BOOK CHAPTER | *"The More The Authentication – The Merrier"*

Internet of Things (IoT) & Underwater Network Forensics

Timothy Kwaku
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: kwaku.timothy@st.gimpa.edu.gh
Phone: +233244287747

ABSTRACT

The proliferation of IoT devices and technology in recent years cannot be overstated. With the diverse area of application, IoT devices will be prone to unscrupulous attacks. Applying digital forensics in this field makes it a multi-faceted area that necessarily implies a lot of challenges out to be addressed in order to ensure compatibility. This research extensively considers existing literature with the view of highlighting the application areas of IoT, underwater networks and digital areas as well the research challenges that needs attention in order to realize a robust IoT and underwater forensics regime. These recommendations as well policy directions were also added

Keywords: Internet of Things (IoT), Underwater Network Forensics, Cybersecurity, Compatibility

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Timothy Kwaku (2022): Internet of Things (IoT) & Underwater Network Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 291-300
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P47

1. INTRODUCTION

The Internet's pervasiveness, along with the cost-effective downsizing of smart electronic devices, has given rise to a new computer paradigm known as the Internet of Things (IoT) (Zawoad & Hasan, 2015). The main strength of the IoT idea is without a doubt how much it will change many parts of people's daily lives and how they act. From a private user's point of view, the most obvious effects of the Internet of Things will be seen at work and at home (Atzori et al., 2010). As a new area in technology, IoT have potential applications ranging from building smart cities (Kaur & Maheshwari, 2016), virtual reality (Hu et al., 2021), Smart Farming, Smart Health, Smart Energy and The Smart Grid (Korade et al., 2020). The relevance of IoT in this modern technological dispensation cannot be overemphasized.

Digital forensics (DF) is a field concerned with the investigation of crimes involving technology. These crimes include those committed against, with, or via technology (Oriwoh et al., 2013). With the Internet of Things (IoT), crimes performed and originating exclusively from technology would be an important contribution. DF investigations are conducted by skilled, experienced, and competent investigators who employ open source and/or proprietary tools (for example, the

Computer Aided Investigative Environment - C.A.IN.E. and Encase) to perform duties such as obtaining and evaluating pertinent digital evidence. The proliferation of ubiquitous technologies necessitates the need for digital forensics as the propensity of internet crime cannot be ignored. Due to the proliferation of networks, network forensics has become a very significant topic of research. It is described as the capture, recording, and analysis of network events in order to find the source of security assaults or other issue instances (Rizal et al., 2018). Every area that uses internet networks or networks of any kind will need the application of network forensics in order to detect, prevent or monitor unscrupulous activities. This research will specifically understudy IoT, and underwater network forensics in order to establish the issues, frameworks, correlations and applications to enrich the existing body of knowledge.

1.1 Background to the Study

The notion of network forensics focuses on the data discovered over a network connection between two hosts. Network forensics examines the traffic data captured by firewalls, intrusion detection systems, and other network devices, including routers(Burić & Delija, 2015). The objective is to track back to the attack's origin in order to identify its perpetrators. Researchers in terrestrial radio-based sensor networks are becoming increasingly interested in underwater sensor networks. When compared to terrestrial sensor networks, many, but not all, underwater sensor networks are expected to have more costly equipment, higher mobility, sparser deployments, and different energy regimes (Partan et al., 2006b).

Wireless Sensor Networks (WSNs) offer a lot of potential for monitoring aquatic ecosystems since they can sense, collect, and transmit data wirelessly to users in real time. It has indirectly led to the establishment of underwater wireless sensor networks, a new paradigm in wireless sensor technology (UWSNs)(Fattah et al., 2020). Domingo, 2012 rehashed a concept of Internet of underwater things and described it as "..a world-wide network of smart interconnected underwater objects with a digital entity". Most critical data are conventionally deployed through contemporary underwater network systems. It is therefore only necessary that robust digital forensics framework be provisioned especially in an era of many miniaturized devices with internet access.

In order to have a full grasp on the field of underwater networks and the opportunities IoT presents, there is the need to assess the current state of literature, analysis the state of technology including existing frameworks and improvements and figure out the ways to close gaps in the various IoT and underwater developments.

