Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 27 No. 3 (2024)

Lightweight Cryptography using Pairwise key generation and malicious node detection in large UAV

Reshma C Sonawane[1], A. Muthukrishnan[2]

[1]Phd Scholar : at Veltech Rangarajan Dr. Sanguthala R&D Institute of Science and Technology Chennai[1]

reshmagold@gmail.com[1]

[2]Associate Professor: at Veltech Rangarajan Dr. Sanguthala R&D Institute of Science and Technology Chennai[2]

drmuthukrishnana@veltech.edu.in[2]

Article History:

Received: *07-03-2024*

Revised: *30-04-2024*

Accepted: *27-05-2024*

Abstract

Data security is very essential concern in network data transmission between various sensor nodes. Data encryption is the only way to provide security to sensitive information during the transmission. Various researchers have developed the different encryption techniques with heterogeneous encryption and decryption keys. Nevertheless, the standard does not include guidance for the administration, storage, or distribution of encryption keys. Various researchers proposed key management techniques, but those methods still generate high overhead during data communication. To eliminate such problems, we suggest lightweight key encryption using pairwise cryptography and malicious node detection from large UAVs. The proposed encryption algorithm compresses the cypher data, reducing the network overhead, and detecting malicious nodes provides higher security from internal and external intruders. In extensive experimental analysis, our simulation obtains better results than existing systems. That enhances around 7-9% throughput with other QoS parameters.

Keywords: Unmanned Aerial Vehicles, intrusion detection system, energy consumption and conservation, broadcast tree construction, lightweight key encryption, pairwise key generation.

1. Introduction

Data security and misbehaviour node detection is very important in Unmanned Aerial Vehicles (UAV). The sink receives either the raw data or the data that has been aggregated from the sensor nodes. The sink is able to command the network to assign jobs to the sensors and makes judgments based on the combined data. These decisions are based on the combined data. Wireless sensor nodes have additional vulnerabilities on top of the multiple fundamental security issues they already have. This is due to the fact that they are often installed in areas that are not overseen and rely on substandard radio connectivity. End users may get erroneous sensing data as a result of several attacks, which can be damaging in contexts such as war monitoring and environmental monitoring. To ensure that systems are protected in an appropriate manner, appropriate security measures need to be implemented.

The paired key encryption and watchdog system that has been presented is designed to automatically recognise hostile nodes and shut them down before the system is hacked while it is moving data. The system may also be capable of enabling secure communication while detecting many forms of network attacks, including active attack, network attack, denial of service attack, MiM attack, jammer attack, and passive attack. Internal nodes use the least amount of energy, which results in the network's lifespan being extended and the quality-of-service metrics being improved more efficiently. The building approach known as broadcast tree reduces any network and packet overhead that may be present on the internal nodes by making use of the fewest resources feasible. The system is equipped with three essential features, namely intrusion detection systems, intrusion prevention systems, and intrusion responding systems, which block malevolent nodes from talking with other network nodes for a certain amount of time after an intrusion has occurred. The rest of the paper describes section 2 defines a literature survey which contains a study of various existing researchers. Section 3 demonstrates a proposed system model with algorithm details. Section 4 provides results and discussion with a conclusion describes in section 5.

2. Literature Review

In 2020, Pallavi Joshi et al. [1] describes an UAV security that describes a over the past ten years, UAVs have been widely used for a variety of purposes, giving rise to route-discovering techniques, often known as routing protocols. Discovering the optimum path is a fundamental requirement for any sensor network because SNs are energy-constrained. This paper discusses the application of various routing protocols, mostly responsive and composite. The protocols have been contrasted in regards to energy usage in transmission and receiving modes for multiple situations and duty cycles. According to analysis, reactive protocols such as Dynamic Source as well as Dynamic MANET on Demand Routing function best than composite protocols such as Zone Routing Protocol when used in sensor systems with higher duty cycles.

