electronics

MDPI

Article

Research of Security Routing Protocol for UAV Communication Network Based on AODV

Xiaopeng Tan, Zhen Zuo *, Shaojing Su, Xiaojun Guo and Xiaoyong Sun

College of Intelligence Science and Technology, National University of Defense Technology, Changsha 410073, China; tanxiaopeng14@nudt.edu.cn (X.T.); susj-5@163.com (S.S.); jeanakin@nudt.edu.cn (X.G.); sunxiaoyong14@nudt.edu.cn (X.S.)

* Correspondence: z.zuo@nudt.edu.cn; Tel.: +86-130-7733-7333

Received: 1 July 2020; Accepted: 21 July 2020; Published: 23 July 2020

Abstract: With the rapid development of information technology and the increasing application of UAV in various fields, the security problems of unmanned aerial vehicle (UAV) communication network have become increasingly prominent. It has become an important scientific challenge to design a routing protocol that can provide efficient and reliable node to node packet transmission. In this paper, an efficient Digital Signature algorithm based on the elliptic curve cryptosystem is applied to routing protocol, and an improved security method suitable for on-demand routing protocol is proposed. The UAV communication network was simulated through the NS2 simulation platform, and the execution efficiency and safety of the improved routing protocol were analyzed. In the simulation experiment, the routing protocols of ad-hoc on demand distance vector (AODV), security ad-hoc on demand distance vector (SAODV), and improved security ad-hoc on demand distance vector (ISAODV) are compared in terms of the performance indicators of packet delivery rate, throughput, and end-to-end delay under normal conditions and when attacked by malicious nodes. The simulation results show that the improved routing protocol can effectively improve the security of the UAV communication network.

Keywords: UAV communication network; routing protocol; security; performance analysis

1. Introduction

With the progress and development of science and technology, UAV is becoming more and more mature in technology and widely used in production and life. UAV has the advantages of low cost, small size, light weight, easy to operate, high flexibility, high adaptability, high stability, and easy concealment. Therefore, it plays an important role in dealing with film and television shooting, agricultural monitoring, electric cruise, meteorological monitoring, forest fire detection, and emergency rescue [1–4].

With the wide application of UAV in production and life, how to improve the communication quality of UAV communication network has become a research hotspot. The UAV communication network is an extended application of mobile ad-hoc networks (MANET) in the field of UAV [5–7]. Each UAV node in the UAV communication network has an equal status. It does not need to set up any node responsible for central control, and it has a strong anti-destructive ability. Network nodes not only have the functions required by ordinary mobile terminals, but also have the ability of data packet forwarding. When the source node and the destination node are not in the range of direct communication with each other, data packets can be forwarded through the intermediate node for communication. Sometimes data packets need to be forwarded by multiple nodes to reach the sink node [8–10]. The UAV communication network adopts the form of a dynamic network to complete the interconnection of the internal members of the cluster. The advantages of its networking are

self-intelligent organization, automatic healing, and high performance, and low latency, which can meet the needs of a UAV cluster in special scenarios [11–13].

The UAV communication network has the characteristics of open channel, dynamic topology, no center authorization, distributed cooperation, and limited bandwidth. Therefore, the security of its routing protocol is much more complex than traditional networks, and some existing security solutions for wired networks cannot be directly applied to UAV communication networks. However, the existing routing protocols in MANET only focus on the function and efficiency of route discovery, and hardly mention the security of the protocols [14–17]. The AODV routing protocol is widely used in UAV communication networks because of its simplicity and low control overhead. However, it does not have any security mechanism, and it is easily attacked by various malicious nodes [18–20]. Figure 1 shows the attacked UAV communication network. When the UAV communication network is attacked by malicious nodes, the wireless signal is easily intercepted and interfered. At this time, the UAV communication network is more vulnerable to network attacks such as eavesdropping, active intrusion, and denial of service. Therefore, designing an efficient and secure routing protocol for UAV communication networks is particularly critical [21–24].

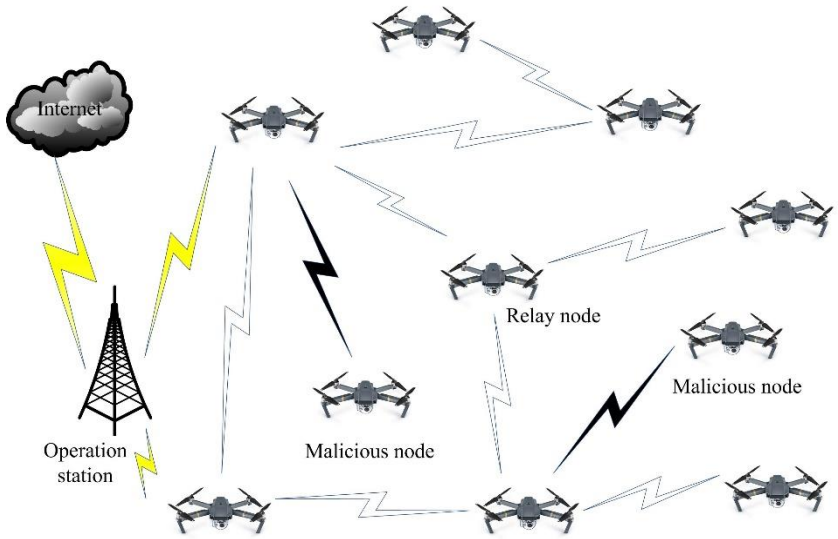

Figure 1. The attacked unmanned aerial vehicle (UAV) communication network.

Shounak et al. [25] proposed a secure protocol based on an optimization algorithm, Monarch-Earthworm Algorithm (Monarch-EWA), which is the modification of the Monarch Butterfly algorithm using the Earthworm Optimization Algorithm (EWA) in order to render effective security to the network. Alouache et al. [26] researched, compared, and classified enhanced vehicle routing protocols with different security mechanisms, including authentication, integrity, confidentiality, non-repudiation, and availability of data and communications. Liu et al. [27] proposed a trust detection-based secured routing (TDSR) scheme to establish security routes from source nodes to the data center under malicious environment to ensure network security. Neumann et al. [28] presented the design and analysis of securely-entrusted multi-topology routing (SEMTOR), a set of routing-protocol mechanisms that enable the cryptographically secured negotiation and establishment of concurrent and individually trusted routing topologies for infrastructure-less networks without relying on any central management. Kavitha et al. [29] proposed the framework that deals with the security flaws through hyper elliptic curve based public key cryptosystem, which combines Digital Signature Algorithm (DSA), ElGamal approaches that ensure the entity authentication, and secure group communication.

