




A New Cyber Security Framework Towards Secure Data Communication for Unmanned Aerial Vehicle (UAV)

Md Samsul Haque^(✉)  and Morshed U. Chowdhury

School of Information Technology, Deakin University-Burwood Campus, Melbourne, Australia
{mshaq,morshed.chowdhury}@deakin.edu.au

Abstract. Cyber Physical Systems (CPS) like UAVs are used for mission critical tasks including military and civilian operations. Their potentiality of usage is rapidly increasing in commercial space. The need for a secure channel to wirelessly communicate and transfer message between CPS is very crucial. Key idea behind this study is to propose a novel framework that is lightweight, robust and at the same time do not compromise security and pragmatic in the jurisdictions of energy-efficient atmospheres. This paper presents an idea for a practical and efficient hierarchical architecture for UAV network using identity-based encryption. Also, proposes selective encryption technique to reduce overheads and data hiding mechanism to increase confidentiality of the message.

Keywords: Identity-based cryptography · Watermarking · Cyber security
Unmanned aerial vehicle

1 Introduction

The need for cyber security has grown with the growth and expansion of digital tools and technology. The devices we use in our everyday life are now becoming smart and connected to a global network of computers, software systems and communication links called Internet of Things (IoT). Thus, ensuring security of digital data has become a critical challenge. Traditional computer and network security approaches fails to adequately address integrity, confidentiality and availability threats for cyber physical system (CPS) and do not address a unified manner for survivability from malicious intimidations and recoverability from attacks [1]. Recent years, research has explored towards vulnerability of CPS, particularly for Unmanned Aerial Vehicle and ground control systems, but little research has been done in secure trust creation, communication and message transfer. In this paper, we surveyed the available literature and defined a secure framework to enhance security to cyber physical system communication for UAV network. The rest of this paper is organized as follows: Sect. 2 describes background information, and security threat to UAV, Sect. 3 reviews the existing literature, Sect. 4 proposes a solution for the problem, Sect. 5 briefly analyses the performance and security for the proposed framework and finally Sect. 6 concludes and discusses future work.

2 Background

Cyber physical systems (CPS) are autonomous systems which are the convergence of communication, computing and control systems [2]. There are several uses of CPS, which includes smart grid system, oil and gas distribution networks, advanced communication systems, UAV and smart ground vehicles. UAVs are cyber physical systems that can be controlled remotely from a ground control station or can fly autonomously using on-board computers based on pre-programmed flight plans. They are also intelligent system, able to communicate with its controller and return payload data, capable of automatically take corrective action or automatic decision making during an event [3]. The main elements of an UAV are control elements, wireless and satellite communication link, sensors and actuators. UAVs are resource constraint device. They use batteries for power, however Top Flight Technologies [4] has designed a hybrid gas-electric aircraft that uses both batteries and gasoline, significantly improving its performance.

UAVs were mainly used in defense operational environment but nowadays, they are ubiquitous and their uses are rapidly expanding in commercial, scientific, recreational and other applications. They are used as a major tool [5] for law enforcement agencies, shippers, aerial photographers, farmers, humanitarian agencies, and more. Giant companies such as Amazon, Google are planning to use UAVs for goods and services delivery [6]. The FAA forecast [7] estimates that by 2020 there will be 7 million of unmanned aerial vehicle occupying United States airspace.

With the increase in UAV usage potential risks and security threats also starts to arise. UAVs are potentially easier to hack as because they are designed to have a quick and easy setup and often uses unencrypted communication and data transfer with many ports are still open. Moreover, the unique configuration such as open state of the sensors, wireless network, serially safety structure, etc. makes these devices highly exposed technical systems. In recent years, research has explored cyber security threats to the UAV that are used for defense industry, but little research has been done to explore what additional cyber threats are for the use of commercially available UAVs. Also, much of the security technology and processes are currently being developed without doing a proper threat analysis. Because of utilizing unsecure devices [8] could result in unauthorized disclosure of classified information.

