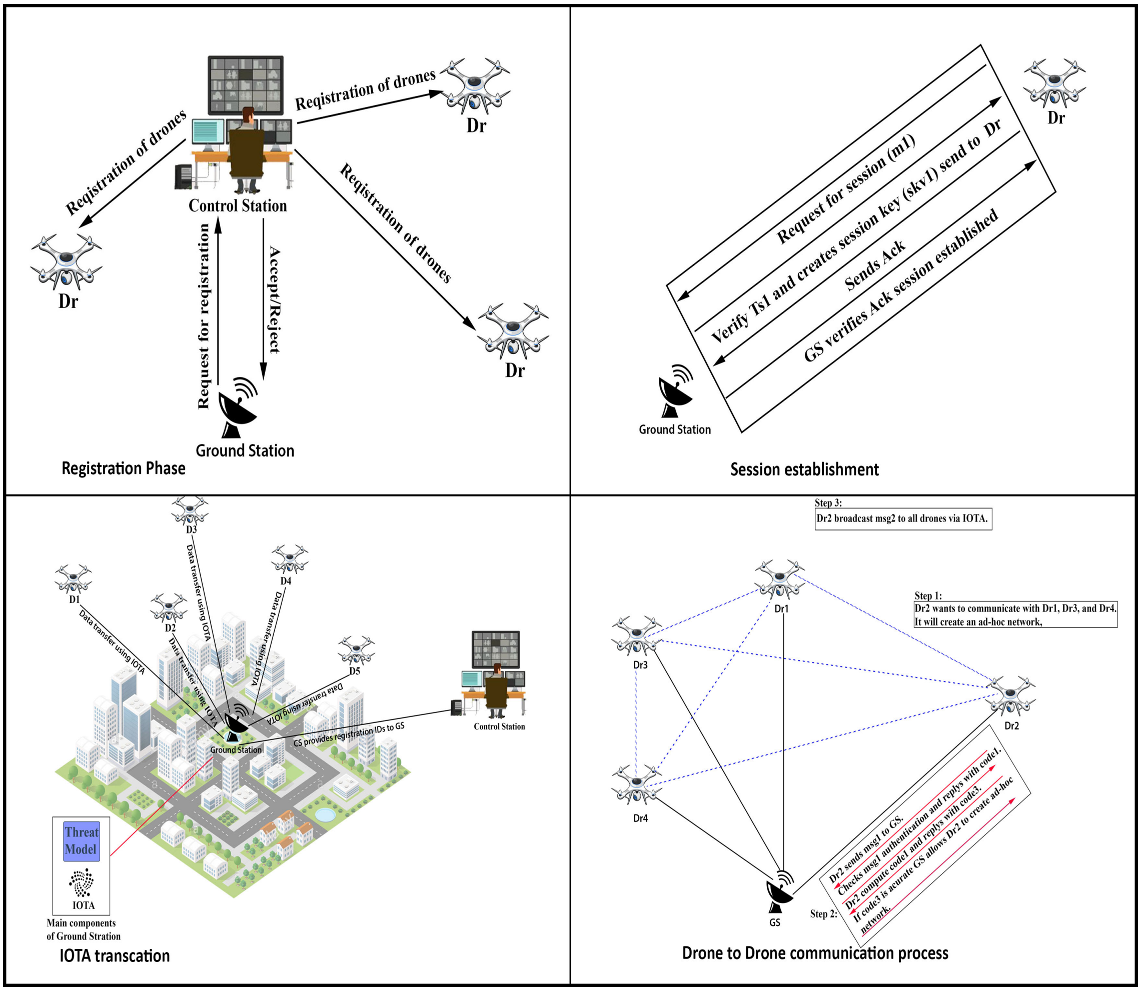


Figure 3: The System Architecture illustrates different network phases: Registration Phase, Session Establishment Phase, IOTA Transaction, representing drone communication with GS and GS communication with Cr, and Drone to Drone Communication phase.

5.2. Phase2: Session Establishment

The session establishment phase is inspired by Irshad et al. [16], which have removed the flaws of Bera et al. [13] phases. Some changes are made according to the requirements of the proposed model. Further detail of this phase is explained below.

This phase is based on mutual authentication between GS and its associated Drs. This is an important phase for the communication and transfer of data as shown in Figure 5. It also provides security to the information transferred within the session and prevents intrusions. Both GS and Dr use pre-loaded data from the registration phase to establish a session. This phase performs authentication and verification of timestamps, certificates, and signatures based on ECC and hashing. Details of the session establishment between a Dr and GS are as follows.

Dr contains information like: $\{Dr_n, Ct_{d_r}, (k_{d_r}, Pk_{d_r})pub_1, E_q(u.v), H(.), B\}$ transferred in it by Cr. Dr selects a secret key for one session as $r_n \in Z \ast_q$, and compute timestamp $Ts1$. Then it computes the signature key as $r'_n = H\{Dr_n||r_n||Ct_{d_r}||k_{d_r}||Ts_1\}$ and compute its corresponding public key $A_1 = r'_n.B$. And then generated signatures S_{d_r} and sends message to the GS as $m1 = \{Dr_n, A_1, Ct_{d_r}, S_{d_r}, Ts_1\}$.

GS contains information: $\{Cr_n, GS_n, Ct_{G_S}, (rsk_n, pub_{g_n}), Pb_n Eq(u.v), H(.), B\}$ collected in the registration phase. GS receives $m1$. It verifies the $Ts1$ and then computes the certificate as $Ct_{d_r}.B = Pk_{d_r} + H(Dr_n||Pb_n||pub_{g_n}||Pk_{d_r})$. If the Ts_1, Ct_{d_r} are valid then it checks the signature as $S_{d_r}.B = A_1 + H(Pk_{d_r}||Dr_n||Pb_n||pub_{g_n}||A_1||Ts_1).Pk_{d_r}$,

