A Functional Encryption Technique in UAV Integrated HetNet: A Proposed Model

Diwankshi Sharma [1], Aabid Rashid [2], Sumeet Gupta [3], Sachin Kr. Gupta [4*]

[1,2,3,4] *School of Electronics & Communication Engineering*
Shri Mata Vaishno Devi University
Kakryal-182320, Katra, Jammu & Kashmir, India.
Email: [1] diwankshisharma96@gmail.com, [2] waniaabid1992@gmail.com,
[3] sumeet.gupta@smvdu.ac.in, [4] sachin.rs.eee@iitbhu.ac.in

***Abstract* - Data users are increasing rapidly in dense urban scenarios. For managing this huge increase, a shift has occurred from the traditional homogeneous network to Heterogeneous Network (HetNet). Unmanned Aerial Vehicles (UAVs) can also be used with HetNets resulting in optimization in the network. However, in UAV integrated HetNet, plenty of User Equipment (UE) is operating. In such a huge variety, intruder nodes can operate easily and can spread malicious activities in the network. This makes the overall communication vulnerable to various kinds of security attacks. Hence, to secure the data against the intrusion attacks, Functional Encryption (FE) technique is used in this paper. The FE allows the users to learn only about particular information in the message without decrypting the whole message. The whole process of implementing FE is proposed in two phases: first between UE & Macro Base Station (MBS) and second between MBS & UE through UAV. The proposed idea will be validated using the AVISPA tool with the help of HLPSL codes. The expected outcome of the proposed technique is the secure communication in the urban area.**

Keywords - Functional Encryption, HetNet, UAV, dense urban scenarios, intruder nodes.

I. INTRODUCTION

The demand for cellular data traffic is increasing rapidly. According to the Cisco white paper, annual global IP traffic will reach 4.8 ZB (ZB=ZettaBytes) per year by 2022 as compared to 1.5 ZB per year in 2017. Moreover, global IP traffic will increase threefold over the next five years. By 2022, the number of devices connected to IP networks will be more than three times the overall global population and the mobile data traffic will increase sevenfold between 2017 and 2022 globally [1].

To handle such increasing demand, the traditional homogeneous networks were found inefficient. Hence, the HetNets came into existence which is a collaboration of various kinds of other networks [2]. In HetNet, a diverse set of base stations can be utilized to improve the spectral efficiency per unit area in dense urban scenarios. The HetNet consists of high power macro base station with several low power base stations in picocells, femtocells, and relay nodes. While the placement of macro base station is done with careful planning, the placement of low power base stations is generally done in an ad-hoc fashion. The picocells, femtocells, and relays are used to remove coverage holes in the network, thereby, increasing its capacity [3]. Unprecedented developments have been seen in the UAVs' domain over the past few years. Owing to their several merits of dynamic reconfigurability, fast response, and ease of deployment, their applications can be extended to public safety, medical services, disaster management, and military missions. Moreover, many big industries such as Google, Facebook and Amazon have also been attracted towards the applications of UAVs [4]. The capability of UAVs for public safety and surveillance of targets can also be further explored.

Integration of UAVs and HetNets together can be the solution to various challenging tasks. Their collaboration results in efficiently managing the exponential increase in the demand for mobile data traffic. With more optimization in this network, the user throughput gets exceedingly increased in dense urban scenarios by minimizing the end to end delays. Moreover, this integration can also be utilized to improve the spectral efficiency per unit area for dense urban scenarios. This leads us to a point where we can deploy HetNets assisted by UAVs in dense urban areas for handling the capacity of the network. The example of the UAV integrated HetNet architecture for urban scenarios is shown in figure (1). However, the data users operating in these networks need to be secured against the intruder nodes. The intruder nodes can spoof, masquerade or eavesdrop the data. The intruder nodes can even impersonate the sender or receiver of crucial data. The presence of these intruder nodes makes the data transmission in the network very vulnerable. Moreover, it becomes difficult to remove these nodes from the network. Hence, the privacy, confidentiality, and authenticity of data become important in dense urban scenarios. For making the users data more secure against the attacks, various security techniques can be applied over this network. The security mechanism will help to make the data robust against the attacks. One of such techniques is the FE technique. The main advantage of FE is that using this technique, there is no need to decrypt the whole message. Only a particular function of the message will be decrypted

and the information will be provided to the users. In this way, the whole data of the user will remain secured.

