Received: 12 March 2020 | Revised: 31 July 2020 | Accepted: 2 August 2020

DOI: 10.1002/ett.4114

SPECIAL ISSUE ARTICLE

WILEY

A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique

Diwankshi Sharma[1] | Sachin Kumar Gupta[2] | Aabid Rashid[2] | Sumeet Gupta[2] | Mamoon Rashid[3] | Ashutosh Srivastava[4]

[1]Department of Electronics and Communication Engineering, Model Institute of Engineering and Technology, Kot Bhalwal, India

[2]School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, 182320, India

[3]School of Computer Science and Engineering, Lovely Professional University, Jalandhar, India

[4]Department of Electrical Engineering, Indian Institute of Technology (BHU), Varanasi, India

Correspondence
Sachin K. Gupta, School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Kakryal, Katra - 182320, (Jammu & Kashmir), India.
Email: sachin.gupta@smvdu.ac.in

Abstract

As the number of user equipment (UE) in any heterogeneous network (HetNet) assisted by unmanned aerial vehicles (UAV) continues to grow, so does the number of intruder nodes. The intruder/malicious nodes are able to interfere with the ongoing data transmission in the network and carry out different kinds of active and passive attacks such as spoofing, masquerading, impersonating, and so on in the network thus requiring an optimized security technique for the network. This article implements the novel functional encryption (FE) technique in the proposed UAV assisted HetNet model for the dense urban area to secure data against such intrusions. In this network model, UAV acts as a relay node for those UE which are in nonline-of-sight communication with macro based station (MBS). For securing the data transmission among UAV, UE, and MBS, FE technique is implemented in the network in two phases: the first phase between UE and MBS and the second phase between MBS and UE through UAV. During implementation, the Dolev-Yao attack model is considered in which intruders are able to intercept or modify the UE data. The main objective of the FE technique implementation is to provide security from such intrusion attacks. The proposed methodology is validated using automated validation of Internet security protocols and applications (AVISPA) tool. The results of the AVISPA tool clearly indicate that the proposed technique is safe to implement in the UAV assisted HetNet, even in the presence of intruder nodes.

1 | INTRODUCTION

Heterogeneous networks (HetNet) in the dense urban areas are widely used for accommodating the proliferating demand for user equipment (UE) based data very efficiently.[1,2] HetNets increase the capacity of the overall network by removing the coverage holes both in the indoor and the outdoor premises.[3,4] Nowadays, unmanned aerial vehicles (UAVs) are deployed widely in the network along with macro based station (MBS) to further increase the coverage and to provide various public services such as disaster management, surveillance, traffic control, remote sensing, and so on. Potential of the applications using UAVs is drawing even the top level companies such as Google, Amazon, and Facebook.[5] The collaboration of UAVs with MBS in any HetNet is desired since it can result in increasing spectral efficiency per unit area in dense

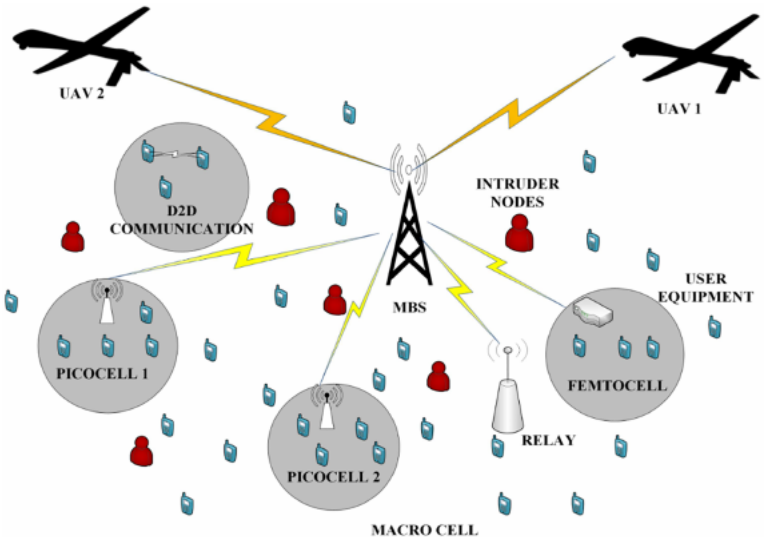

FIGURE 1 Conceptual overview of UAV integrated HetNet for an urban scenario. HetNet, heterogeneous network; UAV, unmanned aerial vehicles

urban scenarios[6] or it can maximize the coverage area of the network.[7] UAVs can be deployed for ensuring public safety communications keeping in view the energy efficiency perspective. The energy constraints of UAVs can be addressed by using wireless power transfer technology.[8,9] Figure 1 shows the conceptual overview of an urban scenario of UAV integrated HetNet, which consists of a macro cell along with MBS, picocells, femtocells, a device to device communication setup, relay node, and various number of UEs. In addition, it shows the deployment of the UAVs in the scenario with the presence of intruder nodes.

Ever advancing technologies are paving ways for more efficient data transfer in the network but this is also leading to a rise in malicious activities. The number of UE are increasing rapidly over the years and so is the number of intruder nodes in every network. Cisco White Paper has stated that the global IP traffic will reach 4.8 ZB (ZB = zetabytes) annually by 2022 as compared with 1.5 ZB per year in 2017.[10] This clearly indicates that data transfer is increasing progressively and so is the vulnerability of this data to various attacks and threats. The intruder nodes can affect the network in various ways[11] including spreading the malicious activities in the network, implement active and passive attacks such as spoofing, eavesdropping, impersonating, masquerading, coagulation attacks,[12] and so on for the UE data. These nodes can either listen to the ongoing data transmission or can interfere with the private data of the users or change the destination address of the transmitted data, and so on. Hence, the UE and the data needs to be secured against such malicious activities in order to maintain authenticity, confidentiality, and privacy in the network.[13]

In this context, several works have been done over the last few years. The authors in Reference 14 have done a thorough survey regarding the architecture, routing techniques, mobility models of FANETs. However, the authors have not covered the security aspects and the security challenges related to FANETs in this article. The authors in the article[15] have proposed a routing scheme to have an efficient connectivity in urban VANETs, however, the inclusion of cryptographic techniques to make the network robust against intrusion attacks is shown as a possible work in the future. In another research, authors of Reference 16 have proposed FANET architecture based on point-to-point deployment of UAVs. Detection, tracking, localization, and routing schemes of UAVs have been discussed but still no emphasis is given on providing security measures. Some cryptographic techniques are available which can be used for making the network robust against various attacks. One such technique is attribute-based encryption[17,18] in which each ciphertext and the corresponding private keys are associated with a particular set of attributes. The ciphertexts are decrypted only when the attributes of the private keys matches completely with the attributes of the ciphertext. Another similar technique is identity-based encryption (IBE)[19,20] in which the users communicate with each other by using their own unique identity as public key and a secret key is generated by trusted key generation center. The encryption of the message is done by using public key whereas the decryption is done by using secret keys. Diffie and Hellman key exchange scheme[21] is another such technique in which two users, who want to communicate with each other, shares a secure secret key over an insecure channel. The secret key shared is, then, used to encrypt various plain messages. These messages are, then, transmitted between them. Another similar technique is homomorphic encryption[22,23] in which computations are done on ciphertexts rather than plain messages to generate an encrypted message. When this encrypted message is decrypted, it produces the same result as if the decryption is done on the plain message. All these cryptographic techniques have one common disadvantage which makes them unsuitable for practical usage. In the above-said techniques, the decryption is an "all or nothing" process. This means that when an encrypted data needs to be decrypted, it can either be decrypted "whole" which reveals all the contents or cannot be decrypted "at all." When an encrypted data is decrypted wholly, all the contents become visible, and then anybody can read that private data. This proves to be a major disadvantage when data transmission is taking place in a network, full of intruders.

1.1 | Research objective, motivation, and contribution

The objective of this research article is to overcome the "all or nothing" disadvantage of the aforementioned cryptographic techniques. The contribution of this article lies in implementing the novel functional encryption (FE) technique in UAV assisted HetNet. The advantage of FE over other techniques is that there is no need to decrypt the entire message. Only a particular function (ie, portion) of the ciphertext will be decrypted and only that specific information will be given to the user who has requested the decryption process. Thus, it makes the rest of the data secure from intruders. The level of security that the FE technique offers to data makes it suitable for its implementation in the presence of intruder nodes in UAV integrated HetNets.

The HetNet assisted by UAVs, is prone to several intrusion attacks. If intruder nodes are able to intercept the vital information transmitted between two UEs, they can easily modify the whole data and can even impersonate either sender or receiver. Hence, the main objective is to propose a technique to secure the overall data transmission in the network using the FE technique and to overcome the "all or nothing" disadvantage of other techniques. The FE technique will ensure that the transmission and reception of the data occurs, without falling prey to the intruder nodes. Ensuring the security of the whole network is the main objective that has motivated this research work. Moreover, the survey of literature indicates that the FE technique has not been practically implemented to maintain the security of UAV integrated HetNet as yet. Hence, this work is the first practical implementation of this kind of network. The main contributions can be summarized as follows:

- To ensure the security of the network from the intruder nodes.
- To practically implement the FE technique in UAV integrated HetNet.
- To explore and utilize the advantages of FE.

Table 1 list the various notations and glossary that are used throughout this article.

1.2 | Scope of the study

This article focuses on the implementation of the FE technique in HetNet assisted by UAV for securing the data against the intruder attacks. However, the article does not discuss the details about the routing techniques, energy constraints, advantages, and disadvantages of UAV applications. Furthermore, the various aspects of the key management and their secure distribution in the dense urban scenarios have also not been discussed in this article.

1.3 | Organization of article

The rest of the article is organized as: Section 2 explains the existing literature survey which has been carried out in the related work and indicates the research gap. Section 3 provides an insight into the system model while Section 4 presents the preliminaries of FE technique. Section 5 discusses the problem statement and two-phase proposed approach for implementing the mechanism, the first phase is the FE between UE and MBS, the second phase is the FE between MBS and UE through UAV. Section 6 provides us with a brief description regarding the automated validation of Internet security protocols and applications (AVISPA) tool and the validation of the two-phase proposed mechanism has been performed in Section 7. Section 8 provides the simulation results, discussion, and future scope. Section 9 comes up with a conclusion.

TABLE 1 List of notations and glossary

Notations and glossary	Description	Notations and glossary	Description	Notations and glossary	Description
Pp	Public key pair	Fn	List of functions	IP	Internet protocol
Msk, mk	Master key	SND	Send operation	DoS	Denial of service
Λ	Security parameter	RCV	Receive operation	GPS	Global positioning system
K	Keyspace	S-SGW	Simplified sliding group watermark	CPS	Cyber-physical system
S, sk, sk_f	Secret key	MAC	Message authentication code	LODMAC	Location oriented directional MAC protocol
N	Encryption keys	PDR	Packet delivery ratio	PSC	Public safety communication
X, x	Plaintext message	USRP	Universal software radio peripheral	Fe-ICIC	Further-enhanced intercell interference coordination
Ci, c	Ciphertext	SSID	Service set identifier	CRE	Cell range expansion
F	Function	IDS	Intrusion detection system	CIDN	Collaborative intrusion detection networks
Na	Nonce	DTN	Disruption tolerant networks	UAV	Unmanned aerial vehicle
MBS	Microbase station	UE	User equipment	FE	Functional encryption
HLPSL	High-level protocol specification language	AVISPA	Automated validation of Internet security protocols and applications	OFMC	On-the-fly model-checker
CL-AtSe	Constraint logic-based attack searcher	TA4SP	Tree automata based on automatic approximations for the analysis of security protocols	SATMC	SAT-based model checker

2 | RELATED WORK

While establishing any network, security is one of the prime factors. In this section, a detailed study of related work has been presented. Several authors have worked on ensuring the security to UE but FE remains underexplored. In the current state-of-the-art, authors of article[24] use the ciphertext policy attribute-based cryptography along with the FE concept. However, they have used the partial concept of FE technique in IoT e-healthcare system. In Reference 25, the authors have proposed the identity-based authentication scheme to secure the UAV assisted HetNet; however, the decryption process and communication overheads are the major drawbacks of this scheme. The authors in Reference 12 have devised a method to prevent the coagulation attacks in UAV network by improving the encoding scheme at the physical layer. However, in the present scheme, latency has reached beyond the threshold level that makes the network unsustainable.