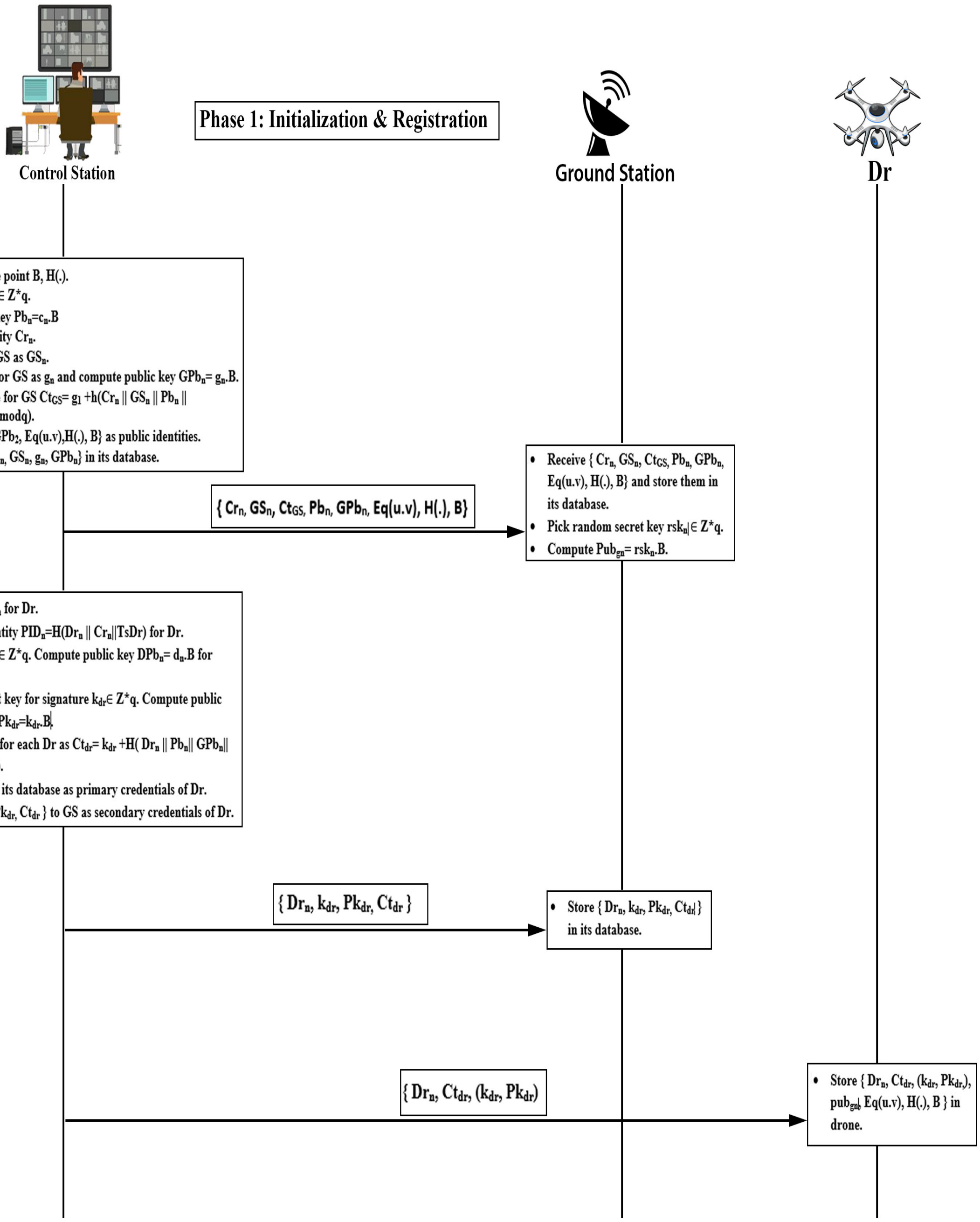

Phase 1: Initialization & Registration
Control Station
Ground Station
Dr
• Pick Eq(u.v), base point B, H(.).
• Pick secret key $c_n \in Z^*q$.
• Compute public key $Pb_n=c_n.B$
• Pick its own identity Cr_n.
• Pick identity for GS as GS_n.
• Pick private key for GS as g_n and compute public key $GPb_n= g_n.B$.
• Create Certificate for GS $Ct_{GS}= g_1 +h(Cr_n \| GS_n \| Pb_n \| GPb_n\|TsGS)^* c_1$ (modq).
• Publishes { Pb_n, GPb_2, Eq(u.v),H(.), B} as public identities.
• Stores { Cr_n,c_n, Pb_n, GS_n, g_n, GPb_n} in its database.
{ Cr_n, GS_n, Ct_{GS}, Pb_n, GPb_n, Eq(u.v), H(.), B}
• Receive { Cr_n, GS_n, Ct_{GS}, Pb_n, GPb_n, Eq(u.v), H(.), B} and store them in its database.
• Pick random secret key $rsk_n \in Z^*q$.
• Compute $Pub_{gn}= rsk_n.B$.
• Select identity Dr_n for Dr.
• Select pseudo identity $PID_n=H(Dr_n \| Cr_n\|TsDr)$ for Dr.
• Pick secret key $d_n \in Z^*q$. Compute public key $DPb_n= d_n.B$ for each Dr.
• Pick instant secret key for signature $k_{dr} \in Z^*q$. Compute public key for signature $Pk_{dr}=k_{dr}.B$.
• Create certificate for each Dr as $Ct_{dr}= k_{dr} +H(Dr_n \| Pb_n\| GPb_n\| DPb_n) * c_n$ (modq).
• Store {d_n, Dr_n,} in its database as primary credentials of Dr.
• Sends { Dr_n, k_{dr}, Pk_{dr}, Ct_{dr} } to GS as secondary credentials of Dr.
{ Dr_n, k_{dr}, Pk_{dr}, Ct_{dr} }
• Store { Dr_n, k_{dr}, Pk_{dr}, Ct_{dr} } in its database.
{ Dr_n, Ct_{dr}, (k_{dr}, Pk_{dr})
• Store { Dr_n, Ct_{dr}, (k_{dr}, Pk_{dr},), pub_{gn}, Eq(u.v), H(.), B } in drone.

Figure 4: System Initialization and Registration

if the signature is valid then it moves further otherwise discards the message and considers it malicious. After the verification of the message, picks a random number $r_2 \in Z *_q$ and timestamp Ts_2. And computes the public key as $r_2' = H(GS_n||Cr_n||r_2||Ct_{G_S}||g_n||Ts_2)$, and compute signature key $B_{G_S} = r_2'.B$. After that it computes Diffie-Hellman $Dhk_1 = r_2'.A_1 = (r_2' * r_1').B$.