The UAV information transmission is a complex task. It is important to design a routing protocol that can provide efficient and reliable node to node packet transmission. In this paper, an efficient digital signature algorithm based on elliptic curve cryptosystem is applied to routing protocol,

and an improved security method suitable for on-demand routing protocol is proposed. Through the simulation of three routing protocols (AODV, SAODV and ISAODV), the performance indicators such as packet delivery rate, throughput, end-to-end delay, and routing overhead are compared and studied. The simulation results show that the performance of the ISAODV and SAODV routing protocols in terms of packet delivery rate, throughput, and routing overhead is very close to the AODV routing protocol. This shows that the ISAODV and SAODV routing protocols inherit the characteristics of the AODV routing protocol and maintain the route discovery and route maintenance capabilities of the AODV routing protocol to the greatest extent. In addition, because each node on the active path of the SAODV protocol must be authenticated and signed based on the certification authority (CA) certificate, the complexity of information transmission is much higher than that of ISAODV based on the elliptic curve cryptosystem. The ISAODV routing protocol proposed in this paper effectively reduces the complexity of the algorithm on the basis of improving network security, and provides a powerful guarantee for the security of UAV communication networks.

The remaining sections of this paper are organized as follows. Section 2 describes the principle of security AODV routing protocol. Section 3 describes the principle of improved security AODV routing protocol. Section 4 describes the simulation and numerical results, and the performance indicators such as the packet delivery rate, throughput, and end-to-end delay of the UAV communication network are compared and analyzed. Finally, Section 5 summarizes the paper.

2. Security AODV Routing Protocol

The SAODV protocol divides the routing message into variable part and invariant part for processing according to the characteristics of hop by hop changes in the AODV protocol. The hop number field in the routing message is a variable part, which is authenticated by a hash chain. Other fields in the routing message are invariant parts, which are authenticated by digital signature [30–33].

2.1. Authentication of Variable Parts

The SAODV protocol uses a hash chain to protect the variable part in the route request (RREQ) and route reply (RREP) messages. Hash chain is realized by repeatedly applying one-way hash function to a random number. Each node that receives a RREQ or RREP message can verify the hops field to ensure that it is not maliciously reduced by the attacker. The process of RREQ or RREP routing messages is shown in Algorithms 1.

Algorithms 1 The Process of RREQ or RREP Routing Messages

for each RREQ or RREP **do**
    Generate a random number (seed)
    Set the *Max_Hop_Count* field, and fill the value of the Time field in the IP header
    Set the *Hash* field, and fill the value of seed
    Set the *Hash_Function* field, which indicates the type of hash function used
    Set the *Top_Hash* field: $Top\_Hash = h^{Max\_Hop\_Count-Hop\_Count}(Hash)$
    Verify the hop count information: $Top\_Hash = h^{Max\_Hop\_Count-Hop\_Count}(Hash)$
        if the result is equal to the value in the *Top_Hash* field **then**
            the hop number field is correct
        else
            the hop number field is wrong
        end if
    Calculate the Hash value to record the new hop: $Hash = h(Hash)$
end for

The *Hash_Function*, *Max_Hop_Count*, *Top_Hash*, and Hash fields are transmitted in the AODV extended message. The format definition of the extended message is shown in Figure 2. The RREQ message format of SAODV protocol is increased by 20 bytes on the basis of AODV

format. The increased part is *Type*2, *Length*, *Hash_Function*, *Max_Hop_Count*, *Top_Hash*, *Signature*, *RREP Signature* (*optional field*), *Hash*.

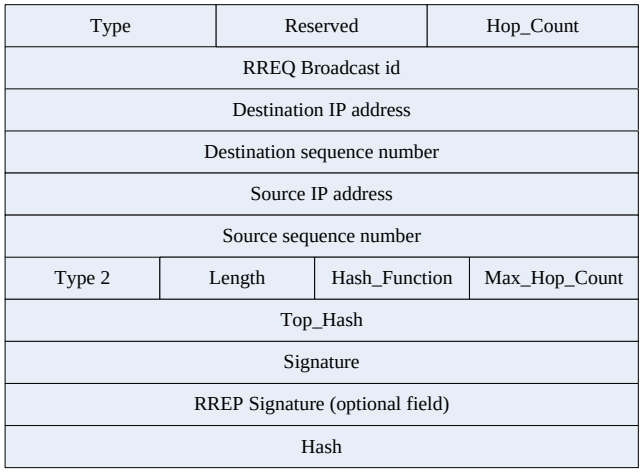

Figure 2. Route request (RREQ) message format of the security ad-hoc on demand distance vector (SAODV) protocol.

2.2. Authentication of Invariant Parts

The SAODV protocol uses digital signatures to authenticate invariant parts of RREQ and RREP messages. The node that sends the routing message signs the invariant part of the routing message. Each node that receives the routing message verifies the signature in the message.

2.3. Intermediate Node Responds to the RREQ Message

In the AODV protocol, when the intermediate node has a sufficiently fresh route to the destination node, it is allowed to reply to the RREQ message. In order to keep this mechanism in the SAODV protocol, an additional RREP signature field is included in the RREQ message broadcast by the source node. The intermediate node uses the RREP signature field to sign the routing response message RREP on behalf of the destination node, thus ensuring that the RREP message generated by the intermediate node can be verified.

In addition, when the intermediate node generates RREP messages, the lifetime of the route changes from the original one. The RREP message generated by the intermediate node contains two lifetimes, the original one and the real one. The original lifetime is signed by the destination node, while the real lifetime is signed by the intermediate node.

In order to distinguish different SAODV signature extension messages, the routing control message with two signatures used by the intermediate node when replying to the RREQ message is called RREQ and RREP double signature extension message.

2.4. The Process of Route Discovery

2.4.1. Generate RREQ Message

When the route to the destination node needs to be obtained, the node broadcasts a RREQ message. The RERQ message has a signature for the invariant part and a hash chain for the variable part. If the intermediate node is allowed to reply, the RREQ message is generated in the form of a double signature extended message with additional RREP signature fields. Otherwise, the RREQ message is generated according to the RREQ signature extension message format.

2.4.2. Processing RREQ Message

After a node receives the RREQ message, it first determines whether it has received the message in the most recent time. If it has received, the message is discarded; otherwise, the signature and hops in the message are verified. Only when the verification is correct, the reverse path corresponding to the message will be stored.

If the RREQ message is in the double-signature extended format, the node stores the RREP signature field in the RREQ message while storing the reverse path; otherwise, the field is not stored.

The node then determines whether it is the destination node. If it is, a RREP message response is generated. If it is not, but the node meets the conditions for the intermediate node to respond to the RREQ message, and has the corresponding RREP signature field, the node generates a RREP double-signature extended message to respond to the RREQ message. Otherwise, the node performs a hash operation on the hop number field of the RREQ message and broadcasts it continuously.

2.4.3. Generate RREP Message

When the destination node generates the RREP message, the node fills the destination node IP address, destination node serial number, next hop node and other relevant information into the corresponding fields of the RREP message, and signs and hashes the message. The message has a signature for the invariant part and a hash chain for the variable part.