The research work done by authors of Reference 26 addresses the critical vulnerabilities and threats of Internet of drones system. They have suggested various cryptographic techniques and mechanisms against denial of service attacks, spoofing, integrity threats, and privacy. Nevertheless, there has been no simulation validation to support this proposed approach. In another reported work by the authors of Reference 27, the tethered network architecture has been proposed in balloon ad hoc network to support the emergency services efficiently and provide a large coverage area but no security mechanism has been proposed against the intruders. The authors of Reference 28 have proposed a scheme of hiding nodes' identity from each other as the solution to spoofing and wormhole attacks in FANETs. The major limitation of this scheme is the absence of any simulation validation.

In article,[29] authors propose the nonchaotic image encryption method using cyclic group and permutation techniques as the solution of illegal copying of multimedia data in digital multimedia communication. However, they did not study the various vulnerabilities for their proposed scheme. The authors in Reference 30 have proposed the idea of monitoring the amateur drones (ADr) by using various monitoring drones (MDr). Here, architecture and deployment scenarios of MDr have been discussed thoroughly along with the routing techniques, jamming and hunting technologies for ADr. However, no implementation of the security mechanism in the architecture or deployment of MDr has been done. Similarly, in other research work,[31] the authors focus on the detection system for ADr using several techniques such as machine learning, Mel frequency cepstral coefficients, and linear predictive cepstral coefficients along with support vector machines. These techniques can be used to effectively detect the sound of ADr among various other sounds and can help the several important agencies to detect the ADr beforehand. But the major limitation of this article is that no security implementation has been done for the important data of agencies. The authors in Reference 32 have only studied the theoretical claims about implementing the FE technique without verifying it. The authors of Reference 33 have proposed an intrusion detection system for anomaly estimation in networks based on UAVs. The proposed methodology has been validated using distributed denial of service attacks. However, the limitation of the article is that the behavior of proposed methodology varies with change in the time scale and sampling method.

Along with the above-reported works in the literature, Table 2 illustrates the comparative study of the existing schemes in the state-of-the-art. Table 2 has been categorized into three different subparts. Part 1 discusses those works in which the FE security scheme has been implemented while part 2 provides a thorough comparison of those security mechanisms which have been implemented on UAV integrated HetNet. Furthermore, part 3 gives the detailed comparison of various other security-related existing works in the domain.

Thus, the proposed FE technique on the UAV integrated HetNet existing scheme, differs from each and every technique mentioned above. We implement the whole concept of the FE technique on the UAV integrated HetNet, which provides security against the various attacks occurring in the network. For verifying the theoretical analysis, the technique has been simulated using the AVISPA tool and detailed implementation and results of the simulation have been discussed further in the article.

3 | SYSTEM MODEL

For implementing the FE technique, we have taken the very basic model of UAV integrated HetNet, where UAVs may be deployed as relay nodes in the network and they form the wireless transmission links between UE and MBS. The UEs, those are direct out of range of MBS will able to communicate to it through UAV. The links are setup in two stages: first between MBS and UAV, the second between UAV and UE. Whenever data is being transferred between UE and MBS through UAV, it is done in the above said two stages. These links are further used for implementing the security scheme in the network in a phased manner. In addition, several UE may be grouped together in clusters and these clusters can then be governed by UAVs accordingly.

Before diving further into the methodology, it is necessary to have the conceptual overview of some details regarding the system which has been thoroughly discussed in Table 3. This table helps to have an insight into the system model.

4 | FUNCTIONAL ENCRYPTION

The concept of FE was introduced by Boneh et al.[51] FE can be defined as a technique which supports the restricted secret keys and enables only a user who holds the key to learn about a specific function of the encrypted data. Vaguely, an authority is present which has the master key with itself. This master key is used for generating various secret keys which, later on, are used for the computation of the function on the encrypted data.[51] Boneh et al gave the definition of FE as A FE scheme for a functionality F defined over (K; X) is a tuple of four PPT algorithms (setup; keygen; enc; dec) satisfying the following correctness condition for all k ε K and x ε X:

- (pp; mk) ← setup(1^{λ}) (generate a public and master secret key pair)
- sk ← keygen(mk; k) (generate secret key for k)

TABLE 2 Comparative study of the existing scheme in the state-of-the-art

Part 1: FE security scheme-based reported work					
Reference	**Application area**	**Attacks**	**Security scheme**	**Simulation platform**	**Remarks**
24	IoT e-healthcare system	Threats on data security and privacy.	Ciphertext policy attribute-based cryptography and functional encryption	CPABE toolkit and pairing-based cryptography library.	• Provides relevant information according to the patient's need. • Limitation: need of double encryption.

Part 2: Comparison of the existing security mechanism in UAV and HetNets based network		
Reference	**Security mechanisms**	**Characteristics**
19	• Identity-based authentication.	• Authentication among entities by involving PKI only once. • AVISPA tool. • Limitation: communication overheads. • UAV-assisted heterogeneous cellular system.
25	• UAV-assisted base station (UABS)	• Handles traffic volume by using UABS. • Uses UAV-based floating relays for dynamic and adaptive coverage.
34	• 3GPP Release-11 FeICIC and CRE techniques. • Genetic algorithm and hexagonal grid model using 5pSE.	• UABS and PSC. • MATLAB. • Limitation of using CRE: increases interference in the downlink.

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
8	Y	UAV network	Nil	Nil	Multilayered architecture	Nil	• Worked on the energy efficiency of UAVs. • Proposed a multilayer architecture for public safety communication.
12	Y	High mobility UAVs ad hoc network	Coagulation attack	Improved encoding scheme at PHY layer.	Flying UAV ad hoc.	MATLAB	• Introduces new attack known as coagulation attack. • PDR decreases abruptly and reaches below threshold, result in an unsustainable network. • Also increases network latency beyond the threshold.
26	Y	Unmanned aircraft system (UAS), cyber-physical systems (CPS)	Integrity and privacy of CPS	Behavior rule specification-based IDS	Sensors and actuators integrated UAS	Monte-Carlo simulation test.	• Lightweight specification-based behavior rules. • Bounded probability of false alarm <5% for reckless and <20% for random attackers. • Support ultra-safe and secure UAS applications. • Effectively trades between false positive and detection rates.
27	N	Tethered balloon ad hoc network	Natural disaster, terrorist attacks	Nil	Tethered network architecture	OPNET modeler 14.5	• Provides large coverage area. • Supports emergency services efficiently. • Better QoS services. • Surveyed security problems and open challenges of FANETs.
28	Y	FANET	Eavesdropping, spoofing, wormhole, easily stolen, session hijacking	Hiding nodes' identities from each other.	Multi-UAV ad hoc architecture	Nil	• Highlighted the characteristics of FANETs to resolve the existing ad hoc network's security issues.

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
29	N	Digital multimedia communication network	Statistical and differential attacks, illegal copying of multimedia data	Nonchaotic image encryption method using cyclic group and permutation techniques	Digital multimedia supportable network architecture	Nil.	• Proposed scheme has two phases-confusion and diffusion. • Nonchaotic digital image secure scheme is efficient and robust against various attacks. • Vulnerability of the proposed scheme has not been studied.
30	Y	Drones system	Nil	Nil	Nil	MATLAB	• Technique based on ML for detection and classification of ADr sounds has been developed. • Results verified that proposed scheme has 17% accuracy.
31	Y	VANETs	Nil	Nil	Urban VANETs	NS-2	• Efficient routing solution has been developed based on flooding techniques.
35	Y	UAV ad hoc	Selective forwarding, data forgery, data replay, tampering	Double-authentication watermarking	Distributed architecture based on clustering stratification	OMNET++	• Maintaining low energy consumption and low latency as compared with S-SGW, MAC, redundancy scheme, and regular network model. • Filter the suspicious data during transmission process.
36	Y	UAV ad hoc network	GPS spoofing, Wi-Fi attack	Jamming-2-noise sensing defense, multiantenna defense, enabling WPA2, disabling SSID	UAV communication architecture	Ettus USRP, GNU radio	• Focused to develop a low-cost GPS record-modify-and-replay system to ensure a good balance between securities strengthen and UAV ad hoc network performance.
37	Y	CPS	Data integrity, confidentiality	• Identity-based encryption. • Selective data encryption.	Hierarchical architecture UAV network	OMNET++	• Provides network flexibility. • Reduce network overheads. • Data hiding mechanism: increases confidentiality

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
38	Y	UAV network	Cyber attacks	Cyber detection mechanism and cyber belief approach based on threat estimation model	Targeted UAV network architecture	NS-3	• Proposed a cyber detection system based on IDS. • Reduces false positive and negative rates. • Exhibits a high accuracy than cyber detection system.
5	Y	Networked UAVs	Malicious, routing, UAV capturing, path alteration	IDS approaches	UAV communication environment	Nil	• Explore UAV-IDS approaches. • Pointed out the taxonomies of UAV-IDS systems. • Discusses open challenges to build cyber-physical UAV-IDS system.
39	Y	Internet of drones (IoD)	DoS, GPS spoofing, IoD freezing privacy, integrity, confidentiality availability	IDS mechanism, cryptographic techniques.	IoD-assisted battlefield HetNet ground station	Nil	• Addresses IoD's critical vulnerabilities and threats. • Explores the challenges and research direction in secure-IoD. • Cryptographic mechanisms help to achieve message security and control signal protections.
40	Y	Commercial UAVs	Cyber-attacks, DoS, Hijacking: network channel or physical hardware.	Second channel security system design, self-destroy functions	Multi-UAV and ground station	Raspberry Pi, Aircrack-ng	• Presented encrypted and secure communication protocol suitable for multi-UAV and ground station. • Shorten time delay between GS and Raspberry Pi. • Future is MOSFET based UAV lithium battery to secure channel

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
41	Y	5G	Nil	Nil	5G and beyond 5G integrated UAV	Nil	• An extensive review of UAV-assisted various 5G techniques. • Discusses open research issues and its possible future directions.
42	Y	Professional UAV	Man-in-middle and control packet injection attacks	XBee 868LP on-board encryption, dedicated hardware, and application layer encryption.	UAV's secure communication hardware architecture	Hardware design, Wi-Fi, and XBee 868LP chips	• Presents security gaps of professional UAVs. • Performs man-in-middle and control packet injection attacks and gives their countermeasures by presenting hardware design.
43	N	Smartphones	Insider or stranger attacks	Continuous/active authentication system	Smartphones architecture	Nil	• Provides a detailed study of the working of active authentication systems. • Presents limitations, demerit, and merit of behavioral biometric.
44	N	Intrusion detection system/networks	Advanced insider attacks such as, passive message fingerprint attack	Challenge-based trust mechanism	Challenged-based CIDN architecture	CIDN environment	• Improves the sending strategy in simulated CIDN. • Strategy can be failed, if the malicious nodes have information about nearby traffic.
45	N	Insecure public networks	Adversary and known attacks, user anonymity	Enhanced smart-card-based authenticated key agreement scheme	Insecure communication channel between remote users	AVISPA	• Overcome the flaws of Jiang et al's scheme. • Scheme is robust against active and passive attacks and supports the smartcard revocation phase. • Shows better results in terms of overheads: communication and computational.

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
46	N	Organizational networks	Insider attacks	Situational crime and social bond theory	Internet-based information technology systems	Structural equation modeling.	• Main finding shows negative attitudes of employee's towards organization. • Results show that information security involvement efficiently decreases insider attacks. • Points out environmental factors that motivate employees to engage in misbehaving activities.
47	N	Internet of things	Potential threats, message, and identity broker	Authentication, authorization, and access control, SSL/TLS, AES 256, SHA-256	Industrial and consumer-based IoT	IoT frameworks	• Reported the various commercially available framework and platform to develop industrial and consumer-based IoT applications. • Survey various IoT platforms in terms of security that includes: AWS IoT from Amazon, ARM Bed from ARM and other partners, Azure IoT Suite from Microsoft, Brillo/Weave from Google, Calvin from Ericsson, Home Kit from Apple, Kura from Eclipse, Smart Things from Samsung.