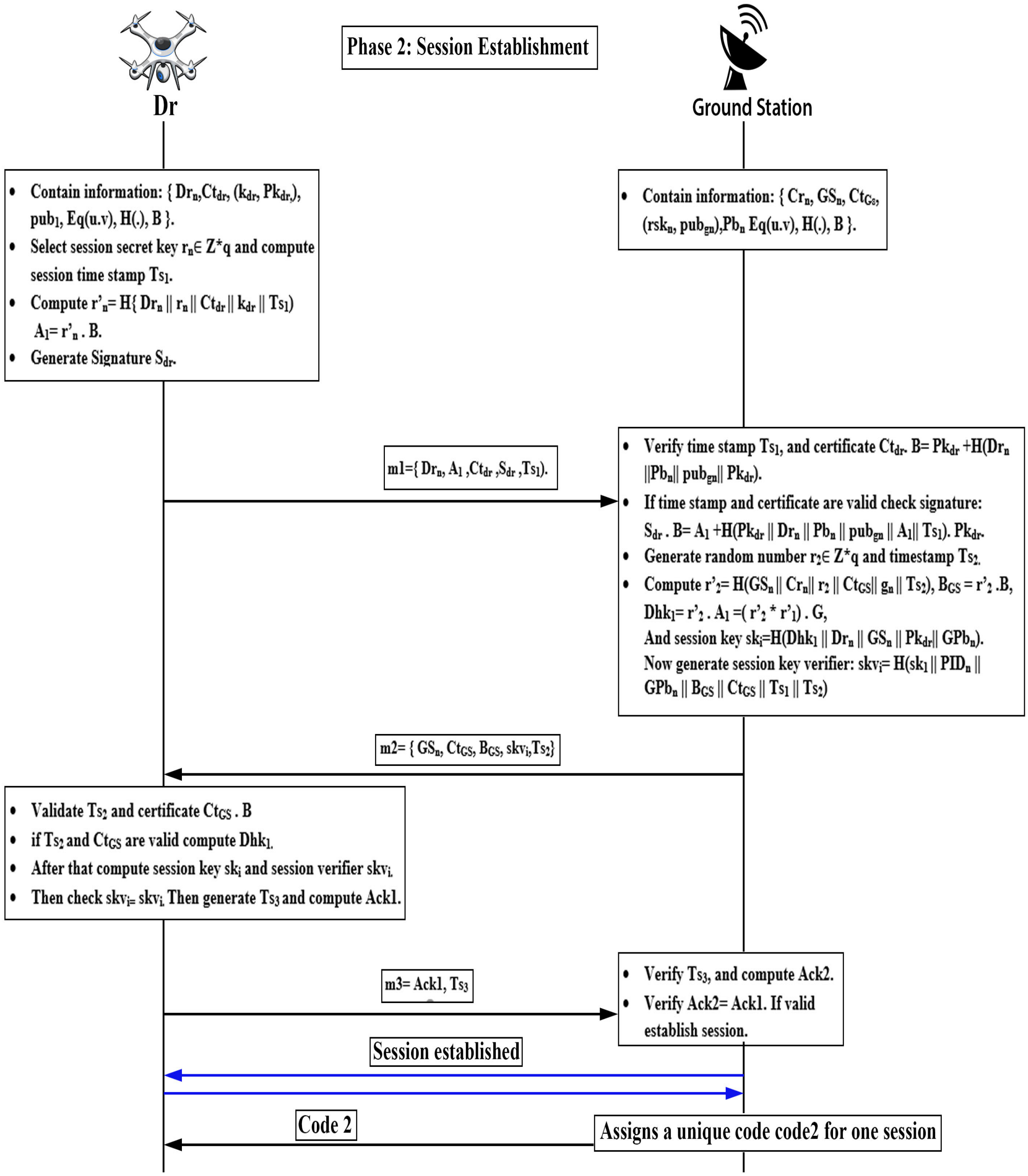

Phase 2: Session Establishment
Dr
Ground Station
Contain information: { Drn,Ctdr, (kdr, Pkdr,), pub1, Eq(u.v), H(.), B }.
Select session secret key rn∈ Z*q and compute session time stamp Ts1.
Compute r'n= H{ Drn || rn || Ctdr || kdr || Ts1) A1= r'n . B.
Generate Signature Sdr.
Contain information: { Crn, GSn, CtGs, (rskn, pubgn),Pbn Eq(u.v), H(.), B }.
m1={ Drn, A1 ,Ctdr ,Sdr ,Ts1).
Verify time stamp Ts1, and certificate Ctdr. B= Pkdr +H(Drn ||Pbn|| pubgn|| Pkdr).
If time stamp and certificate are valid check signature: Sdr . B= A1 +H(Pkdr || Drn || Pbn || pubgn || A1|| Ts1). Pkdr.
Generate random number r2∈ Z*q and timestamp Ts2.
Compute r'2= H(GSn || Crn|| r2 || CtGS|| gn || Ts2), BGS = r'2 .B, Dhk1= r'2 . A1 =(r'2 * r'1) . G,
And session key ski=H(Dhk1 || Drn || GSn || Pkdr|| GPbn).
Now generate session key verifier: skvi= H(sk1 || PIDn || GPbn || BGS || CtGS || Ts1 || Ts2)
m2= { GSn, CtGS, BGS, skvi,Ts2}
Validate Ts2 and certificate CtGS . B
if Ts2 and CtGS are valid compute Dhk1.
After that compute session key ski and session verifier skvi.
Then check skvi= skvi. Then generate Ts3 and compute Ackl.
m3= Ackl, Ts3
Verify Ts3, and compute Ack2.
Verify Ack2= Ackl. If valid establish session.
Session established
Code 2
Assigns a unique code code2 for one session

Figure 5: Session Establishment

After that GS computes session key as $sk_i = H(Dhk_1||Dr_n||GS_n||Pk_{d_r}||GPb_n)$, and then generates session key verifier as $skv_i = H(sk_1||PID_n||GPb_n||B_{G_S}||Ct_{G_S}||Ts_1||Ts_2)$. It transfers message 2 to the Dr as $m2 = \{GS_n, Ct_{G_S}, B_{G_S}, skv_i, Ts_2\}$.