A. Research Objective and Motivation

A dense urban area has a huge number of active UE that are transmitting the data. In such a huge amount of user nodes, any node can spread some malicious activities in the network, thereby, posing a threat to the users' privacy and confidentiality. Any important information will get modified or lost due to several intrusion activities. Thus, in this paper, FE technique will be implemented over the network. This technique will ensure that the users' data remains secured against the intrusion attacks. Only authenticated users will be able to receive the information. The whole message will be encrypted and only respective secret keys will allow the decryption of the message. Thus, the malicious nodes will not be able to get the whole information of that message.

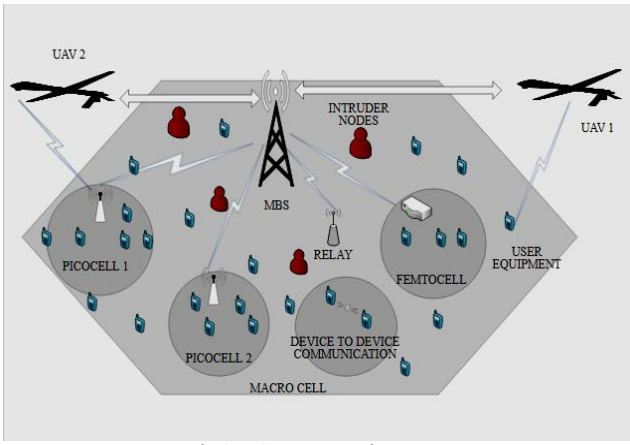

Fig 1: UAV Integrated HetNet.

B. Organization of Paper

The rest of the article is organized as: section 2 discusses existing literature survey that has been carried out in the related work and introduces the research gap. Further, section 3 presents the preliminaries of FE technique, section 4 is regarding the proposed approach to implement the mechanism and finally, section 5 comes up with a conclusion and future directions.

II. LITERATURE SURVEY

As the UAV integrated HetNets are vulnerable to various security attacks, many research scholars have implemented various security techniques on these kinds of networks. A lot of research work is going on in this field to make the network more robust against the attacks.

According to Choudhary et al [4], the state-of-the-art UAV-IDS survey has been done along with its approaches and taxonomies. A brief description of the existing IDS mechanisms based on information gathering sources, deployment strategies, detection methods, detection states, IDS acknowledgment, and intrusion types has been made.

The various challenges faced in implementing UAV-IDS has also been discussed. In Bekmezci et al [5], the researcher has discussed the flying ad-hoc networks (FANETs) and its various security issues and challenges. Issues such as eavesdropping, spoofing, wormhole attacks and many more have been discussed in detail. According to Sun et al [6], a data authentication scheme has been proposed for UAV ad hoc network communication by designing an efficient and energy-saving network architecture based on clustering stratification. A double authentication watermarking scheme has also been proposed for maintaining the integrity of collected data and the filtering of malicious data from the network. The authentication watermark is generated using self-characteristic of the collected data and then is embedded into the data at random. In Sedjelmaci et al [7], an intrusion detection system has been applied in UAV aided networks.

This paper focuses on mainly two things: activation of the intrusion monitoring process and attacker ejection. Moreover, to address security issues in the network, a Bayesian Game Model has been proposed to accurately detect the attacks with low overhead. Apart from the above, the comparative study of the existing security approach of related surveys in the literature has been done in Table I. A close analysis of the studies as mentioned in this section and Table I establishes a research gap that increasing the security of UAV assisted HetNets using FE technique has not been studied, so far. Though, network has been made secured by using various security techniques like probability approaches, estimation models etc. but the numerous advantages of FE remain unexplored for implementation. The security provided by FE can be applied to make a network more robust against the intruders. Hence, the implementation of this technique needs to be explored further.