(Continues)

TABLE 2 (Continued)

Part 3: Detailed comparison of various other security-related existing works in the domain							
Reference	**UAV used**	**Network type**	**Attacks**	**Security approach**	**Architecture**	**Simulation platform**	**Major contributions**
48	Y	PS-LTE	Nil	Nil	IP based EPS	MATLAB	• For PS-LTE, a disaster resilient three-layered architecture has been proposed. • Combines various advantages of SDNs and edge-computing. • Delay is reduced by 20%.
49	Y	UAV-assisted VANET	Nil	Nil	VANET	NS-3	• Enhanced connectivity among vehicles. • Energy consumption of the network has been reduced. • No emphasis has been given to security in the network, which can make the data vulnerable to several attacks.
50	Y	UAV network	Lethal security threats	Agent-based self-protective system based on human immune system	UAV network	NS-3	• Increase in packet delivery ratio and detection rate by 17%, respectively. • However, no authentication mechanism is present which can validate UAVs for security purpose.

Abbreviations: AVISPA, automated validation of Internet security protocols and applications; FE, functional encryption; HetNet, heterogeneous network; ML, machine learning; UAV, unmanned aerial vehicles.

TABLE 3 System model

Parameters	Scheme	Description
Cryptographic scheme	Functional encryption (FE)	Unlike other techniques, FE scheme allows the user to have flexibility in the decryption process. Since, by using FE, there is no need to decrypt the whole message.
Services provided by UAVs	UAVs act as relay nodes	The UAVs deployed in the network will act as relay nodes for those UE which are in nonline of sight communication with the MBS.
Band for UAV to communicate with UE and MBS	S-band and C-band	For the communication aspects, the UAVs will use part of the S-band for control links and the C-band for payload for communicating with UE and MBS.
Adopted mobility model for UAVs	Random waypoint mobility model	Since we have taken a basic model, therefore, the random waypoint mobility model has been chosen to owe to its simplicity and efficiency.
UAV altitude	Low altitude platform	The altitude at which the UAVs will be deployed is in the range of 100 to 250 m above the earth level.
Modulation technique	OFDM	The communication between the MBS, UE, and UAV will have the OFDM modulation technique implemented.
Communication link characteristics	802.11 g/n	The communication link that will be established between UE, UAV, and MBS will have IEEE 802.11 g/n standard having the maximum data rate of up to 600 Mbits/sec and the frequency bands of 2.4 GHz (mandatory) and 5 GHz (optional).
Maximum power requirement	23 dBm (approx.)	The maximum power that can be required by the UAVs to operate in the scenario is approximately 23 dBm or 200 mW.

Abbreviations: MBS, macro based station; UAV, unmanned aerial vehicles; UE, user equipment.

- c ← enc(pp; x) (encrypt message x)
- y ← dec(sk; c) (use sk to compute F[k; x] from c)

Then, we require that y = F(k; x) with probability 1″.

Briefly, in a FE system, authority is present which has the master key (*mk*) known only to itself. When the details of any function *f* are provided to the authority, it generates secret keys (*sk*) from the master key associated to *f*. Now, anyone provided with this *sk* can easily compute *f* and can decrypt that function to view the corresponding plaintext. Moreover, in traditional encryption techniques such as Diffie and Hellman,[21] the decryption process is all or nothing, that is, if the decryption process will occur, the whole of the encrypted message will be decrypted simultaneously, or nothing will be decrypted at all. This concept was overcome in FE technique where the decryption process reveals only partial information about the plaintext and nothing more. [52] The pictorial representation of FE is shown in Figure 2.

Till now, all the FE process has been done considering only a single plaintext for its implementation. However, Goldwasser et al[53] considered more than one plaintext for the FE technique implementation. This was defined as multi-input

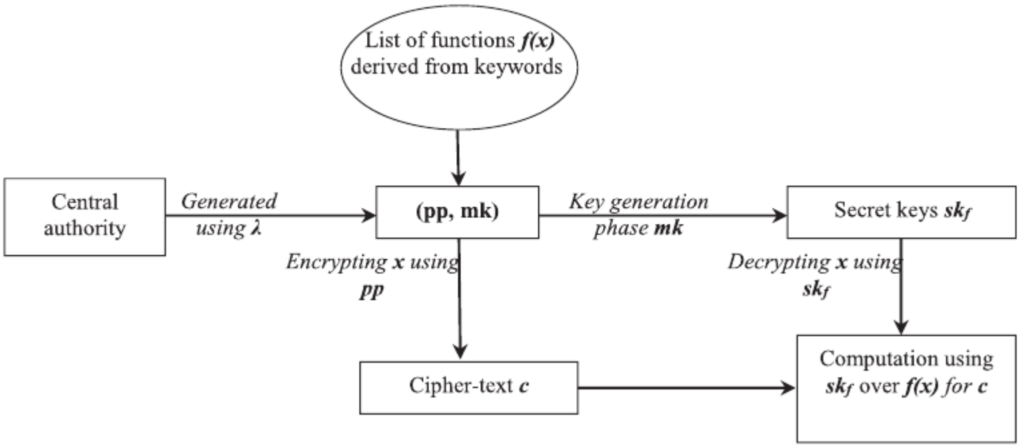

FIGURE 2 Pictorial representation of FE technique. FE, functional encryption

FE in which multiple plaintexts were used corresponding to their ciphertexts or computation of functions defined over plaintexts, given their ciphertexts, each encrypted under different key was given.

5 | PROBLEM STATEMENT AND PROPOSED METHODOLOGY

This section provides an overview of the problem statement based on the limitations of the state-of-the-art works done. Then, a thorough explanation regarding the proposed methodology is given, in which FE technique is implemented in UAV assisted HetNet. The proposed methodology is validated in Section 7 using the AVISPA tool and the results are discussed in Section 8.

5.1 | Problem statement

On doing a detailed study of literature works in Sections 1 and 2 of the article, it can be observed that many techniques are present which can make the network robust against intruder attacks. In Reference 17, attribute-based encryption is used in which the keys are associated with the attributes of the person. In Reference 21, the secret keys are first generated, after which they are exchanged over the insecure channel. But the problem still arises during the decryption process. If an intruder node is able to intercept the secret keys in these techniques, then, that node can easily decrypt the whole ciphertext. One secret key can reveal the whole information of the plaintext message. These intruder nodes, then, can steal or interfere with the private data of users. This limitation poses a grave threat to the data of UE. To overcome this limitation, FE technique is implemented in the network. The detailed implementation of the proposed methodology is discussed in further subsection.

5.2 | Proposed methodology

In this article, the concept of FE technique has been implemented on UAV integrated HetNet in the presence of intruder nodes for dense urban scenarios to provide secure data transmission in the entire network. The advantage of FE technique over other cryptographic techniques is that there is no need to decrypt the whole message. Only a particular function will be decrypted using secret keys, and information corresponding to its plaintext will be generated. Thus, if the intruder, somehow, is able to intercept the encrypted message, he will not be able to decrypt the whole information. This technique is implemented in two phases in the entire proposed network architecture:

- The first phase between UE and MBS.
- Second phase between MBS and UE through UAV.

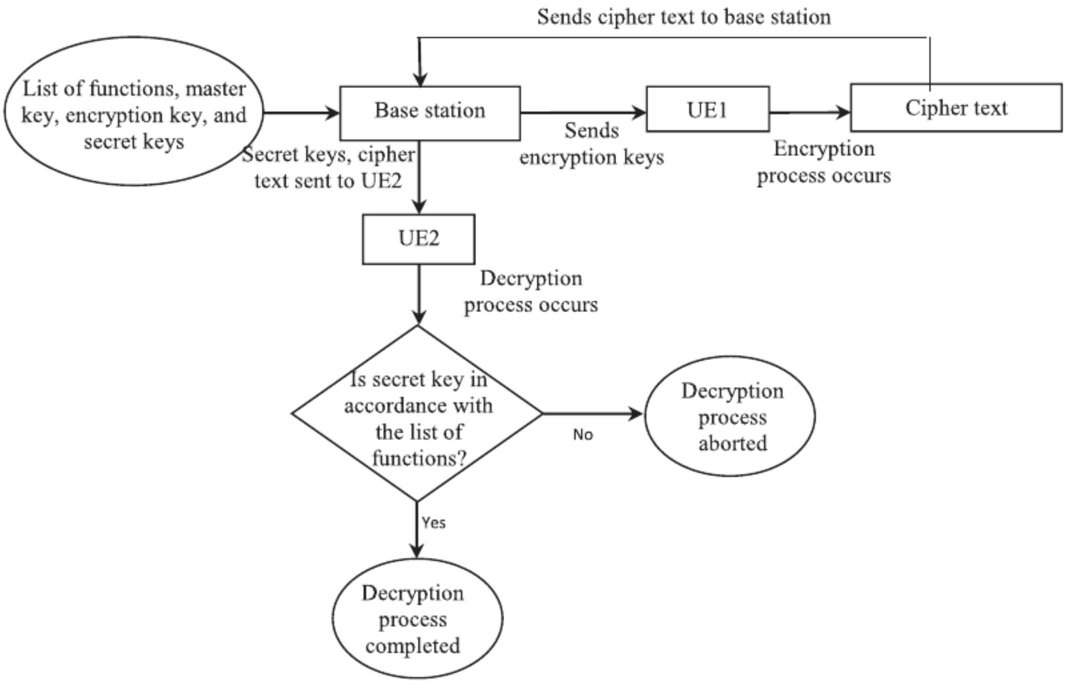

FIGURE 3 Flowchart of FE technique. FE, functional encryption

The overall implementation process of the FE technique in the network has been depicted in the form of a flowchart in Figure 3. Here, the list of functions is provided by the users and master key, encryption keys, and secret keys are generated at the base station and then the encryption keys are sent for ciphering the plaintext. In the decryption phase, secret keys are transmitted which will decrypt only the corresponding data.

Moreover, for implementing the proposed methodology, the following considerations are taken into account:

- Intruders can have full control and access over the whole network.
- Intruders can intercept, analyze, or even modify the messages.
- MBS is the central server that has the full list of functions and it does all the computations.

5.2.1 | FE between UE and MBS

The proposed methodology of FE between UE and MBS has been discussed in this section, supported by Equations (1) to (14). These equations are the prototype for the high-level protocol specification language (HLPSL) codes, which will be validated using the AVISPA tool in the Section 6.

The data transmission is initiated in the network when MBS generates a nonce signal (*Na)*. This nonce signal is transmitted to the UE present in the network. The objective of using nonce signal (*Na)* is to authenticate the UE and to avoid replay attacks, man-in-the-middle attacks in the network. Mathematically, it is written in the form of Equation (1).

$$\text{MBS} \rightarrow \text{UE} : \text{SND}\ (Na). \tag{1}$$

When the nonce signal *Na* is received by the UE, it generates a response corresponding to that nonce signal, as written in Equation (2). The response corresponding to the particular nonce signal is, then, sent back to the MBS along with a list of functions (*Fn*). This list of functions (*Fn*) has been derived from some specific keywords, represented in Equation (3).

$$\text{UE} : \text{RCV}\ (Na), \tag{2}$$

$$\text{UE} \rightarrow \text{MBS} : \text{SND}\ (Na, Fn). \tag{3}$$

When the reply from UE, corresponding to the nonce signal *Na*, is received by the MBS, the MBS, then, completes the authentication process of UE over the *Na* signal. It is mathematically written in Equation (4).

$$\text{MBS} : \text{RCV}\,(Na, Fn). \tag{4}$$

After the UE device is authenticated by the MBS, then, the setup phase begins. In the setup phase, the list of functions (*Fn*), which is received from UE in previous step, is taken as input. Corresponding to *Fn*, a master key *(Msk)* is generated by the MBS along with the encryption keys (*N*), as output of the step. Mathematically, the whole process is written in Equations (5) and (6).

$$\text{MBS} : \text{Input} = \{Fn\}, \tag{5}$$

$$\text{Output} = \{Msk\}, \{N\}. \tag{6}$$

After the setup phase is completed at the MBS, then, the key generation phase is initiated. In key generation phase, the master key *(Msk)*, generated in previous step, is now treated as input. This master key *(Msk)* produces the various secret keys (*Skf*), which are based on the specific functions from *Fn* list. Equations (7) and (8) provide the mathematical representation.