The RREP message generated by the intermediate node is in a double-signature extended format. As described in Section C, it has two more lifetimes and signature fields corresponding to the lifetimes than the RREP message in the signature extension format generated by the destination node.

2.4.4. Processing RREP Message

After a node receives the RREP message, it first verifies its signature and hop number fields. Only when the verification is correct, the node stores the forward path corresponding to the message; otherwise, the message is discarded.

Then, the node determines whether it is the destination node. If it is, the process of route discovery is finished. Otherwise, the RREP message is sent according to the reverse path in the routing table.

2.5. Protection of Route Error (RERR) Message

The SAODV protocol uses hop-by-hop signatures to protect all fields of the RERR message. The nodes that generate or transmit RERR messages sign it. The nodes that receive the RERR message verify it. This can ensure the integrity and resistance of the RERR message. However, because the serial number of the destination node is not signed by the corresponding node, in order to ensure the security of the protocol, when processing the RERR message, the node will not update its destination node serial number according to the RERR message.

3. Improved Security AODV Routing Protocol

The SAODV routing protocol is based on the RSA public key cryptosystem [34], which introduces a lot of computational overhead while enhancing security. Certificates need to be introduced to verify the public key. The verification, transmission, management, and revocation of certificates bring a lot of storage, calculation, and communication overhead. Therefore, this paper studies the improved secure AODV routing protocol, which is based on elliptic curve cryptosystem.

3.1. Elliptic Curve Cryptosystem

Elliptic curve cryptosystem (ECC) is one of the three types of public key cryptosystems that have been proved to be safe and effective so far, and is known for its high efficiency. The security of ECC is based on the intractability of elliptic curve discrete logarithm problem (ECDLP), and it has the

advantages of short key, short signature, and small software implementation scale [35–38]. The elliptic curve defined on the finite field $F(q)$ is as follows:

Assuming $q > 3$, and $4a^3 + 27b^2 \neq 0 \bmod q$, the curve

$$y^2 \equiv x^3 + ax + b(\text{mod}) \ \ a, b \in F(q) \tag{1}$$

is called an elliptic curve on the finite field $F(q)$, which can be represented as $E_q(a, b)$.

3.1.1. Addition Rule of Elliptic Curve

For any two points $P(x_1, y_1)$ and $Q(x_2, y_2)$ on the elliptic curve, there is a third point $R(x_3, y_3) = P + Q$ also on the elliptic curve.

When $P(x_1, y_1) \neq Q(x_2, y_2)$,

$$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3) \tag{2}$$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = (y_2 - y_1)/(x_2 - x_1) \end{cases} \tag{3}$$

When $P(x_1, y_1) = Q(x_2, y_2)$,

$$P(x_1, y_1) + Q(x_2, y_2) = 2P(x_1, y_1) = R(x_3, y_3) \tag{4}$$

$$\begin{cases} x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \\ \lambda = \left(3x_1^2 + a\right)/2y_1 \end{cases} \tag{5}$$

Among them, a is the first-order coefficient in the elliptic curve equation.

3.1.2. Scalar Multiplication of Elliptic Curves

Assuming that m is an integer and G is a point on an elliptic curve, scalar multiplication can be expressed as follows:

$$mG = m \times G = \underbrace{G + G + \cdots + G}_{m} \tag{6}$$

3.1.3. Elliptic Curve Discrete Logarithm Problem

The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). The difficulty of ECDLP is that it is difficult to find the integer L for the discrete points P and Q on the curve, so that LP = Q. When applying an elliptic curve to a cryptosystem, assuming that P is the public key and Q is the private key, its security is that it knows P but cannot derive Q. For a and b on a finite group, if there is a positive integer n, making $a^n = b$, the problem of solving $n = \log_a^b$ is called the discrete logarithm problem on a finite group. For the discrete points P and Q on the elliptic curve, solving L makes LP = Q, which is called the elliptic curve discrete logarithm problem.

The attractive point of ECC is that its key length is shorter when the security is equal. For example, RSA uses a 1024 bit module length to obtain security, and in the elliptic curve cryptosystem, a 160 bit module length can obtain the same security. Table 1 shows the security analysis and comparison between ECC and RSA. Million instructions per second for one year (MIPS-a) in the table refers to the computer that executes 1 million instructions per second runs for one year. At present, it is considered that when the deciphering time is 1012 MIPS-a, it represents security. Compared with other public key systems such as RSA and DSA, ECC can provide better encryption strength, faster execution speed,

and shorter key length. Table 2 shows the comparison of signature length and encrypted message length when the data length to be signed and encrypted is 2000 bit and 100 bit, respectively. A short key means a reduction in computing overhead, storage space, and bandwidth requirements. Therefore, ECC is more suitable for the UAV communication network with limited resources such as bandwidth, storage capacity, and CPU computing power.

Table 1. Security analysis and comparison between elliptic curve cryptosystem (ECC) and RSA.

Deciphering Time/MIPS-a	RSA Key Length/Bit	ECC Key Length/Bit	RSA/ECC Key Length Ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{12}	1024	160	7:1
10^{20}	2048	210	10:1

Table 2. Comparison of signature and encryption length of several cryptosystems.

	Signature Length/Bit	Encrypted Message Length/Bit
RSA	1024	1024
DSA	320	-
ElGamal	-	2048
ECC	320	320

3.2. Secure Routing Scheme Based on ECC

In order to adapt to the limited resources in UAV communication network, this paper studies a secure and efficient digital signature scheme based on SAODV routing protocol. Compared with other public key systems such as RSA, DSA, elliptic curve cryptosystem (ECC) can provide better encryption strength, faster execution speed, and shorter key length.

3.2.1. Digital Signature Scheme Based on Elliptic Curve

It is assumed that network bandwidth resources in the network are limited, and nodes can move freely, and communicate with each other through wireless multi hop channels. The relationship between nodes in the network is also dynamic, and nodes can join or leave at any time. The wireless link between nodes is bidirectional, and the nodes within the range of each other's communication are called neighbor nodes. This scheme assumes that there is a trusted system authorization center (such as distributed certification authority system) in the network, which can verify the validity of each user's identity, and generate a self-certified public key for the user according to the user's identity and other information. Table 3 shows the symbol definition of this secure routing scheme.

Table 3. Symbol definition.