After receiving the message $m2$, Dr then validates $m2$ by testing $Ts2$ and certificate as $Ct_{G_S}.B = GPb_n + H(GS_n||Cr_n||GPb_n||Pb_n).Pb_n$. After the validation process, Dr compute $Dhk_1 = r_1'.B_{G_S}(= (r_1' * r_2').B = Dhk_1)$

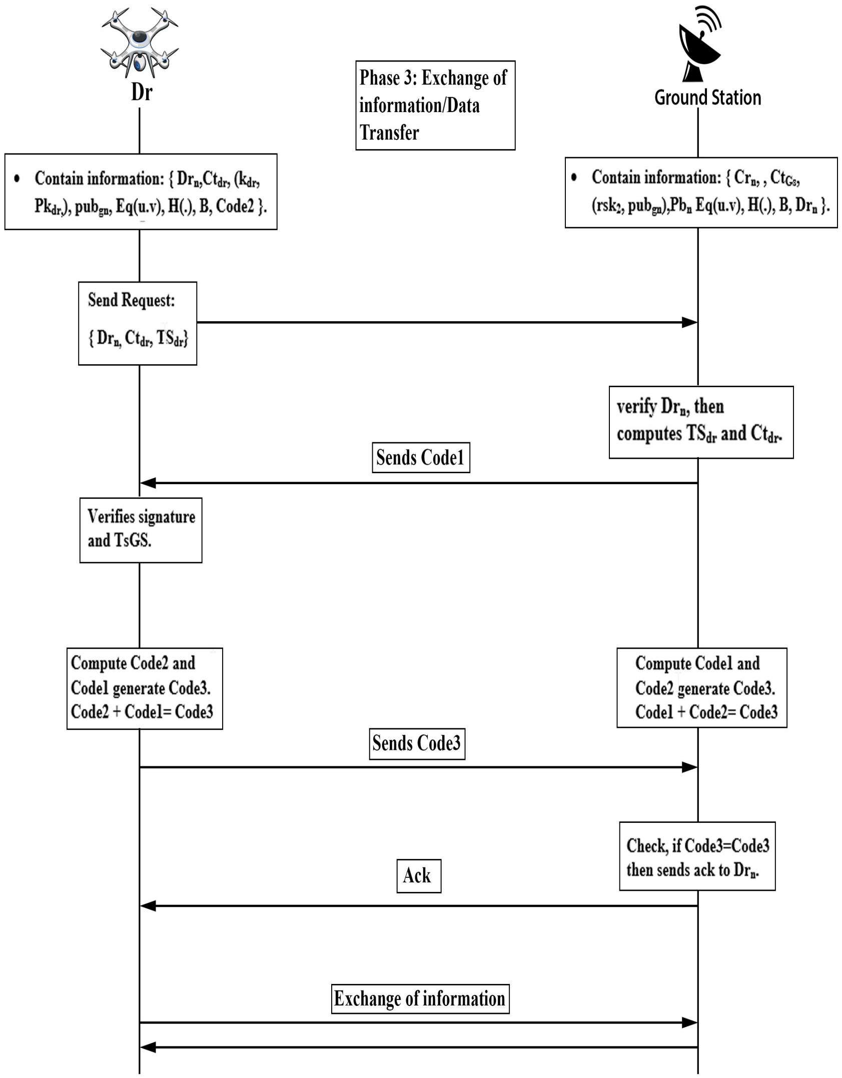

Dr
Phase 3: Exchange of information/Data Transfer
Ground Station
• Contain information: { Dr_n,Ct_{dr}, (k_{dr}, Pk_{dr},), pub_{gn}, Eq(u.v), H(.), B, Code2 }.
• Contain information: { Cr_n, , Ct_{Gs}, (rsk2, pub_{gn}),Pb_n Eq(u.v), H(.), B, Dr_n }.
Send Request:
{ Dr_n, Ct_{dr}, TS_{dr}}
verify Dr_n, then computes TS_{dr} and Ct_{dr}.
Sends Code1
Verifies signature and TsGS.
Compute Code2 and Code1 generate Code3. Code2 + Code1= Code3
Compute Code1 and Code2 generate Code3. Code1 + Code2= Code3
Sends Code3
Check, if Code3=Code3 then sends ack to Dr_n.
Ack
Exchange of information

Figure 6: Exchange of Information/Data Transfer

and derives session key $sk1$ and then computes session verifier skv_i. Then it compares both session key verifiers $skv_i = skv_i$. If both the verifiers are equal, then it acknowledges the GS.

For that, it first computes timestamp $Ts3$ and then computes $Ack1$. And then send it to GS as $m3 = \{Ack_1, Ts_3\}$. After receiving the message $m2$, Dr then validates $m2$ by testing Ts_2 and certificate as $Ct_{G_S}.B = GPb_n + H(GS_n||Cr_n||GPb_n||Pb_n).Pb_n$. After the validation process Dr compute $Dhk_1 = r'_1.B_{G_S}(= (r'_1 * r'_2).B = Dhk_1)$ and derives session key $sk1$ and then computes session verifier $skvi$. Then it compares both session key verifiers $skvi = skvi$. If both the verifiers are equal, then it acknowledges the GS. For that, it first computes timestamp $Ts3$ and then computes $Ack1$. And then send it to GS as $m3 = \{Ack1, Ts_3\}$.

5.3. Phase 3: Exchange of information/Data transfer

In this section, the transfer of data that takes place between Dr and GS is discussed and shown in Figure 6. During surveillance, Dr communicates with GS to send data. To make this communication secure and to avoid fake communication we created a confidence-building scenario. All the data is transferred over the IOTA. IOTA provides security to nodes and makes them available for the long term. The further communication process is explained below.

Table 3
Comparative Analysis of the proposed scheme with state-of-the-art techniques.