$$\text{MBS} : \text{Input} = \{Msk\}, \tag{7}$$

$$\text{Output} = \{Skf\}. \tag{8}$$

During the key generation phase, the encryption keys (*N*) generated, are converted to *N1* using the hashing technique. After the key generation phase is over, the hashed encryption keys (*N1)* are sent to the UE. The hashing is required so that intruders are not able to intercept the encryption keys. Mathematically, the whole step is represented in Equations (9) and (10).

$$N1 = \text{H}\,(N), \tag{9}$$

$$\text{MBS} \rightarrow \text{UE} : \text{SND}\,(N1). \tag{10}$$

The hashed encryption keys (*N1*) are received by the UE. After receiving the keys, encryption phase begins at UE. In the encryption phase, the plaintext (*X*) of the UE is encrypted using the *N*th encryption key. It is written mathematically in the form of Equations (11) and (12).

$$\text{UE} : \text{RCV}\,(N1), \tag{11}$$

$$\text{UE} : Ci = \{X\}N1. \tag{12}$$

After the plaintext (*X*) of the UE is encrypted, it produces a ciphertext (*Ci*). This ciphertext (*Ci*) is, now, to be transmitted over the network and it is received by MBS. The transmission of (*Ci*) takes place through the insecure channel, which is full of intruder nodes. The whole step is written mathematically and presented in Equations (13) and (14).

$$\text{UE} \rightarrow \text{MBS} : \text{SND}\,(Ci), \tag{13}$$

$$\text{MBS} : \text{RCV}\,(Ci). \tag{14}$$

After receiving the ciphertext (*Ci*) from the UE, its decryption is possible only through *Skf*. The decryption of ciphertext (*Ci*) will generate only a particular function of *Ci* and gets the information of plaintext corresponding to that function only. Thus, this proposed methodology secures the transmitted data from the intruders because for getting the information about plaintext, *Skf* must be known and intruders will not be able to intercept the secret keys. Thus, the transmitted data remains secured.

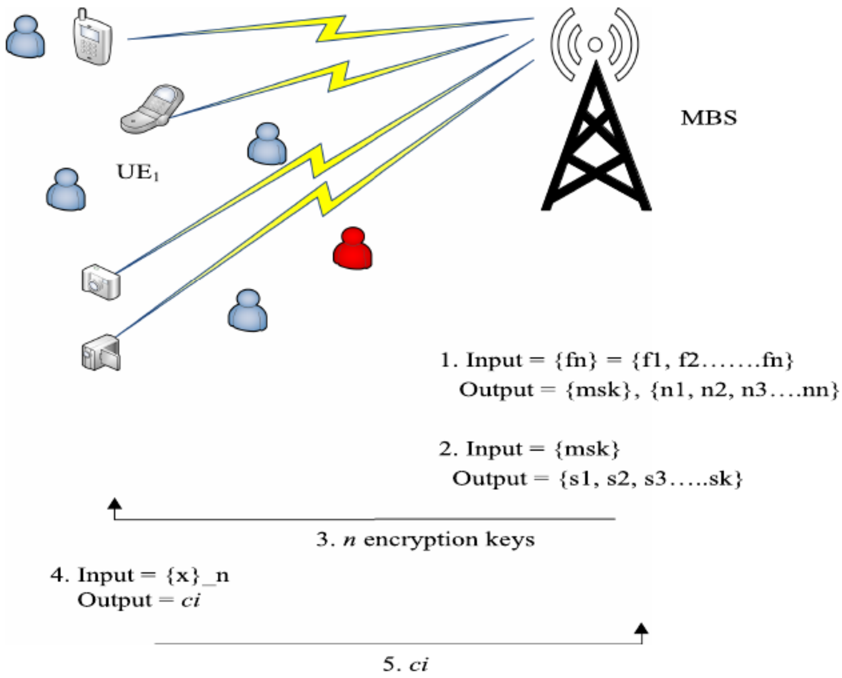

FIGURE 4 Pictorial representation of FE between MBS and UE. FE, functional encryption; MBS, macro based station; UE, user equipment

Figure 4 shows the implementation of FE technique between MBS and UE.

5.2.2 | FE between MBS and UE through UAV

The proposed methodology of FE between MBS and UE through UAV has been discussed in this section, supported by Equations (15) to (36). These equations are the prototype for the HLPSL codes, which will be validated using the AVISPA tool in Section 6.

The data transmission is initiated in the network when MBS generates a nonce signal (*Na)*. This nonce signal is transmitted to UE and UAV present in the network. The objective of using nonce signal (*Na)* is to authenticate both UAV and UE and to avoid replay attacks in the network. Mathematically, it is written in the form of Equations (15) and (16).

$$\text{MBS} \rightarrow \text{UE} : \text{SND}\ (Na), \tag{15}$$

$$\text{MBS} \rightarrow \text{UAV} : \text{SND}\ (Na), \tag{16}$$

When the nonce signal *Na* is received by the UE, it generates a response corresponding to that nonce signal, as written in Equation (17). The response corresponding to the particular nonce signal is, then, sent back to the MBS along with a list of functions (*Fn*). This list of functions (*Fn*) has been derived from some specific keywords, represented in Equation (18).

$$\text{UE} : \text{RCV}\ (Na), \tag{17}$$

$$\text{UE} \rightarrow \text{MBS} : \text{SND}\ (Na, Fn), \tag{18}$$

The UAV in the network, also receives the nonce signal (*Na*). It generates its response, corresponding to that nonce signal and sends it back to MBS, as shown mathematically in Equations (19) and (20).

$$\text{UAV} : \text{RCV}\ (Na), \tag{19}$$

$$\text{UAV} \rightarrow \text{MBS} : \text{SND}\ (Na). \tag{20}$$

After receiving the reply from UE and UAV, the MBS, then, completes the authentication process of both over the *Na* signal. It is mathematically written in Equations (21) and (22).

$$\mathrm{MBS} : \mathrm{RCV}\ (Na, Fn), \tag{21}$$

$$\mathrm{MBS} : \mathrm{RCV}\ (Na). \tag{22}$$

After the UE and UAV is authenticated by the MBS, then, the setup phase begins. In the setup phase, the list of functions (*Fn*), which is received from UE in previous step, is taken as input. Corresponding to *Fn*, a master key *(Msk)* is generated by the MBS along with the encryption keys (*N*), as output of the step. Mathematically, the whole process is written in Equations (23) and (24).

$$\mathrm{MBS} : \mathrm{Input} = \{Fn\}, \tag{23}$$

$$\mathrm{Output} = \{Msk\}, \{N\}. \tag{24}$$

After the setup phase is completed at the MBS, then, the key generation phase is initiated. In key generation phase, the master key *(Msk)*, generated in previous step, is now treated as input. This master key *(Msk)* produces the various secret keys (*Skf*), which are based on the specific functions from *Fn* list. Equations (25) and (26) provide the mathematical representation.

$$\mathrm{MBS} : \mathrm{Input} = \{Msk\}, \tag{25}$$

$$\mathrm{Output} = \{Skf\}. \tag{26}$$

During the key generation phase, the encryption keys (*N*) generated, are converted to *N1* using the hashing technique. After the key generation phase is over, the hashed encryption keys (*N1)* are sent to the UAV. The hashing is required so that intruders are not able to intercept the encryption keys. Mathematically, the whole step is represented in Equations (27) and (28).

$$N1 = H\ (N), \tag{27}$$

$$\mathrm{MBS} \rightarrow \mathrm{UAV} : \mathrm{SND}\ (N1). \tag{28}$$

After receiving the hashed encryption keys (*N1),* the UAV acts as a relay node and forwards the hashed encryption keys (*N1)* to UE. Mathematically, it is represented in Equations (29) and (30).

$$\mathrm{UAV} : \mathrm{RCV}\ (N1), \tag{29}$$

$$\mathrm{UAV} \rightarrow \mathrm{UE} : \mathrm{SND}\ (N1). \tag{30}$$

The hashed encryption keys (*N1*) are received by the UE. After receiving the keys, encryption phase begins at UE. In the encryption phase, the plaintext (*X*) of the UE is encrypted using the *N*th encryption key. It is written mathematically in the form of Equations (31) and (32).

$$\mathrm{UE} : \mathrm{RCV}\ (N1), \tag{31}$$

$$\mathrm{UE} : Ci = \{X\}N1. \tag{32}$$

After the plaintext (*X*) of the UE is encrypted, it produces a ciphertext (*Ci*). This ciphertext (*Ci*) is, now, to be transmitted over the network. The ciphertext (*Ci*) generated, is first transmitted to UAV by UE. The UAV receives the ciphertext

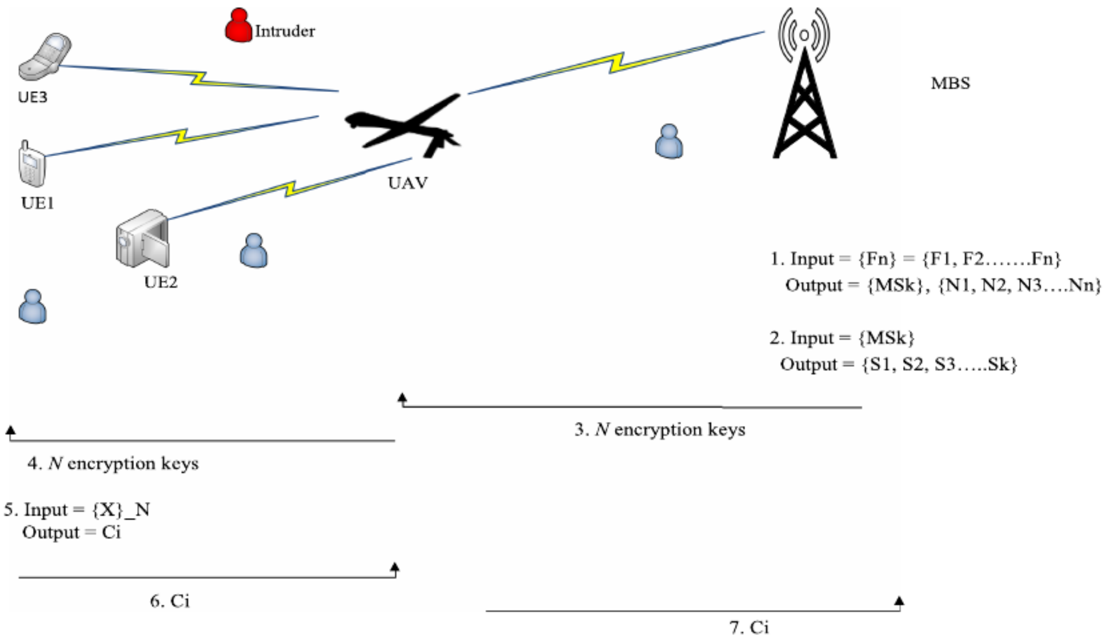

FIGURE 5 Pictorial representation of FE between MBS and UE through UAV. FE, functional encryption; MBS, macro based station; UAV, unmanned aerial vehicles; UE, user equipment

and it is shown mathematically in Equations (33) and (34).

$$\text{UE} \rightarrow \text{UAV} : \text{SND}\ (Ci), \tag{33}$$

$$\text{UAV} : \text{RCV}\ (Ci). \tag{34}$$

The UAV, after receiving the ciphertext (Ci), then, acts as relay node and forwards it to the MBS. It is written mathematically in the form of Equations (35) and (36). The whole transmission of ciphertext takes place through insecure channel, which is full of intruder nodes.

$$\text{UAV} \rightarrow \text{MBS} : \text{SND}\ (Ci), \tag{35}$$

$$\text{MBS} : \text{RCV}\ (Ci). \tag{36}$$

After receiving the ciphertext (Ci) from UE through UAV, its decryption is possible only through Skf. The decryption of ciphertext (Ci) will generate only a particular function of Ci and gets the information of plaintext corresponding to that function only. Thus, this proposed methodology secures the transmitted data from the intruders because for getting the information about plaintext, Skf must be known and intruders will not be able to intercept the secret keys. Thus, the transmitted data remains secured.

Figure 5 represents the implementation of FE technique between MBS and UE through UAV.