2.1 Cyber Security Threats on UAV

Threats on CPS goes beyond attacking the individual system components. By using a multi-vector attack a skilled attacker exploits the weaknesses of individual components and the combined effect however, may be catastrophic. Security threats on UAV can be on the onboard flight controller and ground control system, sensor, actuator, wireless data link and routing infrastructure. Determining the nature of the vulnerability the attacks can be categorized into three groups: hardware, wireless and sensor spoofing attack [9]. Hardware attack is where attacker has access to the UAV autopilot components directly. In wireless attack the attacks are carried out through one of the wireless communication channels and sensor spoofing attack, is carried out by injecting or passing false data by the miscreant through the on-board GPS channels. In this paper

our focus is on the wireless attack to secure wireless data communication channels. An attacker can carry out such attacks from a far distance while the UAV is being operated. The most significant threat of wireless attacks is the fact that an attacker can gain full control of the UAV if the communication protocol is known, and can break the encryption of the communication channel. Successful attack requires breach of at least one of the information security objectives: confidentiality, integrity or availability [10].

Example, of an attack to UAV is deliberately jamming communication link while filming of an Australian triathlon with an UAV. The operator lost complete control over the vehicle, believes that an attacker using a “channel hop” attack intentionally interfered with his operation, causing it to crash into one of the athletes [11]. Another most recent and controversial incidents was that the Iranian forces claimed possession of an RQ 170 Sentinel. One of the theory described that Iranian forces jammed the satellite communication of the UAV and GPS functionality which make it easy to attack the GPS system by sensor spoofing attack [12].

3 Related Literature

Research in communication security is a continuous process. The complex nature in UAV has driven to the domain of new security research. Much of the research has been accomplished on capability, reliability and efficiency of the system in terms of time and power [13].

A hierarchical architecture for wireless sensor network (WSN) based on the Boneh-Franklin algorithm proposed in paper [14]. The author presents a hierarchical key management scheme based on the basic Boneh-Franklin and Diffie-Hellman (DH) algorithms to solve large energy consumption in communication and computation. Identity based hierarchical Key Management Scheme in Tactical Mobile Ad Hoc Networks proposed in paper [15]. Authors offered a technique of key management in distributed hierarchal network. The nodes of hierarchy can get their keys updated either from a threshold sibling or from their parents. The technique of dynamic node selection formulated as a stochastic problem and the proposed scheme can select the best nodes to be used considering their security conditions and energy states.

Cryptography and Steganography are used with enhanced security module in paper [16]. Authors used symmetric encryption algorithm called Advanced Encryption Standard (AES) and image based steganography. A part of the encrypted message is hidden into an image and the unhidden part of the encrypted message will be converted into two secret keys. To decrypt the message one need keys for Cryptography and Steganography, two extra keys and the reverse process of the key generation. The limitations of this paper are that the length of the input and output sequences for the Advanced Encryption Standard (AES) and the proposed framework is a flat network where all users has similar access to data. Paper [17], proposes an approach for securing transmitted message over communication network. It uses symmetric encryption algorithm AES and text based steganography to provide an extra layer of security. The AES provides the initial confidentiality of the secret data and then the encrypted data are represented in binary and then hidden is textual carrier. The AES encryption algorithm uses 256 bits’

key for extra security against brute force attacks. This paper is also lack of providing forward and backward security as it is designed for a flat network system.

The security approach described in paper [18, 19] presents a solution for an agent-based model for cyber physical systems by using hierarchical access. Hierarchy is implemented through a public key cryptosystem with divided private key and steganography. The steganalysis and cryptanalysis provides a higher level of security to the original data. Although the proposed approach brings a new perspective for the security of agent-based cyber-physical systems but it lacks implementing the approach to any specific application domain. Different security threats for UAVs System are analyzed and a cyber-security threat model has been proposed in Paper [10] The proposed model help designers and users of the UAV systems to understand cyber-security threat profile of the system and address various system vulnerabilities, identify high priority threats, and select mitigation techniques for these threats. They have also tried to evaluate risk generation by different vulnerabilities to the UAVs system. Although various security threats to a UAV system is analyzed and a cyber-security threat model showing possible attack paths has been proposed on this paper but it is not clear which threats might affect the UAV systems most.

Traditional information security mechanism such as cryptography, intrusion detection method or steganography alone is not sufficient to protect UAV system. More specifically these techniques do not consider the compatibility of the sensor, actuator, communication link measurements of the physical and control mechanisms of UAV, which has a massive importance for the security of cyber physical systems like UAV. Also, typical communication security mechanisms often increase communication latency to unacceptable levels, specifically for real-time systems. UAVs are complex by nature and need to have embedded security functionalities and the security solutions. Because complex infrastructures have different objectives and assumptions concerning what needs to be protected, and have specific applications that are not originally designed for a general IT environment. Therefore, it is necessary to develop unique security solutions for different application and infrastructures to fill the gap.