Paper	Authentication	Physical Capture Attack	Malicious Node Detection	Untraceability	Anonymity
Faraji et al. [12]	✓	×	✓	×	×
Bera et al. [13]	✓	×	×	×	×
Proposed Scheme	✓	✓	✓	✓	✓

After the completion of phase 2, Dr contains information $\{Dr_n, Ct_{d_r}, (k_{d_r}, Pk_{d_r},), pub_{g_n}, Eq(u.v), H(.), B, code2\}$. The Dr computes timestamp TS_{d_r} and then computes Ct_{d_r} and then compiles a request message $\{Dr_n, Ct_{d_r}, TS_{d_r}\}$ and send it to GS.

GS after receiving the request message verifies its $TSdr$ and then its $Ctdr$. If it is valid then GS sends $Code1$ for confidence-building. The GS computes $Code1$ with $Code2$ and generates $Code3$ as: $Code1 + Code2 = Code3$.

On the other side, Dr receives $Code1$ and verifies its signature and timestamp $TsGS$. Then Dr computes $Code1$ with $Code2$ that is Drs code. It computes as $Code2+Code1 = Code3$. Then Dr sends $Code3$ to the GS. GS compares Dr $Code3$ with its $Code3$. If $Code3 = Code3$ then GS acknowledges that Dr. GS sends Ack to the Dr. This Ack means GS now trusts that Dr and Dr can further communicate after that exchange of information takes place. In this way, GS realizes that information sent by Dr is valid.

5.4. Phase4: Drone-2-Drone Communication

During surveillance how drones can communicate securely is explained very well by Faraji et al. [12]. This phase is inspired by their architecture with some advancements to make it more efficient and secure than theirs. Further detail of this phase is explained below.

The communication between drones works similarly to the third phase. At first, Dr communicates with GS as shown in Figure 7. Then Dr follows all the steps performed in the previous section. after the completion of the confidence-building scenario, GS creates a table of all drones that are going to create an Ad-Hoc network and GS sends the IDs of other drones to that Dr. After receiving ids Dr broadcasts a message to other drones.

6. Experimental Results

Experiments were conducted using MATLAB and VScode. The 'AVISPA' tool was employed to perform security analysis and evaluate how various cryptographic functions enhance security within the model. The efficiency and effectiveness of the model were measured using VScode.

In Figure 8a, the red line represents the proposed model, while the blue line corresponds to the Faraji model [12]. Each value on the graph represents a complete transaction time, measured as the time required for a full communication process. This graph illustrates varying numbers of transactions and the time taken to complete each transaction. The X-axis denotes the number of transactions, and the Y-axis indicates time in milliseconds. It vividly demonstrates the difference in processing time between both models.

Figure 8b displays the varying numbers of transactions executed by the models, providing insights into their scalability. The X-axis represents the number of transactions, while the Y-axis denotes time in milliseconds. It is evident that the proposed ISSCN model outperforms existing techniques, even when the number of transactions is increased.

7. Security Analysis

In this section, we analyze significant security attacks and demonstrate how our proposed model offers protection against them. Table 3 presents a comparison of the security provided by our scheme with other techniques. While Faraji et al. [12] and Bera et al. [13] provide network device authentication, they both lack provisions for physical capture attacks, untraceability, and anonymity, which are essential elements for safeguarding the network from intrusions. Further details are provided below.

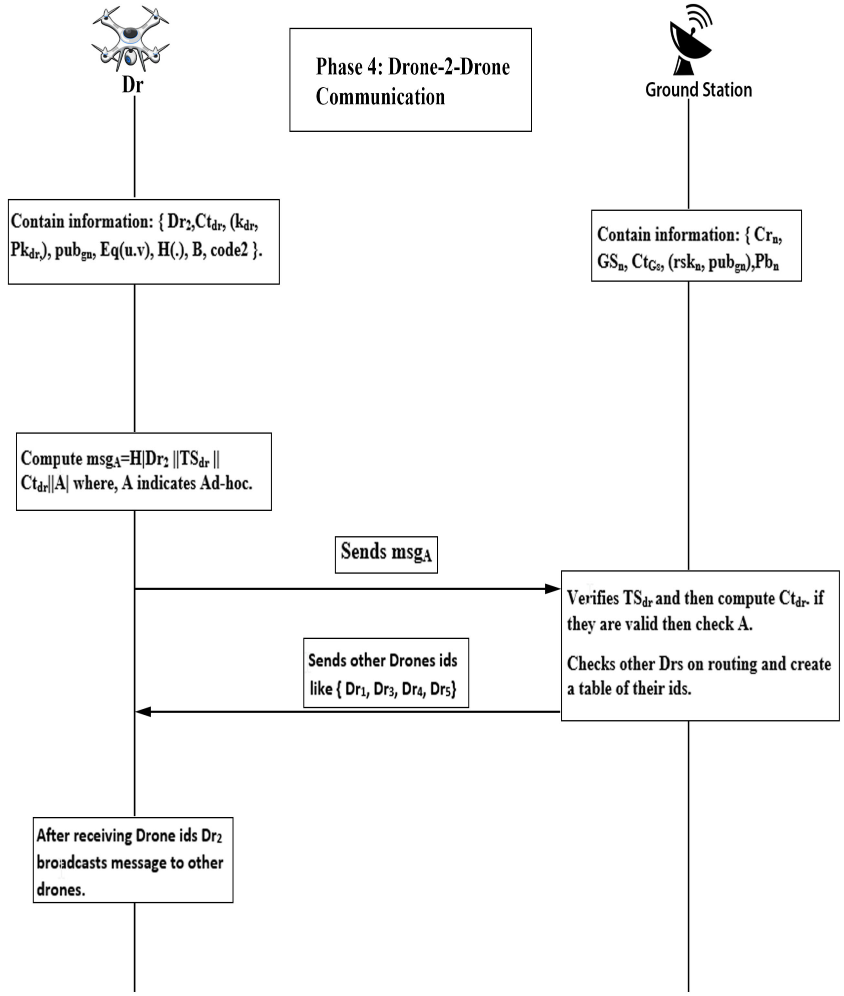
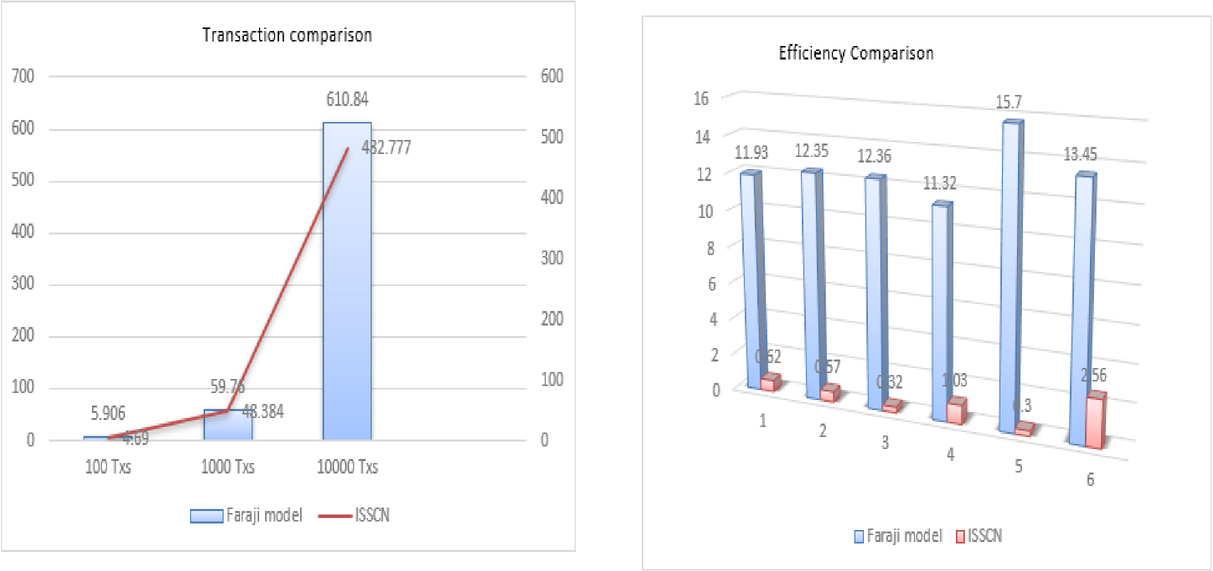