6 | AVISPA TOOL

Over the past many years, the number of Internet users has been increasing dramatically. Having such a huge number of users, there is a direct need to provide security to various network-based services. For providing security, protocols need to be defined and developed without any error. However, developing these protocols is a difficult task as they are error-prone. Hence, appropriate tools need to be used while developing the protocols so that they can detect the vulnerabilities in the early stage of development. One such tool which has seen the widest use is AVISPA.[54]

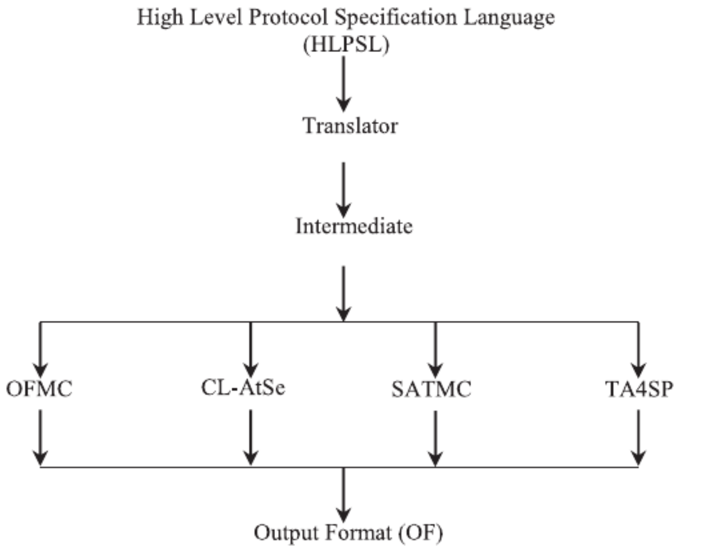

FIGURE 6 AVISPA tool's architecture. AVISPA, automated validation of Internet security protocols and applications

AVISPA is a push-button tool in which Internet security-sensitive protocols are validated automatically. It provides a role-oriented, expressive, and formal language for validation. Every member/participant plays an independent role during the protocol execution.[55,56] The architecture of the AVISPA tool has been defined and shown in Figure 6:

The basic step in the AVISPA tool is to cite the analyzed protocol in HLPSL by writing a file with the extension *.hlpsl*. This language is role-based in which basic roles illustrates participant roles whereas composition roles depict scenarios of basic roles.[57] The HLPSL specifications written are first converted into a lower language which is known as intermediate format (IF). This is done using a translator known as HLPSL2IF translator. Transparency is maintained for the users during the IF translation steps and is read directly by the back-ends to the AVISPA tool. There are four different back-ends: OFMC, CL-AtSe, SATMC, TA4SP.[58]

- **OFMC (On-the-fly model-checker):** responsible for symbolic techniques by exploring state space in a demand-driven way.
- **CL-AtSe (Constraint logic-based attack searcher):** used for translating the security protocol specification written as transition relation in IF to a set of constraints for finding attacks on protocols.
- **SATMC (SAT-based model checker):** generates a propositional formulae, fed it to SAT solver and if any model is found, it is translated back into an attack.
- **TA4SP (Tree automata based on automatic approximations for the analysis of security protocols):** approximates intruder knowledge using regular tree languages.

The results of these back-ends in the output format state that whether the written security protocol is *SAFE*, *UNSAFE*, or *INCONCLUSIVE*. Moreover, the intruder is modeled using the Dolev-Yao (dy) model. Using this model, the intruders have full control over the network. All the messages sent can be received by the intruder, he can intercept, analyze, or even modify the messages.[57-59]

7 | FORMAL VERIFICATION USING AVISPA TOOL

For the purpose evaluation purposes, we have considered the basic model of UAV integrated HetNet for implementing the FE technique. The random waypoint mobility model has been chosen for both UEs and UAVs in the network. In addition, the UAVs deployed in the network act as relay nodes for those UEs that are in nonline-of-sight communication with MBS. The UAVs form the transmission links with UEs and MBS and can use any of the techniques for these links such as 3G, LTE, 5G, Wi-Fi, and so on. But since the basic model has been considered, thus, these transmission links use IEEE 802.11 g/n standard. Once the transmission links are formed between UAV-UE and between UAV-MBS, then, these links are used to balance the load requests that are coming from various UE which are in LOS with the UAV. The UE that

FIGURE 7 Role specification in HLPSL for the MBS (M) of the proposed scheme. HLPSL, high-level protocol specification language; MBS, macro based station

```
role alice(M,U:agent,
           SK1:symmetric_key,
           H:hash_func,
           SND,RCV:channel(dy))
played_by M
def=
        local State:nat,
        Na:text,
        F,Fn,N1,Msk,N,Skf,X,Ci:message,
        Inc:hash_func
        const alice_bob_na,sec1:protocol_id
        init State := 0
        transition
                1. State=0 /\ RCV(start) =|>
                   State':=1 /\ Na':=new()
                             /\ SND({M.U.Na'}_SK1)

                2. State=1 /\ RCV({U.M.Na.Fn}_SK1) =|>
                   State':=2 /\ Msk':=new()
                             /\ N':=new()
                             /\ Skf':=new()
                             /\ N1':=H(N)
                             /\ SND({N1'}_SK1)
                             /\ request(M,U,alice_bob_na,Na)
%%% request indicates that MBS has authenticated UE over Na.
                             /\ secret({Msk,Skf},sec1,M)
%%%secret indicates that msk,skf are only known to MBS.

                3. State=2 /\ RCV(Ci) =|>
                   State':=3
end role
```

want to communicate with MBS sends the service requests to UAV. The UAV, then, manages all these service requests and forward them to the MBS. Furthermore, in order to secure the entire system, the proposed methodology implemented in the above steps has been now verified using the AVISPA tool. The verification will help to determine whether the proposed idea is fit to use in real scenarios or not.

The verification of the proposed idea will also be done in two phases:

- Between MBS and UE.
- Between MBS and UE through UAV.

7.1 | Between MBS and UE

This section thoroughly argues the implementation of the proposed steps between MBS and UE in AVISPA tool. For its implementation, two basic roles have been defined, namely, alice and bob representing MBS (M) and UE (U), respectively, having a symmetric key SK1.

Figure 7 shows the specification in HLPSL for the role named *alice* played by *M*. The *M* receives the *start* signal using *RCV()* operation and makes a transition in going from *state 0* to *state 1*. It then sends a nonce signal *<M.U.Na′>* to *U* through a channel which is secured using the symmetric key *SK1* and *SND()* operation. *Channel(dy)* declaration indicates that the channel is for the Dolev-Yao threat model. In transition 2, the *M* receives the reply of nonce from *U* along with the list of functions *<U.M.Na.Fn>* through the channel which is secured using the *RCV()* operation and *SK1*. Then the generation of the master key (*Msk′*), encryption keys (*N′*), and secret keys (*Skf′*) take place using the *new()* operation and sends the hashed value of encryption keys *<N1′>* to *U* through a secure channel using the *SND()* operation. In transition 3, the *M* receives the ciphertext *Ci* from *U*. The declaration *request(M,U,alice_bob_na,Na)* indicates that MBS has authenticated UE over the value Na and declaration *secret({Msk,Skf},sec1,M)* indicates that master key and secret keys are only known to MBS.

Figure 8 depicts the role of *bob* played by *U*. *U* receives the nonce signal *<M.U.Na′>* using *RCV()* operation and its state changes from *state 0* to *state 1*. Then the list of functions *F′* is generated and its hashed value is sent *<U.M.Na′.Fn′>* to *M* using *SK1* and *SND()* operation. In transition 2, *U* receives *<N1>* from *M* using the *RCV()* operation and *SK1*. Then, plaintext message *X′* is encrypted using *N1* and *<Ci′>* is sent to M using *SND()*.

```
role bob(U,M:agent,
        SK1:symmetric_key,
        H:hash_func,
        SND,RCV:channel(dy))
played_by U
def=
        local State:nat,
        Na:text,
        F,Fn,N1,Msk,N,Skf,X,Ci:message,
        Inc:hash_func
        const alice_bob_na,sec1:protocol_id
        init State := 0
        transition

                1. State=0 /\ RCV({M.U.Na'}_SK1) =|>
                   State':=1 /\ F':=new()
                             /\ Fn':=H(F)
                             /\ SND({U.M.Na'.Fn'}_SK1)

                2. State=1 /\ RCV({N1}_SK1) =|>
                   State':=2 /\ X':=new()
                             /\ Ci':={X'}_N1
                             /\ SND(Ci')
end role
```

FIGURE 8 Role specification in HLPSL for the UE (U) of the proposed scheme. HLPSL, high-level protocol specification language; UE, user equipment

```
role session(M,U:agent,
            SK1:symmetric_key,
            H:hash_func)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                alice(M,U,SK1,H,SND1,RCV1)
                /\ bob(U,M,SK1,H,SND2,RCV2)
end role

role environment()
def=
        const
                m,u:agent,
                sk1:symmetric_key,
                h:hash_func,
                na,f,fn,n1,msk,n,skf,x,ci:message,
                alice_bob_na,sec1:protocol_id
        intruder_knowledge = {sk1,na,f,fn,n1,msk,n,skf,x,ci}
        composition
                session(m,u,sk1,h)
                /\ session(u,m,sk1,h)
end role
goal
        secrecy_of sec1
      authentication_on alice_bob_na
end goal
environment()
```

FIGURE 9 Role specification in HLPSL for the session, goal, and environment of the proposed scheme. HLPSL, high-level protocol specification language

Figure 9 depicts the *session, goal,* and *environment* roles. The *session* section includes *alice* (M) and *bob* (U) with concrete arguments. The *environment* consists of all the global constants and the composition of two sessions. In addition, the following goals have been verified:

- *secrecy_of sec1*: means that the master key (*Msk*) and secret keys (*Skf*) are only known to MBS (M).
- *authentication_on alice_bob_na*: means that the MBS (M) has authenticated UE (U) over nonce value *Na*.

7.2 Between MBS and UE through UAV

This section thoroughly argues the implementation of the proposed steps between MBS, UE, and UAV in AVISPA tool. For its implementation, three basic roles have been defined, namely, alice, bob, and sam representing MBS, UE, and UAV

FIGURE 10 Role specification in HLPSL for the MBS of the proposed scheme. HLPSL, high-level protocol specification language; MBS, macro based station

```
role alice(MBS,UE,UAV:agent,
         Ka,Kb,Ks:public_key,
         H:hash_func,
         SND,RCV:channel(dy))
played_by MBS
def=
        local State:nat,
        Na:text,
        F,Fn,N1,Msk,N,Skf,X,Ci:message,
        Inc:hash_func
        const alice_bob_na,sec1:protocol_id
        init State := 0
        transition
                1. State=0 /\ RCV(start) =|>
                   State':=1 /\ Na':=new()
                             /\ SND({MBS.UE.Na'}_Kb)
                             /\ SND({MBS.UAV.Na'}_Ks)

                2. State=1 /\ RCV({UE.MBS.Na.Fn}_Ka)
                           /\ RCV({UAV.MBS.Na}_Ka) =|>
                   State':=2 /\ Msk':=new()
                             /\ N':=new()
                             /\ Skf':=new()
                             /\ N1':=H(N)
                             /\ SND({MBS.UAV.N1'}_Ks)
                             /\ request(MBS,UE,alice_bob_na,Na)
                             /\ secret({Msk,Skf},sec1,MBS)

                3. State=2 /\ RCV(UAV.MBS.Ci) =|>
                   State':=3
end role
```

having their public keys as Ka, Kb, and Ks, respectively. In addition, *channel(dy)* declaration indicates that the channel is for the Dolev-Yao threat model.

Figure 10 depicts the role of *alice* played by *MBS*. *MBS* receives the *start* signal using *RCV()*and its state changes from *state 0* to *state 1*. Then nonce signal *<MBS.UE.Na′>* is sent to *UE* and another nonce signal *<MBS.UAV.Na′>* to UAV using the public keys *Kb*, *Ks* of *UE*, *UAV*, respectively, and *SND()*. In transition 2, the *MBS* receives the reply of nonce from *UE* along with the list of functions *<UE.MBS.Na.Fn>* using the *RCV()* and the public key of *MBS (Ka)*. It also receives *<UAV.MBS.Na>* from UAV using *RCV()* and the public key of *MBS (Ka)*. Then the generation of the master key (*Msk′*), encryption keys (*N′*), and secret keys (*Skf′*) take place using the *new()* and sends *<MBS.UAV.N1′>* to *UAV* using the *UAV* (*Ks*) and *SND()*. In transition 3, the *MBS* receives *Ci* from *UAV* *<UAV.MBS.Ci>*. In addition, *request(MBS,UE,alice_bob_na,Na)* indicates that MBS has authenticated UE over the value Na and declaration *secret({Msk,Skf},sec1,MBS)* indicates that master key and secret keys are only known to MBS.