4 Proposed Solution

Security research for CPS varies depending on the application domain of the system. UAVs are typically resource constrained in terms of computation, communication, energy and storage. So, the Security solutions for UAV data communication must be robust, efficient, and satisfy the real-time requirements. At the same time, it must be lightweight without affecting performance. In this paper, we are proposing a framework to achieve a collective system lightweightness, that does not compromise security and efficiency of the system. We are partly inspired by the concept presented in the research work in paper [20] that proposed the lightweight security enforcement in Cyber-Physical Systems. Our contributions to the knowledge are as follows:

- **Distribution of Computing Overheads:** Our proposed structure provides lightweightness and security by offloading computationally expensive workloads from resource constrained devices to powerful equipment. Leveraging the architecture of the

underlying system and constructing a multilevel structure we can achieve such a framework.

- **System Lightweightness:** To achieve system lightweightness we are proposing to use a lightweight cryptographic primitive and using selective data encryption technique to attain better system performance and increase efficiency in message transfer without hampering security.
- **Obscuring transmitted data and digital data right management:** Stenography or data watermarking technique increase the confidentiality during data transfer and integrity of the stored data.

The motivation of the proposed framework is to provide balance between UAVs regarding resource consumption and security by creating a robust and new security architecture.

4.1 Distribution of Computing Overheads

Flying Ad-Hoc Network (FANET), is a new form of network family that can perform their task without human intervention which can complete their job without human intervention [21]. In FANET, the UAVs become node. It consists of two parts, ad-hoc network and one or more access point like a satellite or ground base station (BS). The UAV-to-BS communication, the connection is created with an infrastructure like a ground base or satellite to transfer the data. UAVs are comprised of sensors that use wireless networks for data communication. Wireless sensor network (WSN) facilitate the interaction between base station and the UAV. These networks are exposed and unguarded. So, potential interception or eavesdropping can cause security concerns and it is possible for a potential adversary to snoop or fabricate the transmitted information. Also, these sensors are restricted in terms of bandwidth, energy, computing power, storage, and memory. These constrained resources nature make it impractical for WSNs to deploy traditional security schemes to transmit data between UAVs. Moreover next-generation UAVs will use more and more mortification sensors and actuators that will be dynamic and long lasting. Therefore, we are proposing a multilevel hierarchical system for data transfer that distributes computing overhead in FANET and at the same time ensures the independence and security of the sub-networks. Figure 1, shows a hierarchical architecture of UAV network for overhead distribution.

Hierarchical system is organized into a cluster or groups. Each cluster performs the operations in specific areas, with a cluster head (CH) elected for every cluster routinely and dynamically. The approach in hierarchical system is different than a classical flat network system in which all cluster members have the same access rights. In hierarchical network systems access to information brings a new level of security to the system. Information can only be viewed by those who have access to it. The CH is superior to ordinary sensor nodes. They have more computational ability, storage, memory, and energy and battery power. Cluster heads performs tasks such as aggregating information from the ordinary cluster members, processing data within the cluster, forwarding the data to base station and leading the cluster to the destination [22].