2. RELATED LITERATURE

IoT and Applications

Due to the advances and potentials that IoT presents, there are a lot research that have been necessitated in the recent years. For any smart city application deployment, Kaur & Maheshwari, 2016 addressed the convergent field of cloud computing and IoT. Dubai was proposed as a smart city, with several application-based scenarios. The paper also proposed an IoT-based healthcare framework. Kiran & Sriramoju, 2018 used an IoT-based house monitoring system with android devices, relays, sensors, and raspberry pi for a future smart city application. We can save the most amount of electricity by using this programme. The main goal of IOT is to improve the quality of human existence.

Man's efforts are reduced by building this application, and machines function without human interaction. Atzori et al., 2010 categorized a wide range of IoT applications into Transportation and logistics domain, Healthcare domain, Smart environment (home, office, plant) domain and personal and social domain. The open issues cited by that research were: standards, mobility support, naming, transport protocol, traffic characterization and QoS support, authentication, data integrity, privacy and digital forgetting

Digital Underwater Networks

A popular type of Underwater Networks is Underwater Wireless Sensor Networks (UWSN). The UWSN is a network used to monitor activities in a particular region; it is equipped with smart sensors and vehicles that are able to interact collaboratively via wireless links. The surface sink gets sensor node information. The sink node is equipped with a transceiver capable of regulating acoustic signals received from underwater nodes. Additionally, the transceiver may broadcast and receive long-range radio frequency signals for contact with the shore station. The acquired information is utilized locally or linked to another network for a specific purpose(Fattah et al., 2020). The network architecture integrates traditional underwater wireless sensor networks created by (Jindal et al., 2015) and real-time underwater wireless sensor network architecture in the form of the Internet of Underwater Things suggested by (Domingo, 2012).

A number of practical challenges distinguishing underwater acoustic networks from terrestrial radio-based sensor networks were outlined by Partan et al., 2006a. There will be a wide range of operating regimes for underwater networks since there is no one. They do believe, however, that many key underwater networks will be more mobile and sparser than terrestrial sensor networks, due to various energy and cost factors. Moving between sparse and dense zones will need underwater network protocols to adapt, with distinct optimization criteria for each regime. The major needs for establishing critical services as well as shared platforms for UWSN were outlined by Fattah et al., 2020. It also created a taxonomy of important aspects in UWSNs by classifying architectural features, communications, routing protocol and standards, security, and UWSN applications. Finally, as a roadmap for future research directions, the significant difficulties that remain unsolved are were highlighted.

Jindal, 2014 while investigating the challenges associated with Underwater Acoustic Sensor Network (UWASN) stated the following as the various applications of UWASN: savor networks, tremorous monitoring, monitoring of environment, prevention of disaster, undersea reconnaissance, reinforced navigation, monitoring of accessories and prudent surveillance scattering. Their investigation revealed the necessity for new theoretical models to be developed. As a result, they identified a number of issues that must be addressed in order to create competent and decisive underwater acoustic sensor networks, as well as an optimized communication architecture that is adaptable to the characteristics of UWASN for data monitoring and recording in an underwater setting. They're also urged to widen the sector to include autonomous deployment and stationary configurations, as well as high-performance to low-cost operations.

Digital Forensics and Underwater networks

The Internet of Underwater Things (IoUT) is presented in Domingo, 2012, along with its primary distinctions from the Internet of Things (IoT). The proposed IoUT architecture was also discussed. Important application examples that show how IoUT components interact were suggested. Zawoad & Hasan, 2015 developed the first working definition of IoT forensics and analyzed the IoT forensics domain methodically to investigate the problems and concerns in this area of digital forensics. They presented the Forensics-aware IoT (FAIoT) concept as a way to facilitate accurate forensics investigations in the IoT world. They proposed a centralized trustworthy evidence repository in the FAIoT to facilitate the process of evidence collecting and analysis because the IoT infrastructure is very scattered and there is no uniformity among the devices. A diagrammatic representation of the FAIoT model as proposed is shown in fig.1

The proposed model was segmented into:

- Secure Evidence Preservation Module:
  This module will continuously monitor all registered IoT devices and securely save evidence. There are several ways to gather evidence. This module can preserve data while categorizing it by IoT device and owner. Thus, data from various users will not be merged. This module will also protect data from malevolent cloud employees by encrypting it with public-private keys so only investigators can see it.