Figure 11 depicts the role of *bob* played by *UE*. *UE* receives the nonce signal *<MBS.UE.Na′>* from MBS using the public key of *UE* (*Kb*) and *RCV()*. Its state changes from *state 0* to *state 1*. Then the list of functions *F′* is generated and its hashed value is sent *<UE.MBS.Na′.Fn′>* to *MBS* using the public key of *MBS* (*Ka*) and *SND()*. In transition 2, *UE* receives *<UAV.UE.N1′>* from *UAV* using the *RCV()* and the public key of *UE (Kb)*. Then, plaintext message *X′* is encrypted using *N1′* and *<UE.UAV.Ci′>* is sent to UAV using *SND()*.

Figure 12 depicts the role of *sam* played by *UAV*. *UAV* receives the nonce signal *<MBS.UAV.Na′>* from *MBS* using the public key of *UAV* (*Ks*) and *RCV()*. Its state changes from *state 0* to *state 1*. Then *<UAV.MBS.Na>* is sent to *MBS* using the public key of MBS (*Ka*) and *SND()*. In transition 2, *<MBS.UAV.N1′>* is received from *MBS* using the public key of *UAV* (*Ks*) and *RCV()*. Then, *<UAV.UE.N1>* is sent to *UE* using the public key of *UE* (*Kb*) and *SND()*. In transition 3, *UAV* receives *<UE.UAV.Ci′>* from *UE* using *RCV()*. Then, *<UAV.MBS.Ci>* is sent to *MBS* using the *SND()*.

Figure 13 depicts the *session, goal,* and *environment* roles. The *session* section includes *alice* (*MBS*), *bob* (*UE*), and *sam* (*UAV*) with concrete arguments. The *environment* consists of all the global constants and the composition of three sessions. In addition, the following goals have been verified:

- *secrecy_of sec1*: means that the master key (*Msk*) and secret keys (*Skf*) are only known to MBS.
- *authentication_on alice_bob_na*: means that the MBS has authenticated UE over nonce value *Na*.

```
role bob(UE,MBS,UAV:agent,
        Ka,Kb,Ks:public_key,
        H:hash_func,
        SND,RCV:channel(dy))
played_by UE
def=
        local State:nat,
        Na:text,
        F,Fn,N1,Msk,N,Skf,X,Ci:message,
        Inc:hash_func
        const alice_bob_na,sec1:protocol_id
        init State := 0
        transition

                1. State=0 /\ RCV({MBS.UE.Na'}_Kb) =|>
                   State':=1 /\ F':=new()
                             /\ Fn':=H(F)
                             /\ SND({UE.MBS.Na'.Fn'}_Ka)

                2. State=1 /\ RCV({UAV.UE.N1'}_Kb) =|>
                   State':=2 /\ X':=new()
                             /\ Ci':={X'}_N1'
                             /\ SND(UE.UAV.Ci')
end role
```

FIGURE 11 Role specification in HLPSL for the UE of the proposed scheme. HLPSL, high-level protocol specification language; UE, user equipment

```
role sam(UAV,MBS,UE:agent,
        Ka,Kb,Ks:public_key,
        H:hash_func,
        SND,RCV:channel(dy))
played_by UAV
def=
        local State:nat,
        Na:text,
        F,Fn,N1,Msk,N,Skf,X,Ci:message,
        Inc:hash_func
        const alice_bob_na,sec1:protocol_id
        init State := 0
        transition

                1. State=0 /\ RCV({MBS.UAV.Na'}_Ks) =|>
                State':= 1 /\ SND ({UAV.MBS.Na}_Ka)

                2. State=1 /\ RCV({MBS.UAV.N1'}_Ks) =|>
                 State':=2 /\ SND({UAV.UE.N1}_Kb)

                3. State=2 /\ RCV(UE.UAV.Ci') =|>
                 State':=3 /\ SND(UAV.MBS.Ci)
end role
```

FIGURE 12 Role specification in HLPSL for the UAV of proposed scheme. HLPSL, high-level protocol specification language; UAV, unmanned aerial vehicles

8 | SIMULATION RESULTS AND DISCUSSION

This section discusses the simulation results for the proposed scheme. The proposed methodology has been simulated in the AVISPA tool using OFMC back-end. For better understanding, a comparison has been drawn between two entities. First, the data transmission is done without using the FE technique and then, the same data transmission is again done using the proposed FE technique. The comparison and the simulation results are discussed as below:

8.1 | Results: Without using FE technique

This subsection illustrates the data transmission in two phases without implementing the proposed methodology of FE technique. The two phases are: transmission between MBS and UE, and the transmission between MBS and UE through UAV, which are explained in further subsections:

FIGURE 13 Role specification in HLPSL for the session, goal, and environment of the proposed scheme. HLPSL, high-level protocol specification language

```
role session(MBS,UE,UAV:agent,
             Ka,Kb,Ks:public_key,
             H:hash_func)
def=
        local
                SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                alice(MBS,UE,UAV,Ka,Kb,Ks,H,SND1,RCV1)
                /\ bob(UE,MBS,UAV,Ka,Kb,Ks,H,SND2,RCV2)
                /\ sam(UAV,MBS,UE,Ka,Kb,Ks,H,SND3,RCV3)
end role

role environment()
def=
        const
                mbs,ue,uav:agent,
                ka,kb,ks:public_key,
                h:hash_func,
                na,f,fn,n1,msk,n,skf,x,ci:message,
                alice_bob_na,sec1:protocol_id
        intruder_knowledge = {mbs,ue,uav,ka,kb,ks,na,f,fn,n1,msk,n,skf,x,ci}
        composition
                session(mbs,ue,uav,ka,kb,ks,h)
                /\ session(ue,mbs,uav,ka,kb,ks,h)
                /\ session(uav,mbs,ue,ka,kb,ks,h)
end role
goal
        secrecy_of sec1
      authentication_on alice_bob_na
end goal
environment()
```

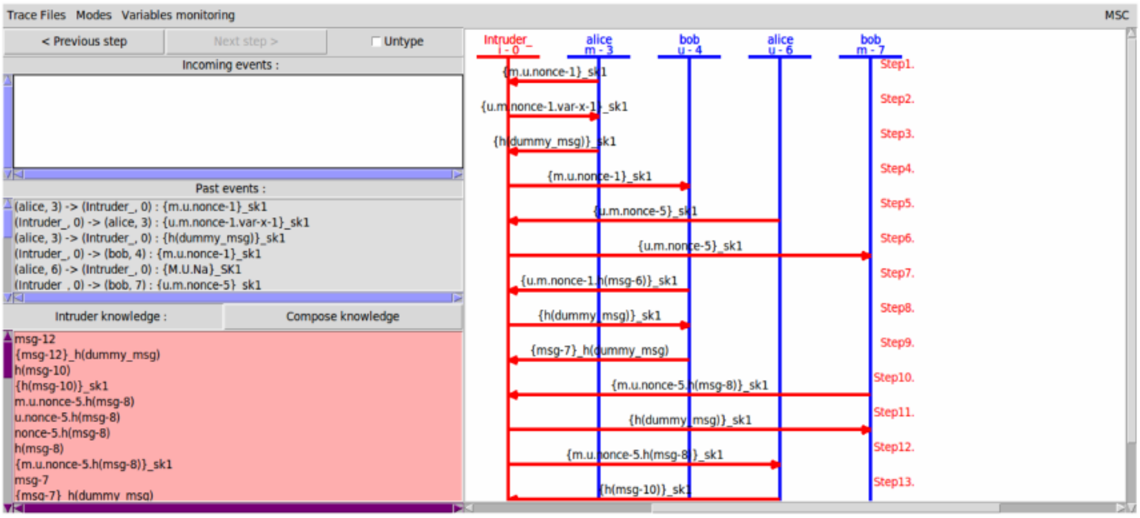

FIGURE 14 Step by step process of data transmission between MBS and UE. MBS, macro based station; UE, user equipment

8.1.1 | Transmission between MBS and UE

Figure 14 depicts the ongoing data transmission between MBS (Alice) and UE (Bob) without using FE technique. Here, two sessions have been started between MBS and UE which are shown pictorially. The data transmission begins when MBS (denoted as m-3) generates the nonce-1 signal. This nonce-1 signal is intended to be sent to UE (denoted as u-4) along with the message but intruder node (denoted as i-0) impersonates itself as UE and hence, receives the message from MBS. The intruder node, then, alters with the original message and sends back the message to MBS, again impersonating as UE. This process continues to go on till step 13, wherein each step, each message is sent or received by intruder node by impersonating itself as either MBS or UE. Moreover, on the left-hand side of the pictorial representation in Figure 14, a tab named "intruder knowledge" is present which shows all the data that the intruder node collects during the transmission.

Furthermore, Figure 15 shows the result of the above said transmission between MBS and UE. The result displayed in Figure 15 confirms that the ongoing data transmission is UNSAFE. This result clearly indicates, in the DETAILS section, that attack has been found and the details of the attack are given in ATTACK TRACE section.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/step1unsafe.if
GOAL
  authentication_on_alice_bob_na
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.05s
  visitedNodes: 1 nodes
  depth: 1 plies
ATTACK TRACE
i -> (m,3): start
(m,3) -> i: {m.u.Na(1)}_sk1
i -> (m,3): {u.m.Na(1).x254}_sk1
(m,3) -> i: {h(dummy_msg)}_sk1
```

FIGURE 15 Simulation result scheme under OFMC. OFMC, on-the-fly model-checker

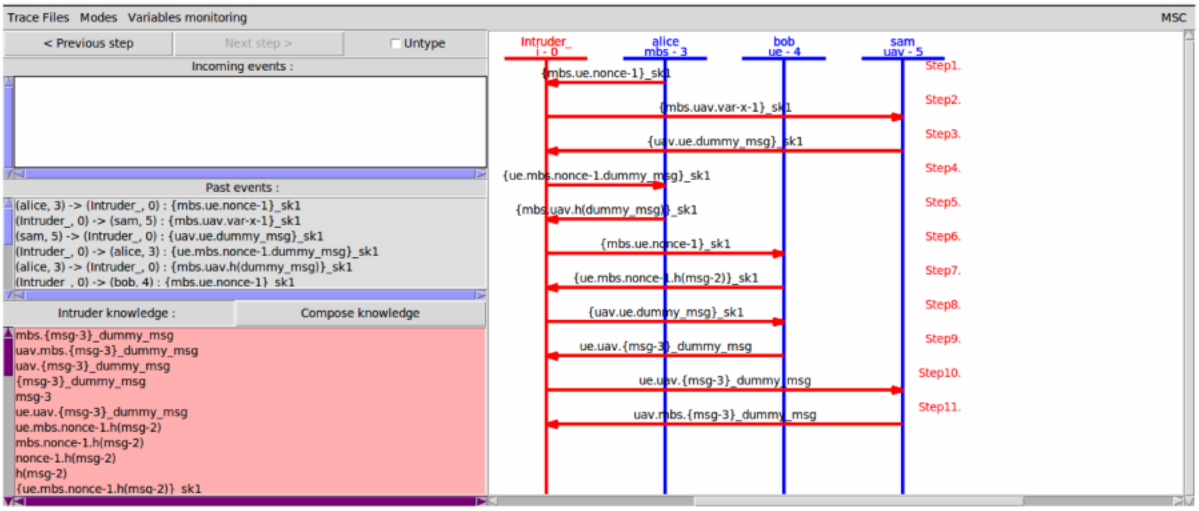

FIGURE 16 Step by step process of data transmission between MBS, UE, and UAV. MBS, macro based station; UAV, unmanned aerial vehicles; UE, user equipment

8.1.2 | Transmission between MBS and UE through UAV

Figure 16 depicts the ongoing data transmission between MBS (Alice), UE (Bob), and UAV (Sam) without using FE technique. Here, one session has been started between MBS, UE, and UAV which is shown pictorially. The data transmission begins when MBS (denoted as mbs-3) generates the nonce-1 signal. This nonce-1 signal is intended to be sent to UE along with the messages but intruder node (denoted as i-0) impersonates itself as UE and hence, receives the message from MBS. The intruder node, then, alters with the original message and sends the message to UAV, again impersonating itself as UE. The UAV sends the message to UE but again this message is received by intruder node, impersonating itself as UE. This process continues to go on till step 11, wherein each step, each message is sent or received by intruder node by impersonating itself as either MBS or UE or UAV. Moreover, on the left-hand side of the pictorial representation, a tab named "intruder knowledge" is present which shows all the data that the intruder node collects during the transmission.

Figure 17 shows the result of the above said transmission between MBS, UE, and UAV. The result displayed in Figure 17 confirms that the ongoing data transmission is UNSAFE. This result clearly indicates in the DETAILS section that attack has been found and the details of the attack are given in ATTACK TRACE section.

FIGURE 17 Simulation result scheme under OFMC. OFMC, on-the-fly model-checker