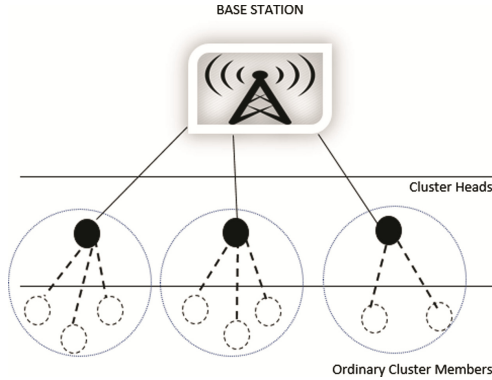


Fig. 1. Hierarchical UAV network architecture for overhead distribution

4.2 System Lightweightness

Embedded systems like UAV, suffer from limited resources in different areas including hardware, energy consumption, and bandwidth usage. This leads to the design and implementation of a framework that uses security primitives to reduce these overheads. Lightweight cryptographic primitives are preferred security methods over generic designs for constrained resources implementations. Cryptography algorithms scramble the secret data in such a way that it is unreadable by a third party. They are generally classified into asymmetric and symmetric key encryption algorithms. With Symmetric key cryptography, only one key is used for both encryption and decryption, which makes it suitable for securing stored data. On the other hand, asymmetric encryption, also known as public-key encryption, a public-key is used to encrypt data. The receiver uses a private key to decrypt the message. Public key cryptosystem (PKC) provides the most effective mechanisms for establishing security services including authentication, non-repudiation, integrity, confidentiality and digital signature. Asymmetric algorithms are much slower than symmetric ones and it is common practice to use both primitives in practical implementation. While symmetric primitives will process the heavy payloads, asymmetric primitives can be used to distribute symmetric keys securely. As Cryptographic key management is fundamental part of network security, in this paper, we are proposing Identity (ID)-based cryptography, using bilinear pairing over elliptic curve cryptography (ECC). The motivation is to provide a balance between resource consumption and security strength in hierarchical ad-hoc network.

4.3 Identity-Based Encryption (IBE)

Shamir [23] proposed the idea of the IBE scheme which uses unique ID of the device as its public key. In FANET, base stations act like a private key generator (PKG) and ID of a node can be assigned at the pre-deployment phase from base station to ensure uniqueness. The three obvious advantages [24] of IBE over conventional PKC are, firstly, IBE removes the need for certificates. Hence, we do not need certificate distribution and verification which save communication and computation overheads for the

resource constrained UAVs. Secondly, IBE enables noninteractive key agreement between UAV nodes and finally, any type of string can be a public key in IBE which does not exist with conventional PKC. Bilinear pairing is the integral part of Identity based key management scheme, which allows non-interactive key distribution between a pair of cluster nodes. Bilinear pairing operations are based on elliptic curves with given parameter. Elliptic curve discrete logarithm problem is more difficult to break than the factorization and discrete logarithm problem. Hence, the security strength of ECC is much stronger and complex than other public key cryptosystems. Also, its encrypted message size is very small as well, which implies lower bandwidth, power, and computational requirements [25]. We will not provide the details implementation of IBE in this paper but mathematical background and encryption and decryption process will be used from paper [14, 24, 26].

4.4 Selective Data Encryption

The fundamental of selective encryption algorithms is to encrypt some certain portions of the messages with less overheads. It is a very useful method for the different data formats such as text, image, audio and video. It can reduce the overhead on data encryption/decryption process, and improve the efficiency of the network without negotiating the security of the system. In our framework, we are proposing using a probabilistic selective encryption approach where a sender node includes proper uncertainty in the process of message encryption, so only the delegated recipient can decrypt the ciphertext and other unauthorized nodes have no knowledge of the transmitted messages. The concept and implementation of selective encryption will be used from paper [27, 28]. Authors of both papers proposed a selective encryption algorithm which is probabilistic in nature and is faster compare to toss a coin method where each alternate word has encrypted.

4.5 Obscuring Transmitted Data and Digital Data Right Management

Data hiding is the mechanism of securely embedding information to some cover medium and in the best case nobody can see that both parties are communicating in secret. A secret message can be plaintext, an image, audio, video, ciphertext, or anything which can be represented in the form of a bit string. Different applications have their unique security requirements for example, some applications may require a larger secret message to be hidden inside data, while others require absolute invisibility of the secret message. Steganography algorithms traditionally hide secret message by using an overt communications channel to carry the secret data and digital watermarking applies data hiding for digital rights management and data authentication. A digital watermark is a digital signal or pattern inserted into a message that provide data confidentiality. For our work, we refer steganography as being the general data hiding technique and digital watermarking as a specific instance of steganography.

Encryption ensures confidentiality but it does not provide data integrity. An attacker still can record packets without knowing what is inside the packets, and replay them. If the impostor record the whole data stream and re-transmits all split packets, then the

recipient would recognize a valid data stream and act accordingly. Again, even if the attacker views the cover file where the information is hidden within, there shall be no clue that there is any hidden data under the cover. In this way, the individual won't endeavor to decipher the data. In this paper, we proposed to use text based watermarking [17, 29] using Word Shift Coding Protocol (WSCP), that hides the secret data in the spaces between the words of the carrier text. Watermarking is also suitable for some tasks which encryption cannot such as copyright marking. Embedding encrypted copyright information within the contents of the file itself can prevent it being easily identified and removed.