A constantly changing, self-configuring UAV with SNs frequently placed in challenging environments was described by Deepali S. Patil et al. in 2017 [2]. Sensor networks are vulnerable to a number of assaults, including Sybil, DOS, Eavesdropping and others because of their uncontrolled nature & lack of equipment that is tamper-resistant. Among the most terrifying attacks is a node clone assault, in which the intruder seizes a node, steals its confidential data, duplicates it, and inserts it into the network area to carry out more harmful behavior. Different detection strategies depending on fixed and movable UAVs have been developed to identify and counteract such attacks. For the purpose of identifying node clone attacks in wireless networks, a novel node's position velocity time dependent detection method has been suggested in this research. This technique increases network performance while lowering communication costs and routing overhead across the board.

In 2019, Manish M. Patel, D.O., and others [3] Nowadays, UAVs are quite common because of their many uses in the defense, environmental monitoring, and healthcare industries. Applications for commercial and warfare monitoring employ these systems as well. With regard to UAVs, protection is very important. Sensor networks are vulnerable to numerous assaults, including wormhole, sinkhole, Sybil, jammer, and selective forwarding. This suggested strategy is focused on determining trust value. The monitoring node constantly determines the trust level. Every node whose trust value falls underneath the threshold is labeled as hostile.

Several uses in UAVs are, to a large extent, governed by network security, according to Tao Liu et al. in 2011 [4]. But since encryption innovation is ineffective at stopping assaults from internal foes or incorrect service from nodes, it is impossible for encryption technology that is solely focused on encryption to address the emerging malign activities. On the basis of a reputation concept, a pair-wise key updating strategy for Unmanned Aerial Vehicless is suggested. The method has successfully implemented the functions such as pair-wise key generation, revoke, and formation when a noval node enters depending on trust level. The distribution is used to characterize the reputational distribution of the SNs, and it is suggested that this distribution's statistical assumption be used to communicate the nodes' level of trust. In addition to repelling assaults from outside nodes, they also stop inside node assaults or suspicious attack. The system is scalable and supports dispersed key establishment, update across nodes as well as flexible key management.

According to Mochamad Teguh Kurniawan et al. [5], Unmanned Aerial Vehicles (UAV) will play a significant role in 2020 in a number of industries, including the military, healthcare, and even information technology like Internet of Things. Due to the receptors' limits in terms of storage, cpu, and power, UAV has a drawback in its usage if there is no built-in security mechanism contained in the sensing element. Unmanned Aerial Vehicles is hence susceptible to attacks; the Denail of service attack is one of the most common ones. By limiting available resources till the network resources are congested, the network gets slow, and finally goes off, Denial of service attacks try to stop authorized users from consuming resources. Therefore, in order to prevent Assaults, it is necessary to identify and mitigate them. In this work, a signature-based IDS is used identify and mitigate DoS assaults by applying a blocking strategy on the attack node and preventing all packets coming from the adversary until the intruder runs out of energy. When intrusion detection system discovered a denial of service attack, the blocking strategy was effectively implemented on the Unmanned Aerial Vehicles. By preventing all packets coming from the attacker, the blocking technique can be utilized to mitigate attack such as [6].

Sensor Networks (UAVs) have become a fascinating research field in recent years, according to V. Vijayalakshmi et al. in 2008 [7]. Uses for these networks call for the cooperative execution of a distributed job by a significant number of sensor nodes. By message passing that are time-stamped using the native clocks on the nodes, cooperative processing is made possible. Time synchronization is therefore crucial in these distributed systems. For many years, technologies like Network Time Protocol (NTP) have perfectly synchronized the clocks of networked systems. UAVs, on the other hand, have a high node density and a finite amount of energy at each node, which increases scaling needs while constricting the resources. In order for each node to be able to withstand partially absent or inaccurate synchronization data supplied by malicious node, this study describes a method called level-based time synchronization. It offers redundant means for every node to sync its clock with the share source. Simulated tests are used to determine the effectiveness of this method.

Fengyun Li et al. [8] How to identify rogue nodes in UAVs and stop them from assaulting trustworthy nodes has emerged as one of the most crucial problems. The sensor nodes cooperate with one another to fend off denial of service attacks and safeguard the assaulted nodes in this article's novel approach. Also suggested is an incentive scheme for cooperation depending on reputation. The suggested

technique can boost the likelihood of success in keeping rogue nodes from assaulting the legitimate nodes in UAVs and has a low false alert rate, according to simulated data.