```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/step2unsafe.if
GOAL
  authentication_on_alice_bob_na
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.08s
  visitedNodes: 6 nodes
  depth: 2 plies
ATTACK TRACE
i -> (mbs,3): start
(mbs,3) -> i: {mbs.ue.Na(1)}_sk1
i -> (uav,3): {mbs.uav.x255}_sk1
(uav,3) -> i: {uav.ue.dummy_msg}_sk1
i -> (mbs,3): {ue.mbs.Na(1).dummy_msg}_sk1
(mbs,3) -> i: {mbs.uav.h(dummy_msg)}_sk1
```

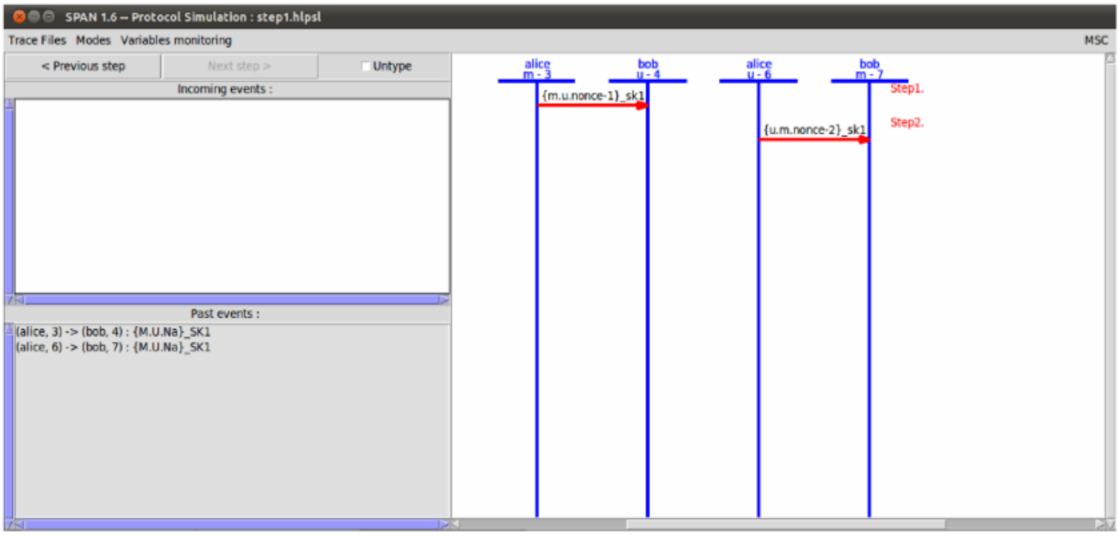

FIGURE 18 Step by step process of data transmission in protocol simulation platform

8.2 | Results: Using FE technique

This subsection illustrates the data transmission in two phases by implementing the proposed methodology of FE technique. The two phases are: transmission between MBS and UE, and the transmission between MBS and UE through UAV, which are explained in further subsections:

8.2.1 | FE between MBS and UE

Figure 18 depicts the ongoing data transmission between MBS (Alice) and UE (Bob) using FE technique. Here, two sessions have been started between MBS and UE which are shown pictorially. The data transmission begins when MBS (denoted as m-3) generates the nonce-1 signal. This nonce-1 signal is transmitted between MBS and UE (denoted as u-4) which has been secured using the symmetric key sk1. Similarly, UE initiates the transmission process between itself and MBS. Nonce-2 is sent from UE to MBS which again has been secured using the symmetric key sk2. Furthermore, the algorithmic denotations of these steps can be observed in the past events section of the protocol simulation platform. Moreover, using FE technique, the intruder node is not able to interfere in the ongoing transmission.

Figure 19 shows the result of the implementation of the proposed technique. The result displayed in Figure 19 confirms that the proposed protocol is SAFE. This ensures that no attack can occur in the transmission of MBS and UE in the UAV-HetNet. The whole data transmission gets secured using the FE technique implementation. Thus, these results approve the theoretical analysis of the consider security mechanism.

8.2.2 | FE between MBS and UE through UAV

Figure 20 depicts the ongoing data transmission between MBS, UE, and UAV using FE technique. Here, three sessions have been started between MBS, UE, and UAV which are shown pictorially. The data transmission begins when UAV (denoted as uav-11) generates the nonce-1 signal. This nonce-1 signal is transmitted between UAV and MBS (denoted as mbs-12) which has been secured using the public key *kb*. Similarly, UAV initiates another transmission process between itself and UE (denoted by ue-13) which has been secured using the public key *ks*. These transmission processes continue like this between MBS, UE, and UAV up to step 12. The algorithmic denotations of these steps have been given in the past events section of the protocol simulation diagram. Moreover, using FE technique, the intruder node is not able to interfere in the ongoing transmission.

Figure 21 shows the result of the implementation of the proposed technique. Figure 21 confirms that the proposed protocol is SAFE. This ensures that no attack can occur in the network. The whole data transmission gets secured using the FE technique implementation. Thus, these results approve the theoretical analysis in the considered network.

8.3 | Discussion and future scope

The simulation results clearly indicate that the proposed FE technique, which has been implemented in two steps: between MBS and UE and between UE and MBS through UAV, is completely safe and secure against the intruder attacks. The results show that it is SAFE to implement this technique for the Dolev-Yao attack model. On doing a detailed review of Table 2, it is noted that various literary studies have done the work to secure several kinds of networks using different security approaches. But the security of UAV collaborative HetNet through the FE technique is hardly explored so far. Few reported works, such as Reference 5 only surveys the state-of-the-art intrusion detection mechanisms for networked UAV environments. The research work in Reference 12 has only talked about the coagulation attack on networked UAV without providing the security mechanism against it. However, the study[19] presents a secure UAV-HetNet by using the IBE technique against the attacks. But, in the decryption phase of the IBE scheme, due to the “all and nothing” process, if the third party like the public key generation center is compromised, then the data is at a greater risk of disclosure. The discussion under our research study provides complete security to the transmitted data by offering distinct keys for various encrypted function in terms of its decryption phase also. The robustness of the decryption process can safeguard the private data of users from the malicious activities within the network as the intruders will be unable to read the contents of data. Moreover, when the decryption process is done by having particular secret keys for the respective function of the encrypted data, rest of the data remains secured, and private from any other user, for whom access is not allowed for that data. Moreover, in order to have a better understanding, a summary of comparative study between conventional approaches and the proposed scheme has been tabulated in the form of Table 4.

Thus, the collaboration of the FE technique and UAV assisted HetNet, makes the network secure, robust, and sturdy against the intruder nodes. However, there are some limitations of this research study, one of them being that the FE technique takes only one input at a time and cannot handle multiple inputs simultaneously. This means that the FE technique is a single-input technique and to handle a large amount of data, this technique can take a huge amount of time for its operations. Furthermore, the technical specifications of the UAV assisted HetNet has not been discussed such as optimal UAV placement height, coverage of UAV, the total area covered under HetNet. Hence, these technical specifications may also be considered in future research studies to attain effectiveness and efficiency for achieving the goals of security and performance. The productiveness of the FE technique implementation can also be increased by taking into consideration the key management process. Moreover, the FE technique implemented in this article has only been verified by the AVISPA tool. However, the same scenario may also be validated through other tools like ProVerif, which can further ensure that this technique is indeed completely safe for the UAV-HetNet.

FIGURE 19 Simulation result of phase-I of proposed scheme under OFMC. OFMC, on-the-fly model-checker

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/step1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 25 nodes
  depth: 4 plies
```

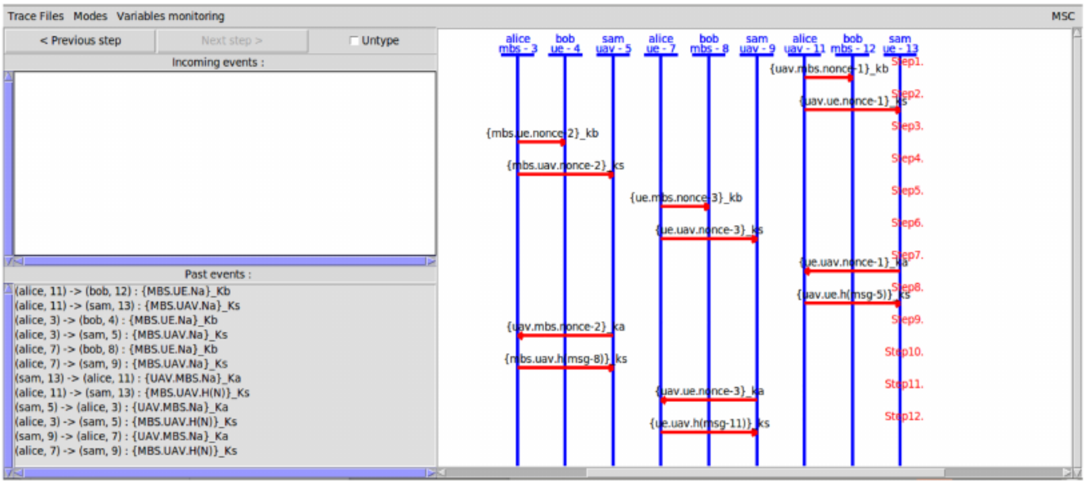

FIGURE 20 Step by step process of data transmission in protocol simulation platform

FIGURE 21 Simulation result of phase-II of proposed scheme under OFMC. OFMC, on-the-fly model-checker