Symbol	Definition
ID_i	Identity information of node i
q	The size of a finite field, which is a prime or a power of two, is about 160 bits long.
$E(F_q)$	Elliptic curve based on finite field F_q
G	The base point on the $E(F_q)$, whose order is n, where n is a large prime (160 bits)
$X(G)$	Take the abscissa value of point G
S_u	Private key of node u
P_u	Public key of node u
M	Routing information to be signed
A	Node that signs routing information
B	Node that verifies signature
S_{SA}	Private key of system CA, $S_{SA} \in [2, n-2]$
P_{SA}	Public key of system CA, and $P_{SA} = S_{SA}G$
$h(\cdot)$	One-way hash function

The process of user U_i registering with system CA is shown in Algorithms 2. It can be seen from the above process that the system CA only generates the user's public key, and the user's private key is generated by the user itself, and the user can verify the authenticity of the public key with the private key generated by itself, so the problem of secure distribution of the user's private key is avoided. After users obtain their own public and private key pairs, they can use the following process for signature and verification.

Algorithms 2 The Process of User U_i Registering with System CA

for each U_i **do**
  Select a user identity information, expressed as I_i
  Randomly select an integer $x_i \in [2, n-2]$ as the random key
  Calculate $V_i = h(x_i \| I_i) \cdot G$
  Submit $\{I_i, V_i\}$ to system CA
  Randomly select an integer variable $k_i \in [2, n-2]$
  Calculate the public key P_i and public key evidence w_i:
$P_i = V_i + (k_i - h(I_i)) \times G = \left(P_{ix} \times P_{iy}\right)$
$w_i = k_i + S_{SA} \times (P_{ix} + h(I_i))(\mathrm{mod} n)$
  Return $\{P_i, w_i\}$ to user U_i
  U_i generates its own private key: $s_i = w_i + h(x_i \| I_i)(\mathrm{mod} n)$
  Verify the authenticity of user public key: $s_i \times G = P_i + h(I_i) \times G + [(P_{ix} + h(I_i))\mathrm{mod} n] \times P_{SA}$
end for

The process of signature and verification is shown in Algorithms 3. It can be seen from the above signature scheme that the public key of the system CA is used in the signature verification process, so that the signature verification process and the validity verification of the public key are completed in one step, thereby avoiding the introduction of certificates to verify the validity of the public key. There is no need to pass certificates during the routing process, which reduces communication, calculation, and storage costs.

Algorithms 3 The Process of Signature and Verification

for each U_i **do**
  A randomly selects an integer variable k, $k \in [2, n-2]$
  Calculate $R = k \times G$, $r = X(R)(\mathrm{mod} q)$, $s = k + S_a \times h(M \| r)(\mathrm{mod} n)$
  A transmits signature (r, s) and M to B
  B calculates V_a: $V_a = P_a + h(ID_a) \times G + [(X(P_a) + h(ID_a))\mathrm{mod} n] \times P_{SA}$

$$\begin{aligned} s \times G - h(M \| r) \times V_a &= k \times G + S_a \times h(M \| r) \times G - h(M \| r) \times (S_a \times G) \\ &= k \times G = (x_1, y_1) \end{aligned}$$

  if $x_1 = r(\mathrm{mod} q)$ **then**
    the signature is valid
  else
    the signature is invalid
  end if
end for

3.2.2. The Process of Routing Discovery

The routing process of the AODV routing protocol mainly relies on RREQ, RREP, and RERR to control the transmission of messages. This is also the main attack target of malicious nodes against the routing protocol. Therefore, these messages must be protected to prevent attacks such as tampering or forgery by malicious nodes.

Figure 3 shows a simple network model for secure route discovery. In the path shown in the figure, the source node is S, the destination node is D, and A and B are intermediate nodes. When S has

data to send, but it has no route to the destination node or the route has expired, S randomly selects an integer $X_s \in [2, n-2]$ and calculates $T_s = X_s \times G(\mathrm{mod} q)$ to broadcast the route request information.

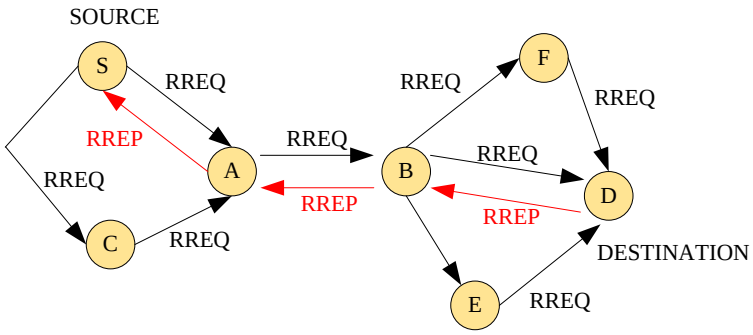

Figure 3. Simple network model for secure route discovery.

$$S \rightarrow * : [RREQ, Hash\_NC, RREQ\_CF\_Hash, RREQ\_FF\_Sig_s, (Null), E_{k_d}(T_s)]$$

Among them, *Hash_NC* is the invariant part related to hash information in the message. *RREQ_CF_Hash* is the hash value calculated by the source node S according to the hop value and serial number in the routing request information. $RREQ\_FF\_Sig_s$ is the signature of the source node S to the invariant part. *Null* is the signature of the intermediate node to the invariant part. For the source node, this field is empty. $E_{k_d}(T_s)$ is the encryption protection of the session key negotiation factor by the source node S with the public key of the destination node D.

When intermediate node A receives the routing request packet from source node S, it will perform the following processing.

Step1: According to *RREQ_CF_Hash* and *Hash_NC*, verify whether the hop value and serial number are maliciously modified.

Step2: Verify the signature $RREQ\_FF\_Sig_s$ of the source node with the public key of the source node S.

After the verification is successful, the reverse path to the source node is established, and the hop value is increased by 1, which means that the normal processing of RREQ is followed and the corresponding hash operation is performed. The node updates the value of *RREQ_CF_Hash* field, then signs the message to be forwarded with its own private key, and fills in the *Null* field. The node continues to broadcast the routing request message. At this time, the format of the routing request message is as follows:

$$A \rightarrow * : [RREQ, Hash\_NC, RREQ\_CF\_Hash, RREQ\_FF\_Sig_s, RREQ\_FF\_Sig_A, E_{k_d}(T_s)]$$

After receiving the routing request message, intermediate node B will perform the following operations:

Step1: According to *RREQ_CF_Hash* and *Hash_NC*, verify whether the hop value and serial number are maliciously modified.

Step2: Verify the signature $RREQ\_FF\_Sig_A$ of the previous hop node A.

Step3: Verify the signature $RREQ\_FF\_Sig_s$ of the source node with the public key of the source node S.