Chungen Xu et al. [9] Unmanned Aerial Vehicless are becoming more prevalent in our daily lives. The research only proposes a few symmetric encryption-based methods, assuming that sensor nodes cannot support public key encryption owing to energy and central processing unit power limitations. This shows that security in Unmanned Aerial Vehicles has not been carefully considered. In this article, a Public Key Infrastructure (PKI) plan for UAVs is presented. The proposal makes use of RSA's version of public key encryption to enhance security on UAVs and attempts to address the issue of security in Unmanned Aerial Vehicles by using public key encryption as a method for guaranteeing the validity of the base station.

In 2019, Rohini et al. [10] Compromise of nodes and DOS are two major assaults in UAVs. The data transmission methods that can most likely avoid the black holes created by these attacks are discussed in this thesis. The primary reason why the traditional multipath routing strategies are susceptible to such attacks is that they are predictable. The data shared via these routes is therefore vulnerable to attack once the attacker obtains the routing mechanism since it can calculate the same routes as those known to the source. A system is created to produce randomly chosen multipath routes. The "shares" of various packets follow distinct routes under this arrangement, which changes over time. All packets are encrypted before being sent, and it is then decoded once it has all been received. Therefore, even if the adversary learns the routing scheme, they still are unable to determine the exact pathways that every packet takes. The created paths are quite capable of ignoring black holes because they are highly dispersive, energy-efficient, and unpredictable.

K. Karthigadevi et al. [1] one of the damaging attacks on Unmanned Aerial Vehicless is the sinkhole attack. The sink node serves as a base station, absorbs all network data, and lowers the performance and scalability of the sinkhole attacking nodes. When a sinkhole assault hits a node, a lot of research is being done in Unmanned Aerial Vehicless to mitigate the damage. To identify and stop the sinkhole attack, a unique decentralized network density estimation technique-based sinkhole recognition mechanism was proposed. Every node in a network keeps a neighbor table to record information about its neighbors, and every node uses this neighbor table to perform the Network Density Estimation Method. Every node in a network records information about its neighbors. By utilizing all of these techniques for network density estimation, one may determine the network density and determine whether any malicious nodes are present in the area. The adjacent nodes are informed of the detected compromised nodes so that they can ignore them during subsequent broadcasts. The overhead of gathering snapshots and routes is decreased by this technique. By boosting the volume of Best Effort traffic, this technique boosts throughput of the network.

In 2019, Anurag Yadav et al. [12] in the world of today, everything is becoming wifi. Through this wireless network, the data are also transmitted. However, as we are all aware, technology is not without its dangers. So with wireless technology it also has a thread of someone can interfere with the connection, listen to the conversation or harm the network. Attackers and uncivilized individuals are constantly trying to harm society, thus to combat this issue, System has IDPS, or an ID and IPS. Wireless communication is made secure for us by IDPS, which aids others in preventing interception of the network. The goal of this study is to make wireless communication systems more secure so that

third parties cannot intrude while messages are being transmitted and that, in the event that they do, third parties are immediately alerted, allowing for immediate intervention to stop the intrusion.

In 2019, Nazli Siasi et al. [13] the efficiency and longevity of a UAV can be negatively impacted by hostile security attacks on the routing protocols. This is more crucial in cluster routing protocols like the low energy adaptive clustering hierarchy (LEACH) protocol, which consists of numerous nodes and a cluster head. Particularly, the entire collection of nodes fails if an attack is successful in taking out the cluster head. In order to defeat security threats and quickly recover packets, it is imperative to build reliable recovery techniques. So, utilizing the LEACH protocol, this research suggests a detection and recovery technique for selective forwarding assaults in UAVs. With no need for input or re - transmission after an assault, the suggested method offers near instant recovery times.