- Secure Provenance Module:
  This module preserves the evidence's access history, ensuring correct chain of custody. It may provide provenance records for evidence usage using provenance aware file system. Because the secure evidence repository provider controls all evidence and access history, they can always alter the provenance record. An attacker can also learn sensitive facts about cloud data from the provenance data.

- Access to Evidence Through API
  They suggest providing law enforcement agencies with secure read-only APIs. These APIs will only be accessible to investigators and the court. They can use these APIs to acquire preserved evidence and provenance information. The secure evidence repository provider will need an extra web server to enable this functionality, which will interface with the previously stated modules to gather the requested data via an API call. The web server uses the synchronized data and the provenance record as resources to deliver a Representational State Transfer (REST) based API. GET procedures on the resources can be used to retrieve this evidence. A REST service caller can supply several arguments to get the desired response.

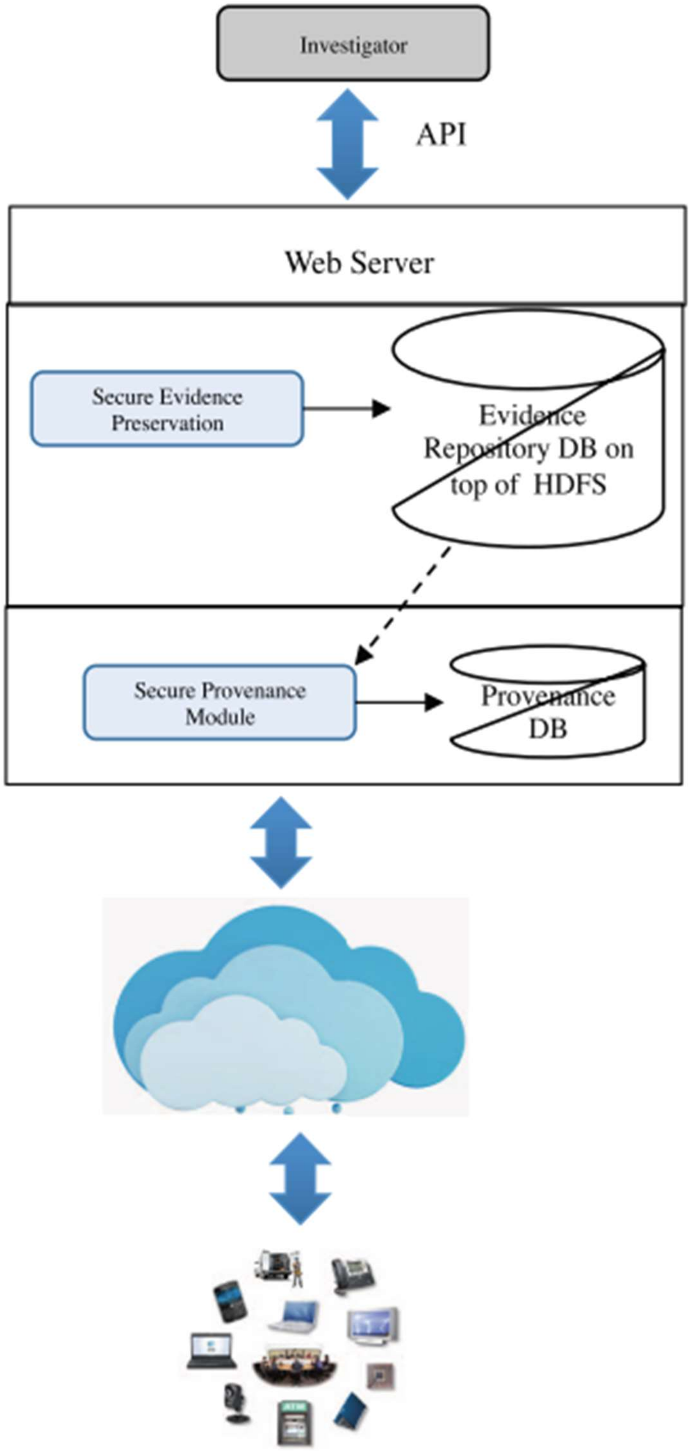
Investigator
API
Web Server
Secure Evidence Preservation
Evidence Repository DB on top of HDFS
Secure Provenance Module
Provenance DB