III. FUNCTIONAL ENCRYPTION

The concept of FE was given by Sahai and Waters in 2011. The pictorial representation of FE is shown in figure (2). Roughly, FE can be defined as a technique in which the key holder can learn only about a specific function of the encrypted data and nothing else. Only a single plaintext is considered for the implementation of the FE technique. This technique has the following four steps [15]:

1. Setup phase: generates a public key and a master secret key pair
   $(pp, mk) \leftarrow setup\ (1^{\lambda})$
2. Key generation phase: generates secret keys sk_f
   $sk_f \leftarrow keygen\ (mk, k)$
3. Encrypt phase: encrypts the message x
   $c \leftarrow enc\ (pp, x)$
4. Decrypt phase: uses sk_f to compute the $f(x)$
   $y \leftarrow dec\ (sk_f, c)$

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

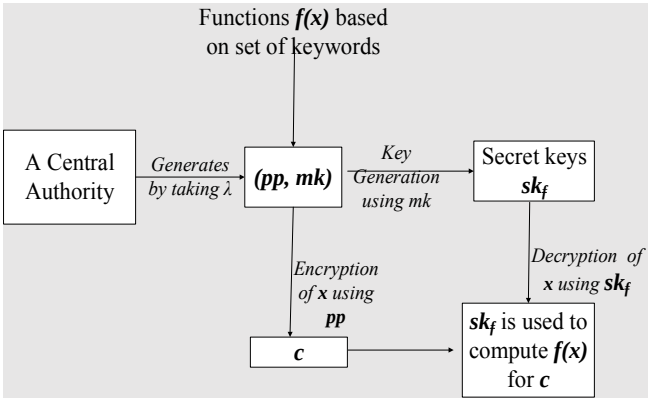

Fig 2: Pictorial representation of FE

TABLE I: COMPARISON OF EXISTING SECURITY APPROACH OF RELATED SURVEYS IN THE LITERATURE

Ref. No.	N/W Type	Attacks	IDS Solution	Routing Support	Security Approach/ Mechanism/Model	Simulation Platform	HetNet	Characteristics
[8]	UAV Aided MANETs & VANETs	Lethal cyber-attacks: false information dissemination, GPS spoofing, jamming, Black and Gray hole	Distributed Intrusion Monitoring and Detection Approach	DTN Routing	Hierarchical Intrusion Detection (Rules-Based & Anomaly Detection Techniques) and Response Scheme implemented at UAV & ground level stations	NS-3	No	• Smart activation of intrusion monitoring process; however trade-off between HDR and overhead is considered. • High-level of security with HDR>93%. • Low false positive rate <3%, • Prompt detection with low communication overhead.
[9]	UAV Communications (wireless standard may be 3G, 4G, 5G, Wi-Fi, WiMAX)	GPS spoofing, Wi-Fi attacks	Non-cryptographic solution: monitoring total received power in GPS band, the antenna array	No	Jamming to noise sensing defense & Multi-antenna defense against GPS spoofing, Enabled WPA2 & disabled broadcast of SSID for Wi-Fi attacks	Ettus radio (USRP)	———	• GPS spoofing & Wi-Fi attacks can be done easily at low cost. • Good balance between the strength of security measures and network performance.
[10]	Interconnected UAV based Base Station Networks	Cyber Attacks: threats to data integrity & network availability	Cyber Detection Mechanism	TLS, DTNs: opportunistic data forwarding	Threat estimation model is based on Belief approach	NS-3	Yes	• High Detection Rate. • Decrease false positive rate and negative rate.
[11]	Sensors or Actuators based UAS	Attacker Archetypes: Reckless and Random	Behavior rule & Transforming rules to State Machines Specification based	———	Detection Probability Approaches	Monte Carlo simulation test bed to collect numerical data	No	• Reduced false alarm probability <5% for reckless attackers & < 20% for random attackers. • The trade-off between false positive & detection rates.
[12]	HetNet WSN	Get data from the sensor	Secure hierarchical topology structure	———	Q-Composite Random Key Pre-distribution	———	Yes	• Effectively improve network connectivity, • Support scalability, and ensure key effectiveness without affecting security connectivity and resilience.