Dr
Phase 4: Drone-2-Drone Communication
Ground Station
Contain information: { Dr_2,Ct_{dr}, (k_{dr}, Pk_{dr},), pub_{gn}, Eq(u.v), H(.), B, code2 }.
Contain information: { Cr_n, GS_n, Ct_{Gs}, (rsk_n, pub_{gn}),Pb_n
Compute msg_A=H|Dr_2 ||TS_{dr} || Ct_{dr}||A| where, A indicates Ad-hoc.
Sends msg_A
Verifies TS_{dr} and then compute Ct_{dr}. if they are valid then check A.
Checks other Drs on routing and create a table of their ids.
Sends other Drones ids like { Dr_1, Dr_3, Dr_4, Dr_5}
After receiving Drone ids Dr_2 broadcasts message to other drones.

Figure 7: Drone-2-Drone Communication

7.1. Formal Security Analysis

This section provides the formal security analysis of the proposed system. AVISPA [35] is an advanced simulation tool for cryptographic schemes. The results of the AVISPA tool are shown in Figure 9, which clearly defines the security level of the proposed model. AVISPA is a high-level language that uses Python for coding and defining protocols. It is used for integration protocols associated with security. As the major threats exist in the session establishment phase it needs to be strong. The threat model of the proposed scheme assumes that the adversary tries to penetrate the session using a legitimate drone of the network.

This section simulates the proposed scheme on the "Automated Validation of Internet Security Protocol and Application (AVISPA)" tool to show that the proposed model is robust against MiTM attacks [14], session hijacking attacks [23], and message authentication attacks [36]. Which leads the adversary to compute the session key. AVISPA works as a real-time simulation environment. It involves different actors like the sender, receiver, and attacker. In the proposed model, the actors are Drone, Ground Station, and Adversary. The actors are signed by specified roles, divided into two types basic roles and composition roles. The protocols are developed in HLPSL (High-Level Protocols Specification Language), which is a role-oriented language. The adversary is represented by the DY model, and the running protocol is unknown to the adversary (known as an intruder in the tool environment). Several sessions, principles, and fundamental roles are specified in HLPSL. HLPSL is translated to the intermediate format (IF) using the HLPSL2IF

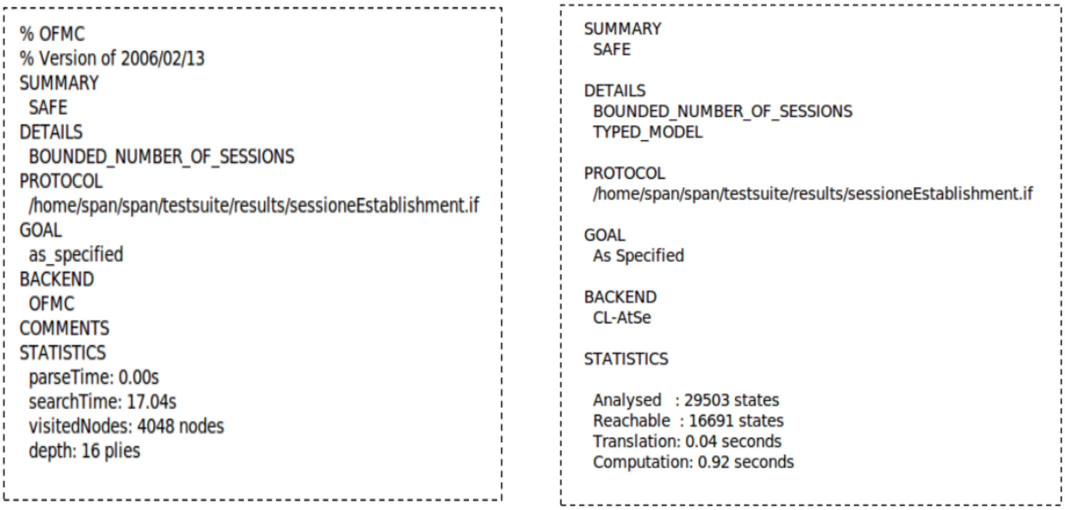


(a) Comparative analysis to check the scalability of the network with respect to the number of transactions increases

(b) Efficiency comparison

Figure 8: Figure is divided into two parts. The first part presents A: Comparative analysis to check the scalability of the network when the number of transactions increases, the second part presents the Efficiency comparison

translator, and then the output format (OF) is produced using one of four backends that are SAMTC, OFMC, TA4SP, and CL-AtSe. The simulation is conducted in OFMC and CL-AtSe environments.