Fig.1 the FAIoT model (Zawoad & Hasan, 2015)

Network forensics is the process of collecting, recording, and analyzing network audit trials to identify the origin of security breaches or other information assurance issues (Burić & Delija, 2015). It becomes necessary that all kind of networks be provisioned in such a way that digital forensics could be performed in the event of any investigation. Network forensics is concerned with data discovered on a network connection, primarily entrance and egress traffic from one host to another. Network forensics attempts to decipher traffic data captured by firewalls, intrusion detection systems, and network devices such as routers and switches(Pilli et al., 2010).

Palmer (2001) defines network forensics as the "use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, or compromise system components, as well as providing information to assist in response." A forensics model for IoTs as proposed by (Rizal et al., 2018) is also very critical to guide the applications of digital forensics on IoT related networks. Figure 2 summarizes the underlying architecture as proposed by (Rizal et al., 2018)

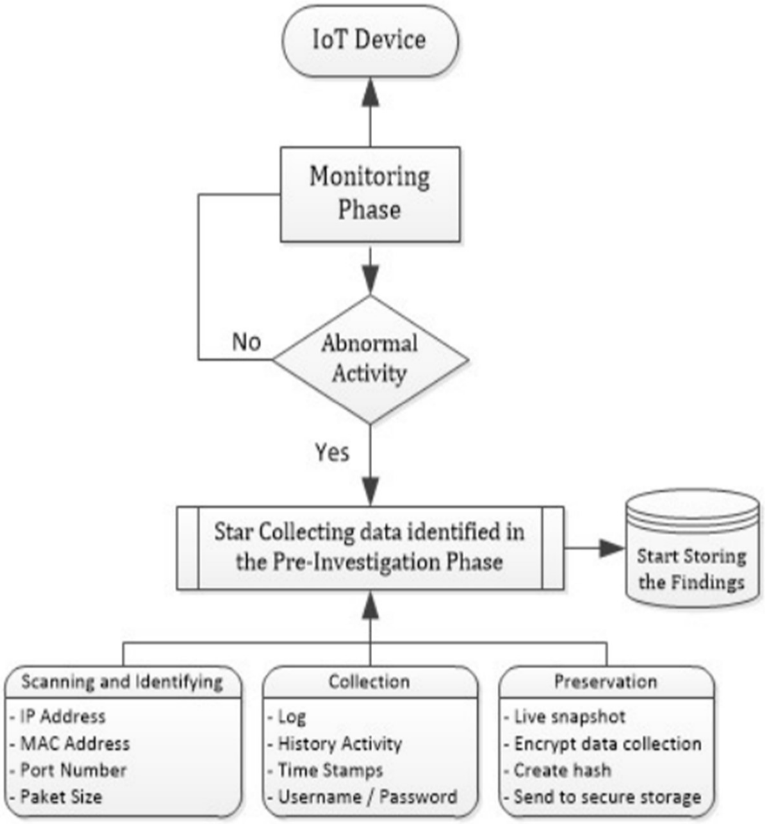

Fig 2. IoT Device Forensics (Rizal et al., 2018)

Using a network forensic process model to detect assaults on IoT devices using Bluetooth Arduino. Detection of flooding assaults on an IoT device. It will be saved in the data logger file. In order to gather evidence, researchers will use Wireshark to reconstruct the data log file included in Bluetooth Arduino UNO Level Forensic Device, network forensics to analyze and record traffic. The IoT devices will generate a lot of data. We will do the data network here. Because the amount of data evidence will be vast, it will be difficult to evaluate the data and detect forensics.

3. RESEARCH GAPS/FINDINGS

As already highlighted, underwater networks are predominantly made up of wide range sensors for various detection activities. Though there are not so much literature on the application of digital forensics in underwater networks, the implementation of its various components raises some issues that needs to be addressed. Some of the challenges that emerged from the extensive literature survey includes:

In terms of the design of the underwater networks, some design challenges that were discovered were: cost of underwater sensors, issues of power, deployment, geographical correlation and memory(Jindal et al., 2015). Partan et al., 2006a pointed out some practical issues that future research can seek to address. Some of issues they pointed out include: energy efficiency (communication energy cost, AUV energy cost), mobility and sparsity (Economics of Oceanographic Operations, Contention between Navigation and Data Signals, Disruption-Tolerant Networks, Network-Motion Interactions, MAC Fairness in Mobile Networks).