[13]	IoT E-Health care system	Threats on data confidentiality and privacy	———	———	Functional Virtual Machine along with Ciphertext-Policy Attribute-based encryption and Functional encryption.	CPABE toolkit and Pairing-based Cryptography (PBC) library.	No	• Provides relevant information according to users' requirements. • The limitation is the use of double encryption. • Preserved data confidentiality and privacy
[14]	UAV assisted Multi-level ad-hoc wireless networks	Repudiation attacks: threats on privacy, integrity, authenticity, availability	Localized Intrusion Detection System	WTLS	De-facto standard RSA-based authentication primitives	Linux Platform & GloMoSim	Yes	• In infrastructure mode: authentication services are implemented on UAV; features low overheads & flexible management. • In case UAV fail, switch on infrastructure less mode. Security scheme is deployed to each ad hoc nodes. • Achieve seamless transmission between two communication modes.

Note: - USRP: Universal Software Radio Peripheral, DTN: Delay Tolerant Network, HDR: High Detection Rate, WPA2: Wi-Fi Protected Access-2, SSID: Service Set Identifier, TLS: Transport Layer Security, DTNs: Disruption-Tolerant Networks, UAS: Unmanned Aircraft System, WTLS: Wireless Transport Layer Security, RSA: Rivest–Shamir–Adleman.

In order to express clearly, symbols for subsequent use are listed in Table II.

TABLE II: SUMMARY OF USED NOTATIONS

Notation	**Description**
pp	Public key pair
mk	Master key
Λ	Security parameter
k	Keyspace
Keygen	Key generation
sk_f	Secret key generated
X	Plain text message
C	Ciphertext
$\{f_n\}$, $\{F_n\}$	List of functions
$\{ms_k\}$, $\{MS_k\}$	Master secret key
n, N	Encryption keys
s, S	Secret keys
c_i, C_i	Ciphertext
SND	Send
RCV	Receive

Briefly, an authority is present which has the master secret key with itself. When a description of the function *f* is given to the authority, it generates new secret keys sk_f using the master secret key. These secret keys are associated with the function *f*. Now, anyone having the secret keys sk_f can compute *f(x)* from encryption of message *x* [16]. However, [17] gave the idea about using multiple plaintexts corresponding to their ciphertext or computation of functions defined over plaintexts given their ciphertext, each encrypted under a different key. This came to be known as multi-input functional encryption.

IV. PROPOSED METHODOLOGY

The basic idea behind using the FE technique over other techniques such as Identity-based encryption (IBE) or attribute-based encryption is that in FE, there is no need to decrypt the whole message, unlike others. Information from the message can be accessed by decrypting a particular function using secret keys. Thus, if the intruder somehow accesses a secret key or the message, he will not be able to get the whole information. The overall message can be protected.

This technique is implemented in two phases within the entire proposed network architecture: the first phase is implemented between UE and MBS and the second one between MBS and UE through UAV. For implementing the FE concept, it is assumed that intruder nodes can access the messages transmitted in the network. Intruders can have full control over the network and they can intercept, analyze or even modify the messages. Moreover, the MBS is the central server that has the full list of functions and it does all the computations. Some examples of the functions (f_n), may be as per users choice, are given below:

- Counting the number of 'voice calls' transmitted over the network.
- Counting the data messages sent from UE_1 to UE_2.
- Out of incoming user traffic, separate the traffic according to text messages, data messages, etc.
- Particular which voice call has to be transmitted to another dense area like Delhi, Mumbai region etc.
- An IP address for data packets has to be noted.
- And, so on, the number of different-different functions can be defined by various users i.e. UE.

A. FE between UE and MBS:

To implement FE between the UE and MBS, the following steps are done which have been represented in an algorithm manner from equation 01 to 16. These steps are the prototype for HLPSL code.