After verification, the reverse path to the source node is also established, the hop value is increased by 1, and the corresponding hash operation is performed. The node updates the value of the *RREQ_CF_Hash* field, and then resigns the packet to be forwarded with its own private key and

replaces the signature $RREQ\_FF\_Sig_A$ of the previous hop node. The node continues to broadcast this route request message, the format is as follows:

$$B \rightarrow * : [RREQ, Hash\_NC, RREQ\_CF\_Hash, RREQ\_FF\_Sig_s, RREQ\_FF\_Sig_B, E_{k_d}(T_s)]$$

After receiving the routing request packet, the destination node performs the same process, decrypts T_s with its own private key after successful verification, and randomly selects an integer $X_d \in [2, n-2]$ to calculate $T_d = X_d \times G(\mathrm{mod}q)$. According to the established reverse path, unicast route replies the message to the previous hop node B.

$$D \rightarrow B : [RREQ, Hash\_NC, RREQ\_CF\_Hash, RREQ\_FF\_Sig_d, Null, E_{k_s}(T_d)]$$

After receiving the message, the intermediate node also performs relevant verification first. The process is the same as the routing request process, which is not described here. Finally, the source node S receives the RREP message, and after all verifications are passed, it also decrypts T_d with its own private key, and the process of route discovery ends.

After the source node and the destination node receive T_d and T_s, respectively, their shared session key can be calculated. The calculation process of source node S is as follows:

$$V_d = P_d + h(ID_d) \times G + [(X(P_d) + h(ID_d))\mathrm{mod}n] \times P_{SA} \tag{7}$$

$$SK = X_s \times V_d + S_s \times T_d = (X_s S_d \mathrm{mod}n) \times G + (S_s X_d \mathrm{mod}n) \times G \tag{8}$$

The calculation process of destination node D is as follows:

$$V_s = P_s + h(ID_s) \times G + [(X(P_s) + h(ID_s))\mathrm{mod}n] \times P_{SA} \tag{9}$$

$$SK = X_d \times V_s + S_d \times T_s = (X_d S_s \mathrm{mod}n) \times G + (S_d X_s \mathrm{mod}n) \times G \tag{10}$$

In this way, the source node S and the destination node D have the shared session key SK. In the next stage of data transmission, the efficient symmetric cryptosystem can be used to complete the secure transmission of a large number of real-time data.

3.2.3. The Process of Routing Maintenance

When a link is interrupted due to node movement or node energy exhaustion in the routing path, the upstream node of the link will send a routing error message (RERR) to notify the upstream node containing this path to delete the corresponding routing table entry. In order to prevent malicious nodes from publishing false routing error information by forging RERR messages, it is necessary to perform identity authentication on the nodes that send RERR messages. Therefore, the intermediate node must sign the RERR message with its own private key. Assume that in Figure 3, the link between nodes A and B is interrupted, and node A will send a routing error message along the reverse path to notify source node S to delete the corresponding routing table entry.

$$A \rightarrow S : [RERR, RERR\_Sig_A]$$

After receiving the routing error message, the upstream node authenticates the source node of the message. Only after the source node of RERR message is authenticated can the corresponding routing table entries be deleted from the routing table. This prevents the illegal node from destroying the network operation by forging the RERR message.

4. Simulation and Numerical Results

In this paper, the network simulation software NS2 with an open source code and good scalability is used to build a network simulation platform, and the effectiveness of the proposed secure routing

scheme is verified through simulation and evaluation. Table 4 shows the simulation parameters setting of the UAV communication network based on NS2. In this paper, the UAV communication network is arranged in a geographical range of 1000 m × 1000 m. The UAV uses a random waypoint model and the data rate is set to 1 Mbps. The MAC protocol adopts 802.11 b protocol. The CBR source generates four packets per second, and the size of each packet is 512 bytes. Each simulation time is 300 s.

Table 4. Symbol definition.

Parameter	Value
Moving range of UAV	1000 m × 1000 m
UAV mobile model	Random waypoint
Number of UAVs	50
Maximum speed of UAV	0–20 m/s
Traffic type	CBR
Packet transmission rate	4 packet/s
The size of packet	512 Byte
MAC protocol	802.11 b
Data rate	1 Mbps
Routing protocol	AODV, SAODV, ISAODV
Simulation time	300 s
Carrier sensing distance	550 m
UAV node coverage	250 m
Bandwidth	2 Mbps
Transmission power	0.28 W

The UAV communication network has the characteristics of open channel, dynamic topology, no center authorization, distributed cooperation, and limited bandwidth. It adopts the form of dynamic network to complete the interconnection of the internal members of the cluster. Considering the limited bandwidth and low capacity of UAV communication network, it is easy to be affected by signal collision and noise interference during communication. In this paper, the carrier sensing distance of the UAV communication network is set to 550 m, the UAV node coverage is set to 250 m, the bandwidth is set to 2 Mbps, and the transmission power is set to 0.28 W. All parameter settings support the special nature of the UAV communication network.

In this paper, packet delivery radio (PDR), average throughput, and average end-to-end delay are obtained to evaluate the performance of the proposed secure routing protocol.

$$\text{PDR} = \frac{\text{Number of packet received}}{\text{Number of packet sent}} \tag{11}$$

PDR is the ratio of the number of packets received to the number of packets sent. From this ratio, it can be seen that the number of data was successfully transmitted in the whole network and the amount of data was lost due to link failure in the transmission process. This parameter can well reflect the efficiency of the routing protocol in data transmission.

$$\text{Throughput} = \frac{\text{reiceived packets} \times \text{packet size} \times 8}{\text{Total time of transmission}} \tag{12}$$

Network throughput characterizes the network transmission rate. The larger the throughput, the higher the transmission rate.

$$\text{Delay} = \frac{\sum(\text{Arrive time} - \text{Send time})}{\text{Number of connection}} \tag{13}$$

The end-to-end delay refers to the time between the source node sending data and the receiving node receiving data, including routing time and data forwarding time. It can reflect whether the network is unobstructed. The smaller the delay, the better the network.

$$\text{Routing overhead} = \frac{\text{num\_rte\_pkt}}{\text{num\_data\_pkt}} \tag{14}$$

where, num_rte_pkt represents the number of control packets used for route discovery and route maintenance. The num_data_pkt represents the number of data packets received. The routing overhead represents the number of routing control packets needed to successfully transmit a data packet. The smaller the routing overhead, the less additional control packets are required for stable transmission of messages.

The simulation experiment in this paper is divided into two situations. Firstly, the performance of ISAODV is compared with AODV and SAODV under normal conditions. Secondly, the performance of ISAODV is compared with AODV and SAODV after adding malicious nodes.

Figures 4 and 5 show the PDR and throughput of UAV communication network under normal conditions, respectively. As can be seen from the figure, the performance of ISADOV and SAODV routing protocols in the packet delivery rate and throughput is very close to the AODV routing protocol. This shows that the ISAODV and SAODV routing protocols inherit the characteristics of the AODV routing protocol and maintain the route discovery and route maintenance capabilities of the AODV routing protocol to the greatest extent. With the increase of the moving speed of UAVs, the link state changes frequently, and the rate of processing packets decreases, which leads to the decrease of packet delivery rate and throughput. Therefore, the faster the UAV moves, the more unstable the communication quality is.