Specifically dealing with Internet of Underwater things (IoUT), the gaps identified in its implementation were aptly listed by (Kao et al., 2017) as transmission media; propagation speed; transmission range; transmission rate; difficulty to recharge; mobility; and reliability. These challenges are essentially the limitations the technology involving underwater networks presents over terrestrial based network infrastructure.

Domingo, 2012 in the implementation of IoUT architecture which is critical for apparent digital forensics outlined the following as the research challenges. Self-management challenges: This is the method through which the IoUT runs its own operations without the assistance of humans. Support for self-configuration, self-healing, self-optimization, and self-protection capacities is necessary for this purpose. Energy efficiency issues were equally raised. Another significant problem is to enhance tracking methods. Because they are often applied to living animals in the IoUT, it must be carefully researched if the resulting tags injure or hinder their activities, as well as the appropriate form and size of these tags and the materials used to make them.

Burić & Delija, 2015 catalogued a set of challenges in relation to network forensics. The following were the research challenges or gaps:

- Network-based evidence: This encompasses issues from acquisition, content, storage, privacy, seizure and admissibility.
- Network forensic investigation: This also comprises issues like: data sources, data granularity, data integrity, data as legal evidence, privacy issue and data analysis.

Pilli et al., 2010 also categorized the challenges in network forensics into collection and detection, data fusion and examination, analysis, investigation and incident response.

- Collection and Detection
  The challenge is to discover valuable network events and record the bare minimum of representative qualities for each event in order to keep the least amount of data with the best probability of success. As a result, data storage requirements are reduced. A data digest will enough to detect malicious activities, but a full capture will be necessary to reconstruct attack behavior.

- Data fusion and examination
  To determine if an inquiry should be launched, data from multiple tools must be compiled and analyzed. Data fusion from diverse security technologies placed on each host on the network is a critical issue. An attack's dependency on multiple tools and reconnaissance of different hosts legitimizes it. Identifying aberrant network events and differentiating attack traffic from regular traffic is a serious difficulty.
- Analysis
  The final stage in network forensics is to evaluate attack data and pinpoint the source. Network events must be classified and clustered to allow for simple analysis of enormous amounts of data. Complicated protocol analysis also requires attention. Soft computing and data mining approaches may be used to classify, correlate, and link abnormalities. This study is needed to categorize attack patterns and reconstruct attack methodologies to understand the attacker's goal and approach.
- Investigation
  An attack must be attributed to a host or a network. The results must be admissible in court. Analyzing logs and other network traces should reveal attack origins. Bypassing IP spoofing allows IP traceback to the attacker's originating address (Mitropoulos et al., 2005). Detecting and analyzing TCP connection chains can reveal attack steps. Creating a topology database and IP mapping to find an attacker is difficult. As new protocols like IPv6 become operational and popular, resolving problems involving them will become critical.
- Incident Response
  It is necessary to respond to network usage in real time so that crucial data is not lost before the reaction is launched. When the alerts start, the reaction procedures should start right away. The crucial point to remember is that the attacker must be unaware of the reaction.

4. CONCLUSION

IoT and underwater network forensics are a multi-faceted area of study. The enormous application areas of these concepts cannot be overemphasized. Network forensics under water can be used to solve problems link undersea surveillance for various purposes ranging from exploration, tracking where items are in an event of an accident and other uses. In order to implement the various digital frameworks in underwater networks, a myriad of concerns of modern underwater networks and digital forensics ought to be addressed.

Some the general network and IoT issues this paper cited power and energy issues, self-management, cost of equipment, transmission media; propagation speed; transmission range; transmission rate; difficulty to recharge; mobility; and reliability. In relation to the digital forensics, some of the challenge cited were collection and detection, data fusion and examination, analysis, investigation and incident response. It is the conclusion of this research that future research aimed at developing better frameworks in the field of IoT and underwater networks should address these challenges in order to make more impact.