5 Performance and Security Analysis

Proposed security framework improves the performance of resource constraint CPS in the following dimensions [30]:

- Flexibility: Addition and removal of new nodes are very flexible by allowing only new nodes, BS and CH to be involved in node addition and BS for node revocation, keeping other nodes free from overheads.
- Storage: It decreases storage requirements, saving memory to store keys and increases scalability of the system.
- Communication: Less communication in key distribution, therefore decreasing energy consumption. Because of reduced network traffic communication overhead decreases and increases systems lifespan.
- Efficiency: Uses less computing power to generate keys using fast and efficient encryption mechanism. Simple, short, and effective private key used to extract the secret message.

The framework also provides a secure communication mechanism in terms of:

Data embedding: The objective of data embedding is to safeguard the message against the adversary so the opponent cannot perceive the existence of message inside the cover object. Protection vanishes after decryption. Therefore, after encryption, watermarking technique embeds hidden copyright protection information to digital information being transmitted. These two techniques are complementary rather than overlapping.

Forward and backward secrecy: New nodes cannot detect previous messages because of periodic cluster head alteration of secret keys related to each cluster. Key reinforcement assures that keys related to the lower level nodes of hierarchy are also updated. Hence, the enemy can only get information in a certain region for a limited time span although the private keys are exposed.

Resilience against node capture attack: Compromised nodes are nodes that are manipulated by the adversary. Communication links between non-captured nodes are protected by using discrete logarithmic problem imposed by bilinear pairing. The key reinforcement mechanism assures that security limitations of key pre-distribution technique are kept limited within the cluster.

6 Conclusion

Security must be built into the applications themselves for an embedded system like UAV. In this paper, we proposed a system that ensures data security and confidentiality by tailoring traditional information security solutions. We have proposed a hierarchical structure for key distribution and information sharing to ensure confidentiality and increase the overall security of the system. The main benefit of our framework is that it provides network flexibility by allowing nodes to serve as cluster heads periodically and dynamically. Then the ordinary cluster nodes use IBE to create trust and negotiate keys with CH. Because of resource constrained nature of UAV, instead of using IBE, nodes use selective encryption techniques for message transfer. One part of the message will be send using selective encryption and other part will be sent using steganography. Future work will involve developing applicable techniques for UAV domain and conducting extensive security testing. The framework will be validated under controlled and reproducible environment. We will simulate the security framework in a testbed environment using OMNeT++, an object oriented modular discrete event-based network simulation framework mainly focused on the modeling of dynamic nature of ad-hoc communication networks.

References

1. Burmester, M., Magkos, E., Chrissikopoulos, V.: Modeling security in cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **5**(3), 118–126 (2012)
2. Dini, G., Tiloca, M.: A Simulation Tool for Evaluating Attack Impact in Cyber Physical Systems. In: Hodicky, J. (ed.) *MESAS*. LNCS, vol. 8906, pp. 77–94. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13823-7_8
3. Austin, R.: *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. Wiley, Hoboken (2011)
4. Airborg™ H8 10 K with top flight hybrid-power system (2017). <http://www.tflighttech.com/products/airborg-h8-10k-with-top-flight-hybrid-power-system.html>. Accessed July 2017
5. Snell, B.: McAfee labs 2017 threats predictions: “Dronejacking” places threats in the sky (2016). <https://www.mcafee.com/au/resources/reports/rp-threats-predictions-2017.pdf>
6. Rani, C., Modares, H., Sriram, R., Mikulski, D., Lewis, F.L.: Security of unmanned aerial vehicle systems against cyber-physical attacks. *J. Def. Model. Simul. Appl. Methodol. Technol.* **13**(3), 331–342 (2015)
7. FAA releases 2016 to 2036 aerospace forecast (2016). <https://www.faa.gov/news/updates/?newsId=85227>
8. Mansfield, K., Eveleigh, T., Holzer, T.H., Sarkani, S.: Unmanned aerial vehicle smart device ground control station cyber security threat model. In: 2013 IEEE International Conference on Technologies for Homeland Security (HST), pp. 722–728. IEEE (2013)
9. Kim, A., Wampler, B., Goppert, J., Hwang, I., Aldridge, H.: Cyber attack vulnerabilities analysis for unmanned aerial vehicles. In: *Infotech@ Aerospace*, pp. 1–30 (2012)
10. Javaid, A.Y., Sun, W., Devabhaktuni, V.K., Alam, M.: Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In: 2012 IEEE Conference on Technologies for Homeland Security (HST), pp. 585–590. IEEE (2012)
11. Gallagher, S.: Triathlete injured by “hacked” camera drone (2014). <https://arstechnica.com/security/2014/04/triathlete-injured-by-hacked-camera-drone/>. Accessed June 2017