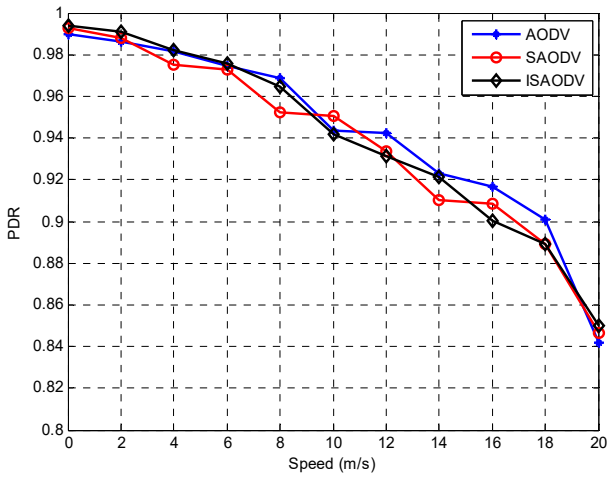

Figure 4. The packet delivery radio (PDR) under normal conditions.

In this paper, the common malicious node attack model is implemented in the simulation experiment. After receiving the RREQ message that does not take itself as the destination node, the malicious node will immediately reply to RREP and set the hop number to 1. The source node chooses the path of the malicious node for data transmission, and all packets passing through the malicious node will be discarded. In the simulation experiment, five malicious nodes are set up.

Figures 6 and 7 show the PDR and throughput of UAV communication network after adding malicious nodes, respectively. As can be seen from the figure, the packet delivery rate and throughput of AODV routing protocol without the security guarantee are much lower than those under normal conditions when there are malicious nodes in the network, and the performance is far lower than ISAODV and SAODV routing protocols. Due to the added security guarantee, the packet delivery rate and throughput of SAODV and ISAODV routing protocols have not decreased significantly with the

addition of malicious nodes. Therefore, SAODV and ISAODV routing protocols can effectively resist malicious node attacks, and the effect of ISAODV is better than SAODV, with higher security.

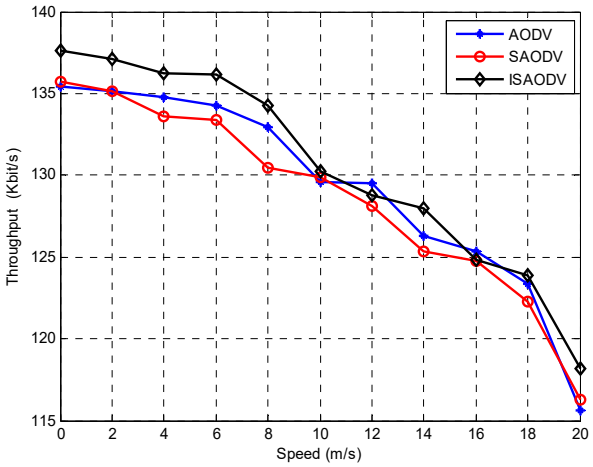

Figure 5. The throughput under normal conditions.

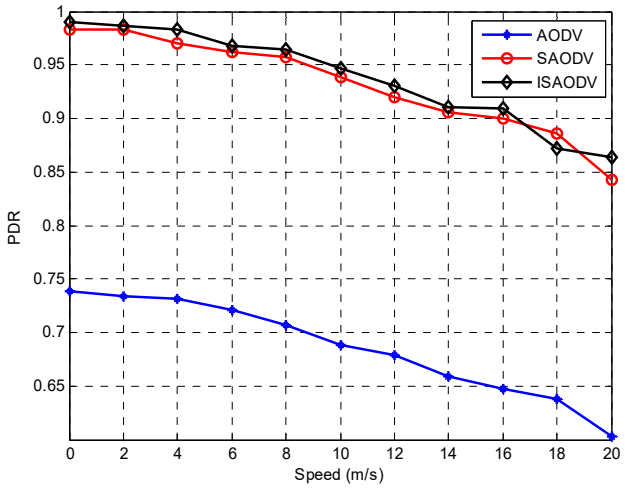

Figure 6. The PDR after adding malicious nodes.

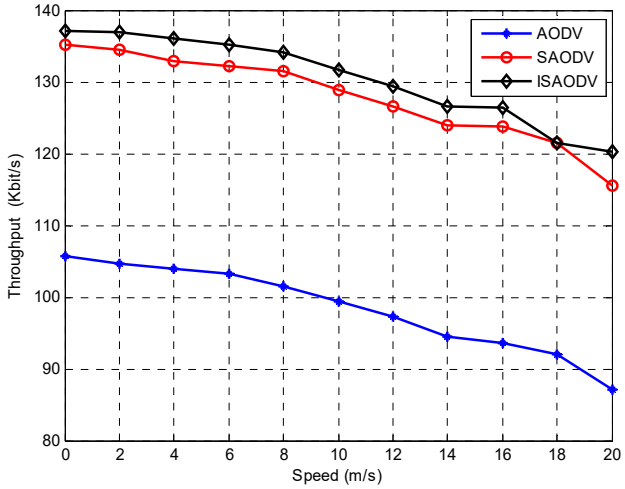

Figure 7. The throughput after adding malicious nodes.

Figure 8 shows the end-to-end delay of UAV communication network under normal conditions. It can be seen from the figure that the delay of AODV is the lowest no matter what mobile rate the

node is. The delay of SAODV is higher than that of ISAODV. This is because the complexity of the algorithm is related to the packet delay. The AODV routing protocol does not consider the security factor, so the complexity of the algorithm is relatively low and the delay is the lowest. Since each node on the active path of the SAODV protocol must be authenticated and signed based on the CA certificate, the complexity of information transmission is much higher than that of ISAODV based on the elliptic curve cryptosystem. The end-to-end delays of the three protocols increase as the speed of the UAV moves. This is because when the link state changes frequently, the chance of signal collision and collision increases, the proportion of route failure increases sharply, and the route reconstruction process suddenly becomes frequent, thereby increasing the end-to-end delay.

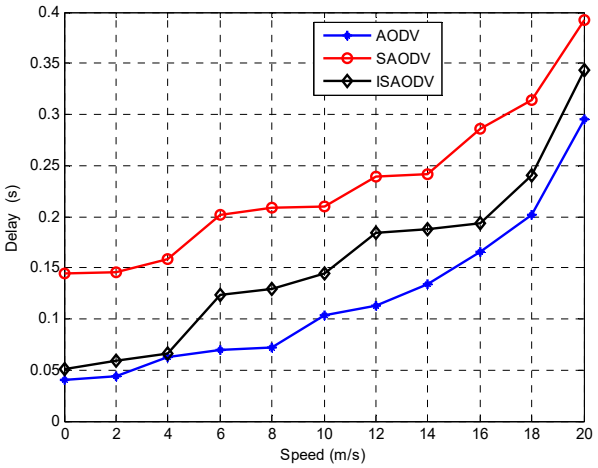

Figure 8. The delay under normal conditions.