$UE_1 \rightarrow$ MBS: SND (f_n)…… (01)
MBS: RCV (f_n)…….... (02)

Setup phase at MBS:

MBS: Input = $\{f_n\}$…….. (03)

Output = $\{ms_k\}$, $\{n\}$…….. (04)

Key generation phase at MBS:

MBS: Input = $\{ms_k\}$…….. (05)

Output = $\{s\}$…….. (06)

MBS → UE_1: SND (n)…….. (07)

UE_1: RCV (n)…….. (08)

Encryption phase at UE_1:

UE_1: $c_i = \{x\}_n$…….. (09)

UE_1 → MBS: SND (c_i)…….. (10)

MBS: RCV (c_i)…….. (11)

MBS → UE_2: SND (c_i)…….. (12)

UE_2: RCV (c_i)…….. (13)

MBS → UE_2: SND (s)…….. (14)

UE_2: RCV (s)…….. (15)

Decryption phase at UE_2:

UE_2: $x = \{c_i\}_s$…….. (16)

The implementation of these steps have been explained in detail in table III.

TABLE III. STEP BY STEP PROCESS: FE IMPLEMENTATION BETWEEN UE & MBS

Steps	Process
1.	MBS will have a list of all functions (f_n), provided by UE_1, that will be used in the network. These functions are based on specific keywords. $MBS = \{f_n\} = \{f_1, f_2 \ldots\ldots f_n\}$
2.	The setup phase will be done at MBS. The list of functions $\{f_n\}$ will be used as input and a master secret key $\{ms_k\}$ along with *n* encryption keys $\{n_1, n_2, n_3 \ldots n_n\}$ will be generated as output.
3.	The master secret key $\{ms_k\}$ will be treated as input and during key generation phase, *s* secret keys $\{s_1, s_2, s_3 \ldots\ldots s_k\}$ will be generated as an output at the MBS.
4.	*n* encryption keys $\{n_1, n_2, n_3 \ldots n_n\}$ will be sent to the all UE_1.
5.	Message *x* of the UE_1 will then be encrypted using the n^{th} encryption key. The result of the encryption will be a cipher-text c_i which will be transmitted over the network.
6.	c_i will be transferred to MBS.
7.	If UE_2 wants to access the data of UE_1, s^{th} secret key will be provided to him. By using the s^{th} secret key, the UE_2 will be able to decrypt only that portion of the *x* message for which that secret key was generated. No other data of the *x* message will be provided to UE_2.

This c_i will be secured against the intruder attacks because to decrypt the c_i the intruders will require the *s* secret keys and for this, they will require the $\{ms_k\}$ which will only be known to the MBS. Hence, the transmitted data will be secured.

The pictorial representation for the implementation of these steps between UE and MBS has been illustrated in figure 3.

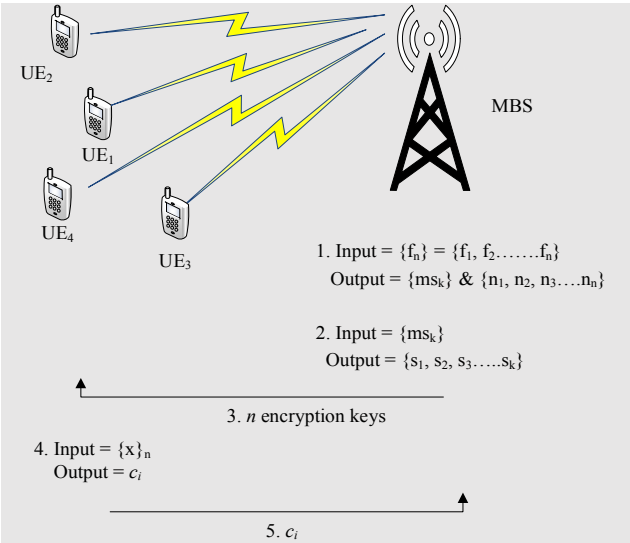

Fig 3: Pictorial representation of FE between UE & MBS.

B. FE between MBS and UE through UAV:

To implement FE between the MBS and UE through UAV, the following steps are done which have been represented in an algorithm manner from equation 17 to 36. These steps are the prototype for HLPSL code.