Konstantinos Skoufas et al. [14] predict that in 2020. For the scientific community, security of UAVs and internet of things devices is a serious concern. These systems are susceptible to hostile hardware and software due to the abundance of wireless assaults. Because of their low power and poor processing power, internet of things equipment is frequently an accessible target for assaults. Several security measures to thwart assaults have recently been developed as a result of study. The Distributed Denial of Service attack is a well-known one. A network is overburdened during this assault, which causes it to perform badly or not at all. This study examines the packet delivery ratio in order to identify such an assault. It is suggested that a rate monitoring technique be used to identify connected nodes that are engaging in malicious behaviour by looking at the speeds of the incoming traffic from those nodes and blacklisting them. In a wireless road network, automobiles receive data from wireless stations located on traffic signals in order to carry out a task. This method is used to assess a road network that allows for the tracking of specific metrics.

3. Prposped System Implementation

3.1 : Lightweight encryption method: In the first phase we proposed an lightweight encryption method using pairwise key generation approach. Initially source node S_N select the destination node D_N. The each D_N having own identity such as ip address or MAC address. So, S_N usage the encryption as D_N identity for data encryption and forward it to destination node. The source node message generation is defined in below equation;

$$M \leftarrow \text{encrypt (msg, } D_N)$$

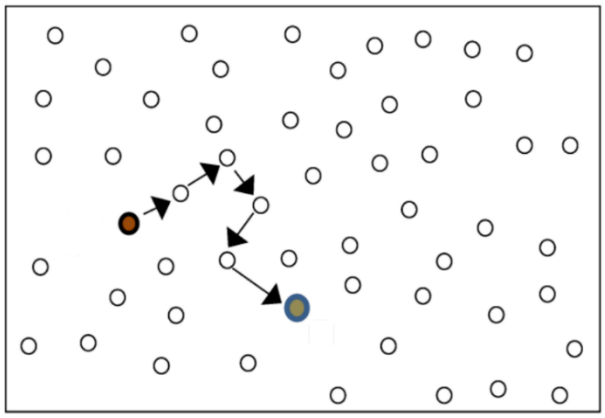

Figure 1 : proposed system model for lightweight data encryption between source to destination

The major advantage of this method, only D_N can descripty of cipher data by using own identity otherwise remaining nodes are not able to decrypt received encrypted data due to incorrect keys. The description process done by destination node is describes as below

$$\text{Msg} \leftarrow \text{decrypt (M, } D_{id})$$

The M is the cipher text, D_{id} is the destination nodes and Msg is the recovered plain text data. This method gives assurance of no data leakage and data loss issues.

3.2 : Attack detection model :

The watchdog technique is a mechanism that depends on broadcast capabilities and may be used in UAVs to discover rogue nodes in the network. A node, such as node A, that has the aim of transferring the data to another node, such as node C, may listen in on the sent traffic of another node, node B, and determine whether or not the other node, node B, will transport the data to the node C, as shown in Figure 2.

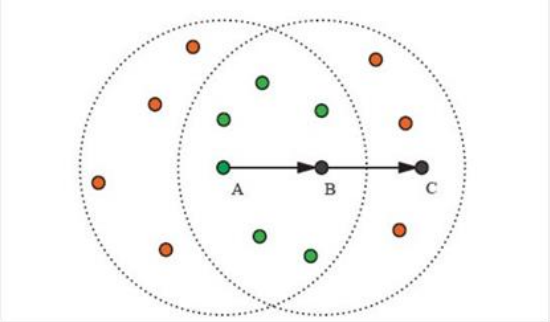

Figure 2 : proposed system model for malicious node detection in UAV

The above Figure 2 demonstrates a detection of malicious nodes between source and sink nodes. We make an effort to provide an unique approach that is based on the Watchdog methodology but is altered to improve the security of UAVs. Improved Watchdog is the name given to this approach. In contrast to the basic technique, which considers node A to be the watchdog and assumes that the cluster heads were the first layer watchdogs, the I-Watchdog approach presupposes that the cluster heads were the first layer watchdogs, as shown in figure 5.2.