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/sessioneEstablishment.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 17.04s
 visitedNodes: 4048 nodes
 depth: 16 plies
```

```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/sessioneEstablishment.if

GOAL
 As Specified

BACKEND
 CL-AtSe

STATISTICS

 Analysed   : 29503 states
 Reachable  : 16691 states
 Translation: 0.04 seconds
 Computation: 0.92 seconds
```

Figure 9: (A:Results of Simulation in OFMC) (B:Results of Simulation in CL-AtSe)

7.1.1. Resilience to Botnet Attack

Assume an adversary physically captures a drone that is on routing and uses it as a botnet. The adversary knows all the basic information that was embedded in the drone, and we assume it is also successful in achieving the session key. Using the session key adversary can be able to communicate and access the traffic in the network. To secure that we use a technique in which before communication with any entity drones need to compute codes and want to build confidence and we restrict the routing pattern of drones. For example, drones cannot directly communicate with each other before creating an Ad-Hoc network drone needs to send msg to the GS and compute codes if GS approves the request, then the drone can create an Ad-Hoc network [37]. Further, GS can detect fake nodes by behavior detection as the drone's patterns are fixed if any drone works in a different pattern it will be easily detected. In this case, the adversary knows the behavior detection technique as it is widely used in such systems, and succeeds in passing. Then it cannot fetch records or data, as all the communication is done over IOTA and IOTA provides strong data privacy and security. So, it's hard for the adversary to communicate and fetch records. Our security surveillance system is robust against botnet attacks.

7.1.2. Detecting Malicious Drone

The malicious drone is detected through codes ($Code1, Code2, Code3$). As drones are moving nodes, they can be faked in the network or can be created by bots. In this case, the adversary is unknown to the network's confidence-building scenario. We assume one drone in a network is physically captured, and an adversary using the same session that is established between that drone and GS penetrates the network. The adversary has all the basic information of the network, but it is unknown about the codes. The adversary sends the message to the GS to transfer information. GS sends $Code1$ to the Dr to validate the drone. The adversary drone receives $Code1$ and tries to compute it but unknown to its mechanism fails to compute. We assume two scenarios that could happen when the adversary will compute $Code1$. First, the timestamp expires and GS does not receive any reply, or GS gets the wrong answer. Then GS will terminate the session with that node and will mark it as a suspicious node. As that drone will be removed from the session it could not further communicate with GS or any other node.

7.2. IS security Analysis

In the following sections, we show that our model has the potential to protect from different attacks:

7.2.1. Message Authentication

As we are using the ECDSA signature scheme, it provides security to the messages in a way that without a private key message cannot be signed. To validate the message, it must be signed by the private key [38]. Furthermore, the certificate is computed to check the authenticity of the message. Therefore, a receiver can verify the authenticity of the message through a certificate.

7.2.2. Modification Attack

We assume that the attacker is in the system by botnet attack which is explained in previous sections. The attacker broadcasts the message to other drones using the session key of that drone. But in our system model, drones cannot directly communicate with other drones as it needs to create an Ad-hoc network first. So, if the attacker broadcasts the message without GS permission, then GS will consider that drone as suspicious as it is behaving differently.

In a scenario where the attacker is not using a botnet attack and tries to communicate with other drones or entities of the network, it will not be possible as all the communication is done over the IOTA, and it provides strong privacy to the data. Drones will not receive any message which is out of the network. In this way modification of messages and communication of attackers is not possible it will be easily detected.

7.2.3. DDoS Attack

Our model uses an IOTA network which is a distributed network and provides security from DDoS attacks. In case, an attacker launches a DDoS attack on our GS servers, then still our data and records will be safe as they are stored in IOTA. So, our proposed model is safe from DDoS attacks.

7.2.4. Man-in-the-middle Attack

Assume that attackers can eavesdrop on the traffic. It can listen to communication or can access the messages transferred between GS and Drones. However, due to less knowledge of the secret credentials, it cannot decrypt the messages. To tamper the message, it also needs secret credentials to generate valid signatures and timestamps. Due to the strong cryptographic scheme, the attacker can not launch a MiTM attack.

8. Conclusion

In summary, this study introduces a model designed to enhance the security of Internet of Drones (IoD) surveillance systems and facilitate secure transactions among network nodes. The model enables efficient and secure communication between devices, offering robust protection against botnet attacks through a confidence-building scenario. Simulations and security analyses validate the model's effectiveness, highlighting its superiority in terms of scalability, efficiency, cost-effectiveness, and security when compared to the scheme proposed by Faraji et al. [12].

In conclusion, the proposed model establishes a robust framework for ensuring secure communication and transactions within drone networks, contributing to the advancement of IoD surveillance systems. Future research directions may include further optimization of the model to enhance its efficiency and scalability. Additionally, exploring additional applications and scenarios within drone networks could yield valuable insights for advancing the field of IoD surveillance systems.

References

[1] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, J. Chen, Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges, IEEE Communications Magazine 56 (2018) 68–74.