UE_5 → MBS: SND (F_n)…….. (17)

MBS: RCV (F_n)…….. (18)

Setup phase at MBS:

MBS: Input = $\{F_n\}$…….. (19)

Output = $\{MS_k\}$, $\{N\}$…….. (20)

Key generation phase at MBS:

MBS: Input = $\{MS_k\}$…….. (21)

Output = $\{S\}$…….. (22)

MBS → UAV: SND (N)…….. (23)

UAV: RCV (N)…….. (24)

UAV → UE_5: SND (N)…….. (25)

UE_5: RCV (N)…….. (26)

Encryption phase at UE_5:

UE_5: $C_i = \{X\}_N$…….. (27)

UE_5 → UAV: SND (C_i)…….. (28)

UAV: RCV (C_i)…….. (29)

UAV → MBS: SND (C_i)…….. (30)

MBS: RCV (C_i)…….. (31)

MBS → UE_6: SND (C_i)…….. (32)

UE_6: RCV (C_i)…….. (33)

MBS → UE_6: SND (S)…….. (34)

UE_6: RCV (S)…….. (35)

Decryption phase at UE_2:

UE_6: $X = \{C_i\}_S$…….. (36)

The implementation of these steps have been explained in detail in table IV.

TABLE IV: STEP BY STEP PROCESS: FE IMPLEMENTATION BETWEEN MBS & UE THROUGH UAV

Steps	Process
1.	MBS will have a list of functions (F_n), provided by UE_5, based on the set of specific keywords (the keywords will remain the same for both the cases). $MBS= \{F_n\} = \{F_1, F_2 \ldots\ldots F_n\}$
2.	The setup phase is done at MBS. The list of functions $\{F_n\}$ will be used as input and a master secret key $\{MS_k\}$ along with *N* encryption keys $\{N_1, N_2, N_3 \ldots N_n\}$ will be generated as output.
3.	The master secret key $\{MS_k\}$ will be treated as input and during key generation phase, *S* secret keys $\{S_1, S_2, S_3 \ldots S_k\}$ will be generated as an output at the MBS.
4.	The *N* encryption keys $\{N_1, N_2, N_3 \ldots N_n\}$ will be sent to the UAV. The UAV will transmit the N encryption keys to the UE_5 which are connected to it.
5.	The message X of the UE_5 will be encrypted using N encryption keys. The result of the encryption will be a cipher-text C_i.
6.	Now, C_i will be transmitted to UAV which will send the ciphered text to the MBS.
7.	The C_i received by the MBS then can be decrypted using the S secret keys. The secret key will decrypt only that function of the message for which it was generated.

The pictorial representation for the implementation of these steps between MBS and UE through UAV has been illustrated in figure 4.

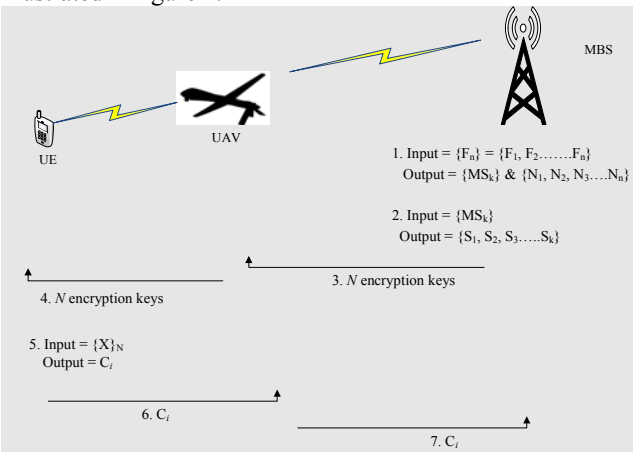

Fig 4: Pictorial representation of FE between MBS & UE through UAV.

C. Proposed Security Validations

The above implemented functional encryption technique will be validated for security proof using AVISPA tool. For the validations in the AVISPA tool, the implementation of functional encryption will be written in HLPSL language as HLPSL codes and then it will be verified. These codes will be implemented in the scenario where intruders are also present. The number of UAVs used and the area in which the UEs will be operating will be determined exactly during the implementation process of the proposed method.