5. RECOMMENDATION FOR POLICY AND PRACTICES

In order to have successful digital forensics in underwater networks especially in the era of IoTs, a multi-factor framework that considers all the underlying requirements of ideal network forensics have to considered. Such frameworks can be a basis of standardization to further regulate future forensic activities in various areas. Also, as a matter of policy, governments and authorities should invest in research that will seek to address the challenges this field. This can aid law enforcement agencies and disaster mitigation agencies to carry out their investigative actives easily.

6. DIRECTION FOR FUTURE WORKS

Future works should essentially focus on the various issues with network setups like energy issues, transmission issues, infrastructure cost and host of others.
Also, a comprehensive framework regime should be put in place to guide implementation of IoUTs to make them digital forensic compliant.

REFERENCES

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Burić, J., & Delija, D. (2015). Challenges in network forensics. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, *May*, 1382–1386. https://doi.org/10.1109/MIPRO.2015.7160490
3. Domingo, M. C. (2012). An overview of the internet of underwater things. *Journal of Network and Computer Applications*, *35*(6), 1879–1890. https://doi.org/10.1016/j.jnca.2012.07.012
4. Fattah, S., Gani, A., Ahmedy, I., Idris, M. Y. I., & Hashem, I. A. T. (2020). A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges. *Sensors (Switzerland)*, *20*(18), 1–30. https://doi.org/10.3390/s20185393
5. Hu, M., Luo, X., Chen, J., Lee, Y. C., Zhou, Y., & Wu, D. (2021). Virtual reality: A survey of enabling technologies and its applications in IoT. *Journal of Network and Computer Applications*, *178*(June 2020). https://doi.org/10.1016/j.jnca.2020.102970
6. Jindal, H., Saxena, S., & Singh, S. (2015). Challenges and issues in underwater acoustics sensor networks: A review. *Proceedings of 2014 3rd International Conference on Parallel, Distributed and Grid Computing, PDGC 2014*, 251–255. https://doi.org/10.1109/PDGC.2014.7030751

7. Kao, C. C., Lin, Y. S., Wu, G. De, & Huang, C. J. (2017). A comprehensive study on the internet of underwater things: Applications, challenges, and channel models. *Sensors (Switzerland)*, *17*(7). https://doi.org/10.3390/s17071477
8. Kaur, M. J., & Maheshwari, P. (2016). Building smart cities applications using IoT and cloud-based architectures. *2016 International Conference on Industrial Informatics and Computer Systems, CIICS 2016*, *November 2018*. https://doi.org/10.1109/ICCSII.2016.7462433
9. Kiran, S., & Sriramoju, S. B. (2018). A study on the applications of IOT. *Indian Journal of Public Health Research and Development*, *9*(11), 1173–1175. https://doi.org/10.5958/0976-5506.2018.01616.9
10. Korade, S. A., Kotak, V., & Durafe, A. (2020). *A Review Paper on Internet of Things (IoT) and its Applications A Review Paper on Internet of Things (IoT) and its Applications*. *June 2019*.
11. Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, COLLABORATECOM 2013*, *December*, 608–615. https://doi.org/10.4108/icst.collaboratecom.2013.254159
12. Partan, J., Kurose, J., & Levine, B. N. (2006a). A survey of practical issues in underwater networks. *WUWNet 2006 - Proceedings of the First ACM International Workshop on Underwater Networks*, *2006*, 17–24. https://doi.org/10.1145/1161039.1161045
13. Partan, J., Kurose, J., & Levine, B. N. (2006b). A survey of practical issues in underwater networks. *WUWNet 2006 - Proceedings of the First ACM International Workshop on Underwater Networks*, *2006*, 17–24. https://doi.org/10.1145/1161039.1161045
14. Pilli, E. S., Joshi, R. C., & Niyogi, R. (2010). Network forensic frameworks: Survey and research challenges. *Digital Investigation*, *7*(1–2), 14–27. https://doi.org/10.1016/j.diin.2010.02.003
15. Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *7*(4), 382–390.
16. Zawoad, S., & Hasan, R. (2015). FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 279–284. https://doi.org/10.1109/SCC.2015.46