Figure 9 shows the end-to-end delay of UAV communication network after adding malicious nodes. As can be seen from the figure, after adding malicious nodes to the network, the end-to-end delay of the AODV routing protocol is still the lowest. This is because the AODV routing protocol does not consider the security factor, and its algorithm complexity is low. Due to the added security guarantees, SAODV and ISAODV routing protocols have higher computational overhead and higher algorithm complexity, so the delay is also higher. Since the algorithm complexity of the SAODV routing protocol is higher than the ISAODV routing protocol based on the elliptic curve cryptosystem, the delay of SAODV is higher than that of ISAODV.

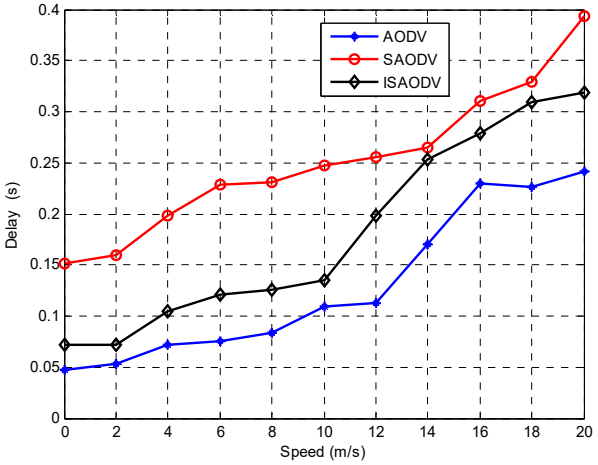

Figure 9. The delay after adding malicious nodes.

Figure 10 shows the routing overhead under normal conditions. It can be seen from the figure that when the UAV moves at a low speed, there is less route breakage, while when the speed increases,

the protocol needs to maintain the route frequently, resulting in a sharp increase in routing overhead. The performance of ISAODV routing protocol is very close to AODV routing protocol in terms of routing overhead, which shows that the improved protocol inherits the characteristics of the original protocol and maintains the routing discovery and maintenance capabilities of the original protocol to the greatest extent. Figure 11 shows the routing overhead after adding malicious nodes. It can be seen from the figure that with the addition of malicious nodes, the routing overhead of AODV routing protocol increases, and the link stability becomes worse, while the routing overhead of ISAODV and SAODV does not change significantly compared with that under normal conditions, which indicates that the secure routing protocol maintains the link stability well. Moreover, the routing overhead of ISAODV is the smallest among the three protocols, and the link stability is the best.

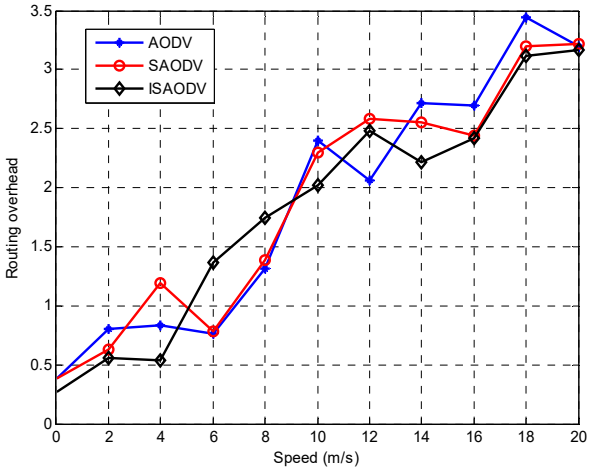

Figure 10. The routing overhead under normal conditions.

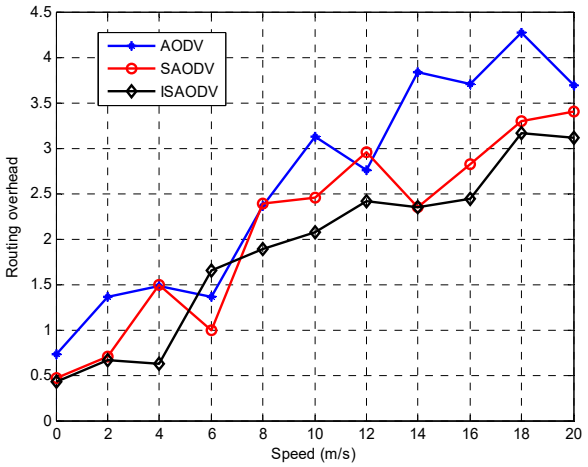

Figure 11. The routing overhead after adding malicious nodes.

5. Conclusions

The AODV routing protocol in the UAV communication network has good performance, but its security is poor and it is easy to be attacked. In this paper, the elliptic cryptosystem is introduced into AODV routing protocol to complete the authentication function, and an improved secure routing protocol is proposed based on the advantages of the existing SAODV routing protocol. Through the simulation of three routing protocols (AODV, SAODV, ISAODV), the performance indicators such as packet delivery rate, throughput, and end-to-end delay are compared and studied. The simulation results show that the ISAODV routing protocol not only inherits the efficient route discovery and maintenance capabilities of the AODV routing protocol, but also reduces the complexity of the

algorithm and has lower delay compared with the SAODV routing protocol. When there are malicious nodes in the UAV communication network, the ISAODV routing protocol can effectively improve the security of the network.