V. CONCLUSION AND FUTURE WORK

A model for highly secured functional encryption technique implementation on UAV assisted HetNet for the dense urban area has been discussed and presented in this article. As UAV integrated HetNet is vulnerable to various kinds of malicious activities especially in dense urban scenarios, therefore, it is needed to create a secure network, which is fulfilled by the implementation of FE technique. The proposed model has been implemented in two phases: UE & MBS and MBS & UE through UAV. The transmission of ciphertexts using functional encryption provides security to users' critical data. Our future direction is to validate this model in the AVISPA tool. The expected outcome will be secure communication in the targeted area.

REFERENCES

[1] Cisco White Paper, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, February 2017. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[2] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, and D. Malladi, "A Survey on 3GPP Heterogeneous Networks," IEEE Wireless Communications, vol.18, no. 3, pp. 10–21, 2011.

[3] A. Khandekar, N. Bhushan, J. Tingfang, and V. Vanghi, "LTE-Advanced: Heterogeneous Networks," IEEE European Wireless Conference, Lucca, Italy, pp. 978-982, April 2010.

[4] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," 14th IEEE International Wireless Communications & Mobile Computing Conference, Limassol, Cyprus, pp. 560-565, June 2018.

[5] Bekmezci, E. Senturk, and T. Turker, "Security issues in Flying Ad-hoc Networks (FANETs)," Journal of Aeronautics and Space Technologies, vol. 9, no. 2, pp. 13-21, July 2016.

[6] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, "A data authentication scheme for UAV ad hoc network communication," The Journal of Supercomputing, Springer, pp. 1-16, 2017. https://doi.org/10.1007/s11227-017-2179-3

[7] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion Detection and Ejection Framework against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 5, pp. 1143–1153, 2017. doi:10.1109/tits.2016.2600370.

[8] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security against Lethal Cyber-Attacks in UAV Networks," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1594–1606, 2018.

[9] D. He, S. Chan, and M. Guizani, "Communication Security of Unmanned Aerial Vehicles," IEEE Wireless Communications, vol. 24, no. 4, pp. 134–139, 2017.

[10] H. Sedjelmaci, S. M. Senouci, and M. A. Messous, "How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?," IEEE Global Communications Conference, Washington, DC, USA, pp. 1-6, December 2016. doi:10.1109/GLOCOM.2016.7841878.

[11] R. Mitchell, and I.-R. Chen, "Specification-based intrusion detection for unmanned aircraft systems," ACM MobiHoc Workshop on Airborne Networks and Communications – Airborne, pp. 31-35, 2012. doi:10.1145/2248326.2248334.

[12] L. Zhu, and Z. Zhan, "A Random Key Management Scheme for Heterogeneous Wireless Sensor Network," IEEE International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, Shanghai, China, pp. 1-5, August 2015. doi:10.1109/ssic.2015.7245677

[13] D. Sharma and D. Jinwala, "Functional Encryption in IoT E-Healthcare System," 11th International Conference on Information System Security, Springer International Publishing, vol. 9478, pp. 345-363, December 2015.

[14] J. Kong, et al., "Adaptive security for multilevel ad hoc networks," Wireless Communications and Mobile Computing, vol. 2, no. 5, pp. 533–547, 2002.

[15] D. Boneh, A. Sahai, and B. Waters, "Functional Encryption: Definitions and Challenges," Lecture Notes in Computer Science, Theory of Cryptography, Lecture Notes in Computer Science, vol 6597. Springer, Berlin, Heidelberg, pp 253-273, 2011.

[16] D. Boneh, A. Sahai, and B. Waters, "Functional encryption," Communications of the ACM, vol. 55, no. 11, pp. 56-64, November 2012. doi: 10.1145/2366316.2366333.

[17] S. Goldwasser, S.D. Gordon, V. Goyal, A. Jain, J. Katz, F.-H. Liu, A. Sahai, E. Shi, and H.-S. Zhou, "Multi-Input Functional Encryption", Advances in Cryptology- EUROCRYPT 2014, vol. 8441, pp. 578-602, Springer, Berlin, Heidelberg, 2014.