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/step2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 63 nodes
  depth: 6 plies
```

TABLE 4 Comparative study between the conventional approaches and the proposed scheme

Conventional approaches			Proposed scheme: Functional encryption
Reference	**Techniques**	**Demerits**	**Merits**
18	Attribute-based cryptography technique	During decryption process, the ciphertext is decrypted wholly which reveals the entire message.	During decryption process, the ciphertext is decrypted in particular portions only, for which secret keys are present.
19	Identity-based encryption	If public key generation center is compromised, then the data is at a greater risk of disclosure.	In MBS, entire data has been stored in accordance with list of functions and the secret keys are generated, respectively, for each function of plaintext. So, if MBS is compromised, even then, entire data is not at a risk of disclosure.
21	Diffie-Hellman key exchange	Authentication process is not done.	Authentication process is done among all entities by using nonce signal.
23	Homomorphic encryption	The decryption of ciphertext will either reveal the entire message or will not be decrypted at all.	The decryption of ciphertext will generate only that portion of plaintext which the user has demanded.
44	Challenge-based trust mechanism	Strategy can be failed, if the malicious nodes have some information about nearby traffic.	Even if the malicious nodes have some information regarding ongoing traffic, they cannot reveal the entire plaintext message as it is encrypted according to different functions.

Abbreviation: MBS, macro based station.

9 | CONCLUSION

A novel approach has been proposed and validated in this article for securing the UAV assisted HetNet in the dense urban scenarios by using the FE technique. As discussed in this article, UAV integrated HetNet is vulnerable to various kinds of security attacks and malicious activities. Hence, it becomes necessary to provide security to the entire network and the data against such attacks. In this article, the implementation of the FE technique has been done in the UAV integrated HetNet in two phases- the first phase is FE between UE and MBS, and the second phase is FE between MBS and UE through UAV. The proposed approach has, then, been validated and simulated using the widely accepted AVISPA tool. The validation and simulation results of AVISPA clearly indicate that the proposed technique is SAFE from intrusion activities. This means that the implementation of this technique on the dense urban areas provides the desired security to the UE and its data transmission from the intruders. The future direction is to enhance the existing proposed methodology by using multi-input FE.

ORCID

Sachin Kumar Gupta https://orcid.org/0000-0001-8270-5853
Mamoon Rashid https://orcid.org/0000-0002-8302-4571

REFERENCES

1. Tang L, He Y, Zhou Z, Ren Y, Mumtaz S, Rodriguez J. A distance-sensitive distributed repulsive sleeping approach for dependable coverage in heterogeneous cellular networks. *Trans Emerging Tel Tech*. 2019;30(11):1–19. https://doi.org/10.1002/ett.3784.
2. Ghosh A, Saha Misra I, Kundu A. Coverage and rate analysis in two-tier heterogeneous networks under suburban and urban scenarios. *Trans Emerging Tel Tech*. 2019;30:e3648. https://doi.org/10.1002/ett.3648.
3. Damnjanovic A, Montojo J, Wei Y, et al. A survey on 3GPP heterogeneous networks. *IEEE Wireless Commun*. 2011;18(3):10-21.
4. Khandekar A, Bhushan N, Tingfang J, Vanghi V. LTE-advanced: heterogeneous networks. Paper presented at: IEEE European Wireless Conference; 2010;978-982; Lucca, Italy.
5. Choudhary G, Sharma V, You I, Yim K, Chen I-R, Cho J-H. Intrusion detection systems for networked unmanned aerial vehicles: a survey. Paper presented at: 14th IEEE International Wireless Communications & Mobile Computing Conference; 2018;560-565; Limassol, Cyprus.
6. Gupta A, Sundhan S, Alsamhi SH, Gupta SK. Review for capacity and coverage improvement in aerially controlled heterogeneous network, Vijay Janyani, Ghanshyam Singh, Manish Tiwari, Antonio d'Alessandro, *Optical and Wireless Technologies. Lecture Notes in Electrical Engineering*. Singapore: Springer; 2020:546.
7. Gupta L, Jain R, Vaszkun G. Survey of important issues in UAV communication networks. *IEEE Commun Surv Tutor*. 2016;18(2):1123-1152.
8. Shakoor S, Kaleem Z, Baig MI, Chughtai O, Duong TQ, Nguyen LD. Role of UAVs in public safety communications: energy efficiency perspective. *IEEE Access*. 2019;7:140665-140679.
9. Simic M, Bil C, Vojisavljevic V. Investigation in wireless power transmission for UAV charging. Paper presented at: 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Marina Bay Sands Hotel, Singapore. Vol. 80; 2015;1846-1855.
10. Cisco White Paper. Cisco visual networking index: global mobile data traffic forecast update, 2016–2021. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. Accessed February 2017.
11. Yaacoub J-P, Noura H, Salman O, Chehab A. Security analysis of drones systems: attacks, limitations, and recommendations. *Internet Things*. 2020;11:100218. https://doi.org/10.1016/j.iot.2020.100218.
12. Sharma V, Jayakody DNK, Srinivasan K, Kumar R. Coagulation attacks over networked UAVs: concept, challenges, and research aspects. *Int J Eng Technol*. 2018;7(3.13):183-187.
13. Tanwar S, Vora J, Tyagi S, Kumar N, Obaidat MS. A systematic review on security issues in vehicular ad hoc network. *Secur Privacy*. 2018;1:e39. https://doi.org/10.1002/spy2.39.
14. Oubbati OS, Atiquzzaman M, Lorenz P, Tareque MH, Hossain MS. Routing in flying ad hoc networks: survey, constraints, and future challenge perspectives. *IEEE Access*. 2019;7:81057-81105.
15. Fotouhi A, Qiang H, Ding M, et al. Survey on UAV cellular communications: practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun Surv Tutor*. 2019;21(4):3417-3442.
16. Kaleem Z, Rehmani MH. Amateur drone monitoring: state-of-the-art architectures, key enabling technologies, and future research directions. *IEEE Wireless Commun*. 2018;25(2):150-159.
17. Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data. Paper presented at: Proceedings of the 13th ACM Conference on Computer and Communications Security- CCS'06; Alexandria Virginia USA. 2006.
18. Belguith S, Kaaniche N, Hammoudeh M. Analysis of attribute-based cryptographic techniques and their application to protect cloud services. *Trans Emerging Tel Tech*. 2019;30:e3667. https://doi.org/10.1002/ett.3667.
19. Rashid A, Sharma D, Lone TA, Gupta S, Gupta SK. Secure communication in UAV assisted HetNets: a proposed model. Paper presented at: Security, Privacy, and Anonymity in Computation, Communication, and Storage, SpaCCS, Atlanta, GA, USA. Vol. 11611; 2019;427-440.
20. Shamir A. Identity-based cryptosystems and signature schemes. Paper presented a: Advances in Cryptology - CRYPT0 '84, LNCS, Vol. 196; 1985;47-53.
21. Diffie W, Hellman ME. Privacy and authentication: an introduction to cryptography. *Proc IEEE*. 1979;67(3):397-427.
22. Yi X, Paulet R, Bertino E. *Homomorphic Encryption and Applications*. Switzerland: Springer Briefs in Computer Science; 2014:2191-5768.
23. Murugesan A, Saminathan B, Al-Turjman F, Kumar RL. Analysis on Homomorphic technique for data security in fog computing. *Trans Emerging Tel Tech*. 2020;31:1–16. https://doi.org/10.1002/ett.3990.
24. Sharma D, Jinwala D. Functional encryption in IoT E-health care system. Paper presented at: Proceedings of the 11th International Conference on Information Systems Security, Kolkata, India. Vol. 9478; 2015;345-363; ICISS.
25. Li Y, Cai L. UAV-assisted dynamic coverage in a heterogeneous cellular system. *IEEE Network*. 2017;31(4):56-61.
26. Choudhary G, Sharma V, Gupta T, Kim J, You I. Internet of drones (IoD): threats, vulnerability, and security perspectives. Paper presented at: The 3rd International Symposium on Mobile Internet Security (MobiSec'18), Waterfront Cebu City Hotel & Casino Restaurants, Cebu, Philippines. Vol. 37; 2018;1-13.
27. Alsamhi SH, Ansari MS, Ma O, Almalki F, Gupta SK. Tethered balloon Technology in Design Solutions for rescue and relief Team emergency communication services. *Disaster Med Public Health Prep*. 2019;13(2):203-210.
28. Bekmezci I, Şentürk E, Türker T. Security issues in flying ad-hoc networks (FANETs). *J Aeronaut Space Technol*. 2016;9(2):13-21.
29. Kandar S, Chaudhari D, Bhattacharjee A, Dhara BC. Image encryption using sequence generated by cyclic group. *J Inform Secur Appl*. 2019;44:117-129.
30. Anwar MZ, Kaleem Z, Jamalipour A. Machine learning inspired sound-based amateur drone detection for public safety applications. *IEEE Trans Veh Technol*. 2019;68(3):2526-2534.

31. Oubbati OS, Chaib N, Lakas A, Lorenz P, Rachedi A. UAV-assisted supporting services connectivity in urban VANETs. *IEEE Trans Veh Technol*. 2019;68(4):3944-3951.
32. Sharma D, Rashid A, Gupta S, Gupta SK. A functional encryption technique in UAV integrated HetNet: a proposed model. *Int J Simul Syst Sci Technol*. 2019;20(S1):7.1-7.7.
33. 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. https://doi.org/10.1016/j.adhoc.2018.09.004.
34. Kumbhar A, Guvenc I, Singh S, Tuncer A. Exploiting LTE-advanced HetNets and FeICIC for UAV-assisted public safety communications. *IEEE Access*. 2018;6:783-796.
35. Sun J, Wang W, Kou L, et al. A data authentication scheme for UAV ad hoc network communication. *J Supercomput*. 2017;76:4041-4056.
36. He D, Chan S, Guizani M. Communication security of unmanned aerial vehicles. *IEEE Wireless Commun*. 2017;24(4):134-139.
37. Haque MS, Chowdhury MU. A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV). *Int Conf Secur Privacy Commun Netw*. 2018;239:113-122.
38. Sedjelmaci H, Senouci SM, Messous M-A. How to detect cyber-attacks in unmanned aerial vehicles network? Paper presented at: IEEE Global Communications Conference (GLOBECOM), Washington DC, USA. 2016.
39. Mitchell R, Chen I-R. Specification based intrusion detection for unmanned aircraft systems. Paper presented at: Proceedings of the First ACM MobiHoc Workshop on Airborne Networks and Communications; 2012;31-36.
40. Yoon K, Park D, Yim Y, Kim K, Yang SK, Robinson M. Security authentication system using encrypted channel on UAV network. Paper presented at: First IEEE International Conference on Robotic Computing (IRC), Taichung, Taiwan. 2017;393-398.
41. Li B, Fei Z, Zhang Y. UAV communications for 5G and beyond: recent advances and future trends. *IEEE Internet Things J*. 2019;6(2):2241-2263.
42. Rodday NM, Schmidt RDO, Pras A. Exploring security vulnerabilities of unmanned aerial vehicles. Paper presented at: NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium; 2016;993-994.
43. Mahfouz A, Mahmoud TM, Eldin AS. A survey on behavioral biometric authentication on smartphones. *J Inf Secur Appl*. 2017;37:28-37.
44. Li W, For Kwok L. Challenge-based collaborative intrusion detection networks under passive message fingerprint attack: a further analysis. *J Inf Secur Appl*. 2019;47:1-7.
45. Mishra D, Kumar Das A, Chaturvedi A, Mukhopadhyay S. A secure password-based authentication and key agreement scheme using smart cards. *J Inf Secur Appl*. 2015;23:28-43.
46. Safa NS, Maple C, Watson T, Solms RV. Motivation and opportunity based model to reduce information security insider threats in organisations. *J Inf Secur Appl*. 2018;40:247-257.
47. Ammar M, Russello G, Crispo B. Internet of things: a survey on the security of IoT frameworks. *J Inf Secur Appl*. 2018;38:8-27.
48. Kaleem Z, Yousaf M, Qamar A, et al. UAV-empowered disaster-resilient edge architecture for delay-sensitive communication. *IEEE Network*. 2019;33:124-132.
49. Sedjelmaci H, Messous MA, Senouci SM, Brahmi IH. Toward a lightweight and efficient UAV-aided VANET. *Trans Emerging Tel Tech*. 2019;30(8):1–15. https://doi.org/10.1002/ett.3520.
50. Fotohi R, Nazemi E, Aliee FS. An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks. *Veh Commun*. 2020;26:100267. https://doi.org/10.1016/j.vehcom.2020.100267.
51. Boneh D, Sahai A, Waters B. Functional encryption: definitions and challenges. Lecture notes in computer science, theory of cryptography. *Lect Notes Comput Sci*. 2011;6597:253-273.
52. Boneh D, Sahai A, Waters B. Functional encryption. *Commun ACM*. 2012;55(11):56-64.
53. Goldwasser S, Gordon SD, Goyal V, et al. Multi-input Functional encryption. *Adv Cryptol*. 2014;8441:578-602.
54. Takkinen L. Analysing security protocols with AVISPA. Paper presented at: TKK T-110.7290 Research Seminar on Network Security; 2006.
55. Amin R, Biswas GP. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Netw*, Ottawa, Canada: 2016;36:58-80.
56. Dhillon PK, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services. *J Inf Secur Appl*. 2017;34:255-270.
57. Team TA. AVISPA v1.1 user manual. Information Society Technologies Programme. http://avispa-project.org/. Accessed June 2006.
58. HLPSL Tutorial. A beginner's guide to modelling and analysing Internet security protocols. The AVISPA team Document Version: 1.1; 2006.
59. Farasha MS, Turkanovi M, Kumari S, Hölbl M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of things environment. *Ad Hoc Netw*. 2016;36(1):152-176.

How to cite this article: Sharma D, Gupta SK, Rashid A, Gupta S, Rashid M, Srivastava A. A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. *Trans Emerging Tel Tech*. 2021;32:e4114. https://doi.org/10.1002/ett.4114