4. Results And Discussions

In this section, we give an evaluation of both the existing and proposed systems. After describing the experimental setup and the many factors we used, including throughput, delivery ratio of packet, expense, and duration, we qUAVtitatively evaluate the research. Our testing is conducted using the NS2 Simulation tool, version 2.35, which has been shown to produce accurate findings. The header input employs both TCL and C++ programming, but the NS simulation just executes TCL code. We use a network design that is built on infrastructure for interaction in our simulations. The wireless connection is always accessible due to the network selection. WMN simulates in NS2. The entire design that was proposed is simulated in the TCL code. The EvalVid Framework is used by TCL to run in the NS2 simulator, and it also aids in recording running connection data messages that use the connection pattern file us1. The trace file for NS2 .tr can be used to evaluate the results. Vector as well as scalar data analysis, filtration, and presentation are all enabled. The us.tr file, which offers the

simulation's overall performance, may be found in the project folder's outcomes folder. We illustrate the outcome variables against the x axis and y axis parameters depending on the us.tr file using the graphical tool. The graph software can depict the graph files, which have awk extensions describes an Table 1.

Table 1 Parameters and values

Parameters	Values
Simulator	NS-allinone 2.35
Simulation duration	25 secs
Type of Channel type	Wireless
Propagation system	2 Ray Ground
Standard	MAC/802.11
Simulation dimension	1000 * 1500
Maximum packet size	1000
Adhoc routing	DSDV, AODV, DSR, SAODV
Traffic	PBR, CBR

The proposed system evaluates both the desired and current systems in this section. It statistically analyses the study after outlining our experimental design and the various elements involved, such as throughput, packet delivery ratio, cost, and time. Filtering, processing, and presenting vector and scalar data may be done in a number of ways. The us. tr file, located in the project folder's results directory, includes the simulation's performance statistics. Using the graph tool, we present the result parameters against the x-axis and y parameters based on the us.tr file. The graph programme can plot graph files with the awk extension.

Table 3: Packet end to end delay

Time	**Random key[15]**	**Pairwise key [16]**	**ECCDH[17]**	**Proposed**
5	1.30	2.10	1.30	1.01
10	1.90	2.35	1.40	0.95
15	1.85	2.30	1.20	0.85
20	2.10	3.0	1.10	0.98

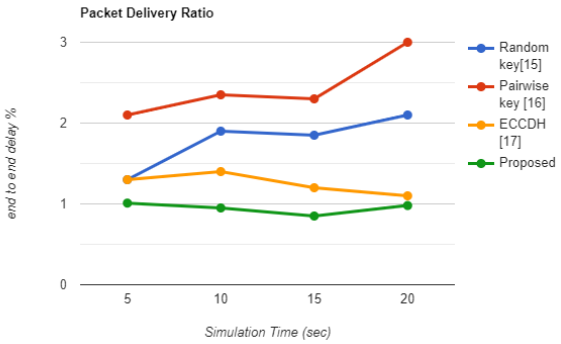

Figure 4: Packet end to end delay

The above graph describes a proposed system that reduces the end-to-end packet delay in all experiments with 5, 10, 15, and 20 sec. We have calculated the delay for specific time intervals and the entire simulation. The delay demonstrates in seconds how more is required for particular data packets sent. It reduces an average of 15% time than Random key generation [15], Pairwise key generation [16], and ECCDH [17], respectively.

Table 4: Packet delivery ratio

Time	Random key[15]	Pairwise key [16]	ECCDH[17]	Proposed
5	89.6	92.6	93.1	96.2
10	90.3	91.3	93	96
15	90.5	91.9	93.5	95
20	90.05	92	93.45	95.4

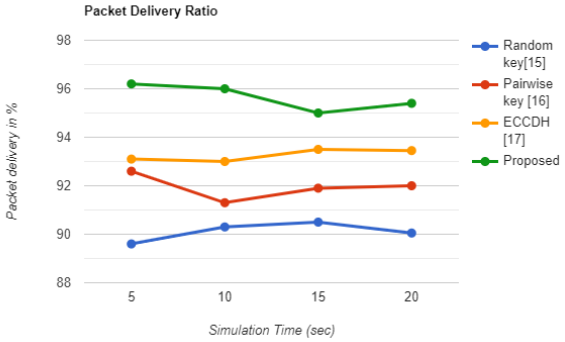

Figure 4: Packet delivery ratio

The above graph describes a proposed system packet delivery ratio for 5, 10, 15, and 20 sec. The number of packets sent by sends sender and no. of successfully received by receiver's node. The proposed system obtains around a 4% average higher successful packet delivery rate than Random key generation [15], Pairwise key generation [16], and ECCDH [17], respectively.