12. Hartmann, K., Steup, C.: The vulnerability of UAVs to cyber attacks-an approach to the risk assessment. In: 2013 5th International Conference on Cyber Conflict (CyCon), pp. 1–23. IEEE (2013)
13. Javaid, A.Y.: Cyber security threat analysis and attack simulation for unmanned aerial vehicle network. University of Toledo (2015)
14. Hu, S.: A hierarchical key management scheme for wireless sensor networks based on identity-based encryption. In: 2015 IEEE International Conference on Computer and Communications (ICCC), pp. 384–389. IEEE (2015)
15. Yu, F.R., Tang, H., Mason, P.C., Wang, F.: A hierarchical identity based key management scheme in tactical mobile ad hoc networks. *IEEE Trans. Netw. Serv. Manage.* **7**(4), 258–267 (2010)
16. Sarmah, D.K., Bajpai, N.: Proposed system for data hiding using cryptography and steganography. *Int. J. Comput. Appl.* **8**(9), 7–10 (2010)
17. Altigani, A., Barry, B.: A hybrid approach to secure transmitted messages using advanced encryption standard (AES) and word shift coding protocol. In: 2013 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE), pp. 134–139. IEEE (2013)
18. Vegh, L., Miclea, L.: A new approach towards increased security in cyber-physical systems. In: Systems, Signals and Image Processing (IWSSIP), pp. 175–178. IEEE (2014)
19. Vegh, L., Miclea, L.: Enhancing security in cyber-physical systems through cryptographic and steganographic techniques. In: 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, pp. 1–6. IEEE (2014)
20. Yang, Y., Lu, J., Choo, K.-K.R., Liu, J.K.: On lightweight security enforcement in cyber-physical systems. In: Güneysu, T., Leander, G., Moradi, A. (eds.) *LightSec 2015*. LNCS, vol. 9542, pp. 97–112. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-29078-2_6
21. Bekmezci, I., Sahingoz, O.K., Temel, Ş.: Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Netw.* **11**(3), 1254–1270 (2013)
22. Faquih, A., Kadam, P., Saquib, Z.: Cryptographic techniques for wireless sensor networks: a survey. In: 2015 IEEE Bombay Section Symposium (IBSS), pp. 1–6. IEEE (2015)
23. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) *CRYPTO 1984*. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
24. Fang, Y., Zhu, X., Zhang, Y.: Securing resource-constrained wireless ad hoc networks. *IEEE Wirel. Commun.* **16**(2), 24–30 (2009)
25. Zhang, L., Tang, S., Luo, H.: Elliptic curve cryptography-based authentication with identity protection for smart grids. *PLoS ONE* **11**(3), e0151253 (2016)
26. Kodali, R.K., Chougule, S.K.: Hierarchical key agreement protocol for wireless sensor networks. *Int. J. Recent Trends Eng. Technol.* **9**(1), 25 (2013)
27. Oh, J.-Y., Yang, D.-I., Chon, K.-H.: A selective encryption algorithm based on AES for medical information. *Healthc. Inf. Res.* **16**(1), 22–29 (2010)
28. Ren, Y., Boukerche, A., Mokdad, L.: Performance analysis of a selective encryption algorithm for wireless ad hoc networks. In: 2011 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1038–1043. IEEE (2011)
29. Almuhamadi, S., Al-Shaaby, A.: A survey on recent approaches combining cryptography and steganography. *Comput. Sci. Inf. Technol.* **7**(3), 63–74 (2017)
30. Sahingoz, O.K.: Large scale wireless sensor networks with multi-level dynamic key management scheme. *J. Syst. Architect.* **59**(9), 801–807 (2013)