[2] M. Yahuza, Mohd yamani idna idris, Ismail Bin Ahmedy, Ainuddin Wahid Abdul Wahab, Tarak Nandy, Noorzaily Mohamed Noor, and Abubakar Bala. "Internet of Drones Security and Privacy Issues: Taxonomy and Open Challenges 9 (2021) 57243–57270.

[3] R. Nouacer, M. Hussein, H. Espinoza, Y. Ouhammou, M. Ladeira, R. Casti neira, Towards a framework of key technologies for drones, Microprocessors and Microsystems 77 (2020).

[4] R. N. Akram, K. Markantonakis, K. Mayes, O. Habachi, D. Sauveron, A. Steyven, S. Chaumette, Security, privacy and safety evaluation of dynamic and static fleets of drones, In 2017 (2017) 1–12.

[5] S. H. Alsamhi, O. Ma, M. S. Ansari, F. A. Almalki, Survey on collaborative smart drones and internet of things for improving smartness of smart cities, Ieee Access 7 (2019) 28125–12815.

[6] Y. Jin, Z. Qian, W. Yang, Uav cluster-based video surveillance system optimization in heterogeneous communication of smart cities, IEEE Access 8 (2020) 55654–55664.

[7] T. Alsboui, Y. Qin, R. Hill, H. Al-Aqrabi, Enabling distributed intelligence for the internet of things with iota and mobile agents, Computing 102 (2020) 1345–1363.

[8] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, A. Tuncer, Uav-enabled intelligent transportation systems for the smart city: Applications and challenges, IEEE Communications Magazine 55 (2017) 22–28.

[9] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. Luong, N. C., D., ... and Guizani, M. (2021), A comprehensive survey. IEEE Communications Surveys & Tutorials, Fast, reliable, and secure drone communication, ????

[10] M. Sharma, B. Narwal, R. Anand, A. K. Mohapatra, R. Yadav, Psecas: A physical unclonable function based secure authentication scheme for internet of drones, Computers and Electrical Engineering 108 (2023) 108662.

[11] A. D. E. Berini, M. A. Ferrag, B. Farou, H. Seridi, Hcala: Hyperelliptic curve-based anonymous lightweight authentication scheme for internet of drones, Pervasive and Mobile Computing 92 (2023) 101798.

[12] M. Faraji-Biregani, R. Fotohi, Secure communication between uavs using a method based on smart agents in unmanned aerial vehicles, The journal of supercomputing 77 (2021) 5076–5103.

[13] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, M. Alazab, Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment, IEEE Transactions on Vehicular Technology 69 (2020) 9097–9111.

[14] C. D. Nguyen, N. Pubudu, M. D. Pathirana, A. Seneviratne, Blockchain for 5g and beyond networks: A state of the art survey, Journal of Network and Computer Applications 166 (2020).

[15] Y. Tian, J. Yuan, H. Song, Efficient privacy-preserving authentication framework for edge-assisted internet of drones, Journal of Information Security and Applications 48 (2019).

[16] A. Irshad, S. A. Chaudhry, A. Ghani, M. Bilal, A secure blockchain-oriented data delivery and collection scheme for 5g-enabled iod environment, Computer Networks 195 (2021).

[17] J. P. A. Yaacoub, H. N. Noura, O. Salman, A. Chehab, Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations, International Journal of Information Security, 2021. doi:10.1007/S10207-021-00545-8.

[18] G. B. T. Alladi, V. Chamola, M. Guizani, Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication, IEEE Transactions on Vehicular Technology 69 (????) 15068–15077.

[19] K. Yoon, D. Park, Y. Yim, K. Kim, ., S. Y.- 2017 (2021).

[20] M. Wazid, B. Bera, A. K. Das, S. Garg, D. Niyato, M. S. Hossain, Secure communication framework for blockchain-based internet of drones-enabled aerial computing deployment, IEEE Internet of Things Magazine 4 (2021) 120–126.

[21] H. Zhang, J. Wang, Y. Ding, Blockchain-based decentralized and secure keyless signature scheme for smart grid, Energy 180 (2019) 955–967.

[22] E. H. Abualsauod, A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network, Computers and Electrical Engineering 99 (2022).

[23] B. Li, Z. Fei, Y. Zhang, M. Guizani, Secure uav communication networks over 5g, IEEE Wireless Communications 26 (2019) 114–120.

[24] G. Militaru, D. Popescu, L. Ichim, . uav-to-uav communication options for civilian applications, In 26 (2018) 1–4.

[25] C. Lin, D. He, N. Kumar, K. Choo, K. R., A. Vinel, X. Huang, Security and privacy for the internet of drones: Challenges and solutions, IEEE Communications Magazine 56 (????) 64–69.

[26] S. Sun, Z. Ma, H. G. L. Liu, J. Peng, . detection of malicious nodes in drone ad-hoc network based on supervised learning and clustering algorithms, in: In16th International Conference on Mobility, Sensing and Networking (MSN) . IEEE.(2020, December, 2020, pp. 145–152.

[27] M. Wang, M. Duan, J. Zhu, Research on the security criteria of hash functions in the blockchain, in: Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, 2018.

[28] A. Abdalla, P. S., M. K., V., & geraci, g, UAV-assisted attack prevention, detection, and recovery of 27 (2020) 40–4723.

[29] X. Wang, M. Cheng, J. Eaton, C. J. Hsieh, F. Wu, Attack graph convolutional networks by adding fake nodes. arxiv, 2018. arXiv:1810.10751, preprint.

[30] S. F. Shetu, M. Saifuzzaman, N. N. Moon, F. N. Nur, A survey of botnet in cyber security, in: 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), IEEE, 2019, pp. 174–177.

[31] W. F. Silvano, R. Marcelino, Iota tangle: A cryptocurrency to communicate internet-of-things data, Future Generation Computer Systems 112 (2020) 307–319.

[32] R. Duerr, D. Dimartino, C. Marier, P. Zappile, G. Wang, J. Lighter, B. Elbel, A. B. Troxel, A. Heguy, Dominance of alpha and iota variants in sars-cov-2 vaccine breakthrough infections in new york city, The Journal of Clinical Investigation 131 (2021) 18.

[33] A. Ossamah, Blockchain as a solution to drone cybersecurity, In 2020 (2020) 1–9.

[34] T. Alladi, et al., Applications of blockchain in unmanned aerial vehicles: A review, Vehicular Communications 23 (2020).

[35] A. Kanade, Vijay "Securing Drone-based Ad Hoc Network Using Blockchain." 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), IEEE, 2021.

[36] A. Kumari, R. Gupta, S. Tanwar, N. Kumar, A taxonomy of blockchain-enabled softwarization for secure uav network, Computer Communications 161 (2020) 304–323.

[37] Y. Tian, J. Yuan, H. Song, Efficient privacy-preserving authentication framework for edge-assisted internet of drones, Journal of Information Security and Applications 48 (2019).

[38] D. Bera, Chattaraj, and a, K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,” Computer Communications 153 (2020) 229–249.