Table 5: throughput of proposed model

Time	Random key[15]	Pairwise key [16]	ECCDH[17]	Proposed
5	0.82	0.84	0.77	0.89
10	0.91	0.76	0.76	0.91
15	0.86	0.81	0.81	0.92
20	0.87	0.78	0.82	0.92

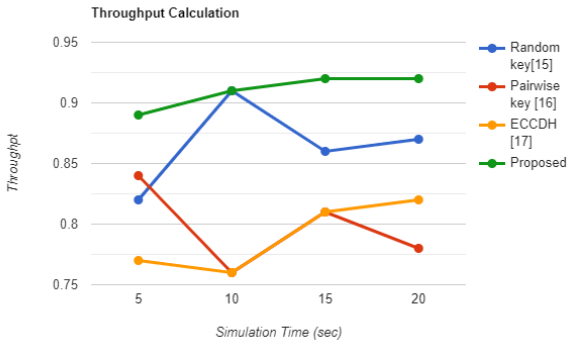

Figure 5: throughput of proposed model

The throughput has been calculated based on bit per second successfully sent for TCP packets. When the connection between the source and the sink node is established, it transfers the real text data; those packets are considered TCP packets. The BTC algorithm enhances the throughput and reduces the packet and network overhead. t also reduces internal data attacks such as buffer overflow. The proposed model provides 7-9% higher throughput than the three existing systems.

Table 6: energy consumption by each vehicle node with simulation time

Time	**Random key[15]**	**Pairwise key [16]**	**ECCDH[17]**	**Proposed**
5	560	653	754	420
10	760	843	799	560
15	1120	1320	1760	755
20	1393	1570	1985	956

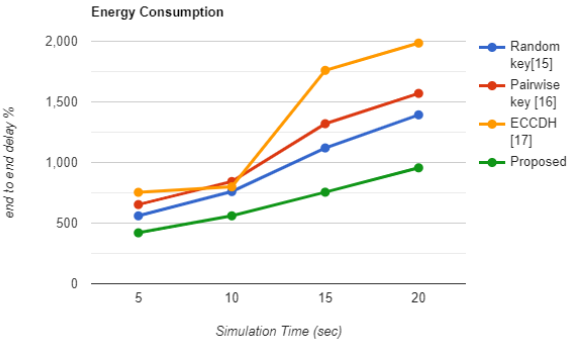

Figure 6: energy consumption by each vehicle node with simulation time (jules)

The above figure demonstrates energy consumption by induvial nodes during the combination. The energy consumption has been calculated in Jules, which is dynamically allocated between 100-3000 Jules to each node. The proposed models only affect internal node communication, which avoids the energy holes of sleep nodes. The proposed model also enhances the network lifetime by using our energy conservation protocol.

5. Conclusion

The work presented in paper focuses on lightweight data encryption and malicious node detection in large UAV. The malicious nodes occurring in sensors are modelled with respect to UAV model. To distinguish between a fault and malicious nodes, proper modelling of an event or phenomenon is required in addition to an algorithm to detect malicious nodes. Without such a model for events it is impossible to determine whether anomalous behaviour is a fault or an event without human intervention. The key distribution phase of the proposed protocol uses modular exponentiation as its primary method of computation. As a result of the method's linear complexity, the running time of an ordinary modular exponentiation is exponential with the size of the exponent e. Because of this, the approach cannot be used in a real setting. We used the square-and-multiply technique in order to make the proposed protocol usable on nodes with limited resources. The system focusses on pairwise key generation and attack detection in large UAV. The experimental analysis describes our model provides around 5-7% throughput as well as reduces the packet loss and packet drop etc. The future outlook is to investigate appropriate algorithms for detection and isolation of malicious nodes.