Author Contributions: Conceptualization, X.T. and S.S.; formal analysis, S.S.; investigation, Z.Z.; methodology, Z.Z. and X.G.; resources, X.G.; software, X.T. and X.S.; supervision, Z.Z. and S.S.; validation, X.T. and X.S.; writing—original draft, X.T., Z.Z., and X.G.; writing—review and editing, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Natural Science Foundation of Hunan Province, under grant number 2018JJ3607.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Song, Y.; Wang, J.; Shang, J. Estimating effective leaf area index of winter wheat using simulated observation on unmanned aerial vehicle-based point cloud data. *IEEE J. Sel. Top. Appl. Earth Observ. Remote Sens.* **2020**, *13*, 2874–2887. [CrossRef]
2. Nguyen, T.L.; Han, D.Y. Detection of road surface changes from multi-temporal unmanned aerial vehicle images using a convolutional siamese network. *Sustainability* **2020**, *12*, 2482. [CrossRef]
3. Feng, Q.; Yang, J.; Liu, Y.; Ou, C.; Li, B. Multi-temporal unmanned aerial vehicle remote sensing for vegetable mapping using an attention-based recurrent convolutional neural network. *Remote Sens.* **2020**, *12*, 1668. [CrossRef]
4. Eltner, A.; Sardemann, H.; Grundmann, J. Technical note: Flow velocity and discharge measurement in rivers using terrestrial and unmanned-aerial-vehicle imagery. *Hydrol. Earth Syst. Sci.* **2020**, *24*, 1429–1445. [CrossRef]
5. Condomines, J.P.; Zhang, R.; Larrieu, N. Network intrusion detection system for uav ad-hoc communication: From methodology design to real test validation. *Ad Hoc Netw.* **2019**, *90*, 101759. [CrossRef]
6. Chen, L.; Qian, S.; Lim, M.; Wang, S. An enhanced direct anonymous attestation scheme with mutual authentication for network-connected uav communication systems. *China Commun.* **2018**, *15*, 61–76. [CrossRef]
7. Sun, H.; Duo, B.; Wang, Z.; Lin, X.; Gao, C. Aerial cooperative jamming for cellular-enabled uav secure communication network: Joint trajectory and power control design. *Sensors* **2019**, *19*, 4440. [CrossRef]
8. Zhang, S.; Zeng, Y.; Zhang, R. Cellular-enabled uav communication: A connectivity-constrained trajectory optimization perspective. *IEEE Trans. Commun.* **2019**, *67*, 2580–2604. [CrossRef]
9. Zhang, J.; Zeng, Y.; Zhang, R. UAV-enabled radio access network: Multi-mode communication and trajectory design. *IEEE Trans. Signal Process.* **2018**, *66*, 5269–5284. [CrossRef]
10. Zhang, S.; Zhang, H.; Di, B.; Song, L. Cellular uav-to-x communications: Design and optimization for multi-uav networks. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1346–1359. [CrossRef]
11. Wang, H.; Wang, J.; Chen, J. Network-connected UAV communications: Potentials and challenges. *China Commun.* **2018**, *15*, 111–121.
12. Rahman, U.S.; Kim, G.H.; Cho, Y.Z. Positioning of uavs for throughput maximization in software-defined disaster area uav communication networks. *J. Commun. Netw.* **2018**, *20*, 452–463. [CrossRef]
13. Sun, Y.; Xu, D.; Ng, D.W.K.; Dai, L.; Schober, R. Optimal 3d-trajectory design and resource allocation for solar-powered uav communication systems. *IEEE Trans. Commun.* **2019**, *67*, 4281–4298. [CrossRef]
14. Liu, B.; Zhu, Q.; Zhu, H. Trajectory optimization and resource allocation for uav-assisted relaying communications. *Wirel. Netw.* **2020**, *26*, 739–749. [CrossRef]
15. Antonio, G.P.; Maria-Dolores, C. Flying ad hoc networks: A new domain for network communications. *Sensors* **2018**, *18*, 3571.
16. Liu, D.; Wang, J.; Xu, K.; Xu, Y.; Anpalagan, A. Task-driven relay assignment in distributed uav communication networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11003–11017. [CrossRef]
17. Lashari, H.N.; Ali, H.M. Implementation of cross layer design for efficient power and routing in uav communication networks. *Stud. Inform. Control* **2020**, *29*, 111–120.
18. Keerthika, V.; Malarvizhi, N. Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt aodv in manet. *Wirel. Pers. Commun.* **2019**, *106*, 621–632. [CrossRef]

19. Gurung, S.; Chauhan, S. A dynamic threshold based algorithm for improving security and performance of aodv under black-hole attack in manet. *Wirel. Netw.* **2019**, *25*, 1685–1695. [CrossRef]
20. Amiri, E.; Hooshmand, R. Improved aodv based on topsis and fuzzy algorithms in vehicular ad-hoc networks. *Wirel. Pers. Commun.* **2020**, *111*, 947–961. [CrossRef]
21. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and privacy issues of uav: A survey. *Mob. Netw. Appl.* **2020**, *25*, 95–101. [CrossRef]
22. Gurung, S.; Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in manet. *Wirel. Netw.* **2019**, *25*, 975–988. [CrossRef]
23. Li, B.; Fei, Z.; Zhang, Y.; Guizani, M. Secure uav communication networks over 5g. *IEEE Wirel. Commun.* **2019**, *26*, 114–120. [CrossRef]
24. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
25. Shounak, S.; Balaso, J. Monarch-EWA: Monarch-earthworm-based secure routing protocol in IoT. *Comput. J.* **2020**, *63*, 817–831.
26. Alouache, L.; Nguyen, N.; Aliouat, M.; Chelouah, R. Survey on iov routing protocols: Security and network architecture. *Int. J. Commun. Syst.* **2019**, *32*, e3849. [CrossRef]
27. Liu, Y.; Liu, X.; Liu, A.; Xiong, N.N.; Liu, F. A trust computing-based security routing scheme for cyber physical systems. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*, 1–27. [CrossRef]
28. Neumann, A.; Navarro, L.; Cerda-Alabern, L. Enabling individually entrusted routing security for open and decentralized community networks. *Ad Hoc Netw.* **2018**, *79*, 20–42. [CrossRef]
29. Kavitha, S.; Alphonse, P.J.A.; Reddy, Y.V. An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System. *J. Med. Syst.* **2019**, *43*, 260. [CrossRef]
30. Cerri, D.; Ghioni, A. Securing aodv: The a-saodv secure routing prototype. *IEEE Commun. Mag.* **2008**, *46*, 120–125. [CrossRef]
31. Hurley-Smith, D.; Wetherall, J.; Adekunle, A. Superman: Security using pre-existing routing for mobile ad hoc networks. *IEEE. Trans. Mob. Comput.* **2017**, *16*, 2927–2940. [CrossRef]
32. Vanitha, K.; Rahaman, A.M.J.Z. Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol. *Cluster Comput.* **2019**, *22*, 13453–13461. [CrossRef]
33. Chakravarthy, V.J. Comparative analysis of SRAAA, SDSR, SAODV routing protocol for video streaming in MANET. *Indonesian. J. Electric. Eng. Comput. Sci.* **2018**, *11*, 1075–1082. [CrossRef]
34. Jyh-haw, Y. A secure time-bound hierarchical key assignment scheme based on rsa public key cryptosystem. *Inf. Process. Lett.* **2008**, *105*, 117–120.
35. Do, T.; Park, S.; Lee, J.; Park, S. M-folding method–based elliptic curve cryptosystem for industrial cyber-physical system. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1–9. [CrossRef]
36. Wang, C.; Ding, K.; Li, B.; Zhao, Y.; Xu, G.; Guo, Y. An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1–13. [CrossRef]
37. Yohan, P.; Youngho, P. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. *Sensors* **2016**, *16*, 2123.
38. Shen, H.; Kumar, N.; He, D.; Shen, J.; Chilamkurti, N. A security-enhanced authentication with key agreement scheme for wireless mobile communications using elliptic curve cryptosystem. *J. Supercomput.* **2016**, *72*, 3588–3600. [CrossRef]