References

[1] Pallavi Joshi, Ghanshyam Singh and Ajay Singh Raghuvanshi. “Impact of Duty Cycle and Different Routing Protocols on the Energy Consumption of a Unmanned Aerial Vehicles”, 2020, International Conference on Communication and Signal Processing, IEEE.

[2] Deepali S. Patil and Shailaja C. Patil. “A Novel Algorithm for Detecting Node Clone Attack in Unmanned Aerial Vehicless”, 2017, IEEE.

[3] Dr. Manish M Patel and Prof. Priyanka K Patel. “Intrusion Detection System Based on Trust Value in Unmanned Aerial Vehicless”, 2019, Third International Conference on Electronics Communication and Aerospace Technology [ICECA], IEEE.

[4] Tao Liu, De-Jun Chen and Ming-Zheng Zhou. “Pair-wise Key Update in Unmanned Aerial Vehicless Based on Reputation Model”, 2011, IEEE.

[5] Mochamad Teguh Kurniawan and Setiadi Yazid. “Mitigation and Detection Strategy of DoS Attack on Unmanned Aerial Vehicles Using Blocking Approach and Intrusion Detection System”, 2020, 2nd International Conference on Electrical, Communication and Computer Engineering (ICECCE), IEEE.

[6] Ramu Kuchipudi, Dr. Ahmed Abdul Moiz Qyser and Dr. V .V. S. S. S Balaram. “An Efficient Hybrid Dynamic Key Distribution in Unmanned Aerial Vehicless with reduced memory overhead”, 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), IEEE.

[7] V. Vijayalakshmi, Dr. T.G.Palanivelu and N.Agalya. “Secure Time Synchronization against Malicious Attacks for Unmanned Aerial Vehicless”, 2008, First International Conference on Emerging Trends in Engineering and Technology, IEEE.

[8] Fengyun Li, Guiran Chang, Fuxiang Gao and Lan Yao. “A Novel Cooperation Mechanism to Enforce Security in Unmanned Aerial Vehicless”, 2011, Fifth International Conference on Genetic and Evolutionary Computing, IEEE.

[9] Chungen Xu and Yanhong Ge. “The Public Key Encryption to Improve the Security on Unmanned Aerial Vehicless”, 2009, Second International Conference on Information and Computing Science, IEEE.

[10] G.Rohini. “Dynamic Router Selection and Encryption for Data Secure in Unmanned Aerial Vehicless”, 2019, IEEE.

[11] K. Karthigadevi, S. Balamurali and M.Venkatesulu. “Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to Detect and Prevent the Sinkhole Attack in Unmanned Aerial Vehicles”, 2019, IEEE.

[12] Anurag Yadav, Himanshu Gupta and Sunil Kumar Khatri. “A Security Model for Intrusion Detection and Prevention over Wireless Network”, 2019, 4th International Conference on Information Systems and Computer Networks (ISCON), IEEE.

[13] Nazli Siasi, Adel Aldalbahi and Mohammed A. Jasim. “Reliable Transmission Scheme against Security Attacks in Unmanned Aerial Vehicless”, 2019, IEEE.

[14] Konstantinos Skoufas, Evangelos D. Spyrou and Dimitris Mitrakos. “Identifying DDoS Attacks from Fluctuations in Wireless Traffic in an Intelligent IoT Road Network”, 2020, IEEE.

[15] Wang, E.K., Hui, L.C.K. Yiu, S.M.: A new key establishment scheme for Unmanned Aerial Vehicless. IJNSA 1(2), 17–27 (2009)

[16] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In2003 Symposium on Security and Privacy, 2003. 2003 May 11 (pp. 197-213). IEEE.

[17] Iqbal S, Prerana S, Sukrutha H, PurushottamShanbhag G. Attack Resistant Secure Key Management in Unmanned Aerial Vehicless. In2019 1st International Conference on Advances in Information Technology (ICAIT) 2019 Jul 25 (pp. 475-479). IEEE.