applied sciences

MDPI

Article

Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things

Ahmad Hasan [1,2], Muazzam A. Khan [3,*], Balawal Shabir [1,4], Arslan Munir [5], Asad Waqar Malik [1], Zahid Anwar [6] and Jawad Ahmad [7,*]

1 Department of Computing, School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
2 Faculty of Computing, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
3 Department of Computer Science, Quaid-i-Azam University, Islamabad 15320, Pakistan
4 Department of Cyber Security, Air University, Islamabad 44000, Pakistan
5 Department of Computer Science, Kansas State University, Manhattan, KS 66506, USA
6 Department of Computer Science, North Dakota State University, Fargo, ND 58105, USA
7 School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK
* Correspondence: khattakmuazzam@gmail.com (M.A.K.); j.ahmad@napier.ac.uk (J.A.)

Abstract: The internet of things (IoT) is prone to various types of denial of service (DoS) attacks due to their resource-constrained nature. Extensive research efforts have been dedicated to securing these systems, but various vulnerabilities remain. Notably, it is challenging to maintain the confidentiality, integrity, and availability of mobile ad hoc networks due to limited connectivity and dynamic topology. As critical infrastructure including smart grids, industrial control, and intelligent transportation systems is reliant on WSNs and IoT, research efforts that forensically investigate and analyze the cybercrimes in IoT and WSNs are imperative. When a security failure occurs, the causes, vulnerabilities, and facts behind the failure need to be revealed and examined to improve the security of these systems. This research forensically investigates the performance of the ad hoc IoT networks using the ad hoc on-demand distance vector (AODV) routing protocol under the blackhole attack, which is a type of denial of service attack detrimental to IoT networks. This work also examines the traffic patterns in the network and nodes to assess the attack damage and conducts vulnerability analysis of the protocol to carry out digital forensic (DF) investigations. It further reconstructs the networks under different modes and parameters to verify the analysis and provide suggestions to design roubust routing protocols.

Keywords: digital forensics; computer forensics; blackhole attack; wireless sensor network; forensic analysis; internet of things; network simulator (NS3)

Citation: Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. *Appl. Sci.* **2021**, *12*, 11442. https://doi.org/10.3390/app122211442

Academic Editor: Corrado Santoro

Received: 29 August 2022
Accepted: 3 November 2022
Published: 11 November 2022

1. Introduction

The emerging integration of IoT and WSNs in various application domains has financial and societal benefits, but when these services are misused or impersonated by malicious entities, they may result in severe threats [1]. These threats may increase from the individual to the community level depending on the capacity of the malicious entity. The extensive use of WSNs and IoT in all domains of life has great risks, such as susceptibility to different security attacks [2]. Network availability, anonymity, confidentiality, access control, and integrity are critical in these vulnerable infrastructures, especially in networks of mobile devices. Data distribution and acquisition in WSNs and IoT is vulnerable to various problems such as mobility, snooping, espionage, and link breakage [3]. The mobile and broadcasting nature of WSNs, along with the resource-constrained infrastructure, makes these networks susceptible to miscellaneous denial of service (DoS) attacks [4,5]. This research work focuses on the blackhole attack (BH), which is a detrimental type of DoS attack. In the BH attack, a malicious node proclaims a latest and shortest route to the

destination in the route-discovery phase of a source node (SN), and then the SN enters the trap and sends all data via malicious node. Consequently, the malicious node drops data packets of SN. The packet dropping behavior can encompass multiple attacker and target nodes, which may lead to an extensive DDoS attack [6]. The forensic analysis of the BH attack in static and mobile WSNs and IoT by comparing diverse parameters is conducted in this work.

The precursory literature indicates various state-of-the-art attack mitigation schemes, but since security is never ultimate, and perfect security is just an illusion; it is imperative to investigate what, when, how, and why a particular security incident happened or is happening, and what damage it costs. The vulnerabilities and loopholes in the system need to be examined and revealed. Furthermore, damage to the system due to the incident(s) needs to be measured, and countermeasures need to be developed from the outcomes of forensic investigations.

Digital forensics (DF) for WSN and IoT is difficult due to the proliferation of devices, heterogeneity, immense network traffic, and lack of transparency in digital evidence (DE) processing. Even though IoT data might be a valuable trace of DE, the DF investigators deal with disparate challenges, from the massive range of IoT devices and improper formats to the multi-tenant cloud organization and the subsequent multi-jurisdictional requirements[7]. Moreover, the identification, capture, discovery, and analysis of network traffic encompassing IoT infrastructure is challenging compared to traditional networks. High-speed data transmission, data extraction locations, IP addresses access, privacy, integrity, data storage on network devices, and intelligent forensic tools are key challenges in traffic analysis in IoT and WSN. Another challenge is end-to-end encryption, which means a compromise between privacy and the achievement of the DF investigation [8,9]. Furthermore, as many IoT nodes are accumulating and processing sensitive data, they turn into a treasure of data for malevolent entities. Thus, security and particularly the capability to identify compromised nodes, together with compiling and preserving the DE of attacks, urhently arise in the effective implementation of IoT networks [10]. Post-mortem analysis of the attack can expose the status of the network at specific times and eventually provide traces about the nature of the attack and the identities of the malicious nodes.

The AODV routing protocol is chosen for this study because it is one of the most notable protocols that is broadly accepted and extensively used in wireless mesh networks (WMN) due to its low setup delay, large-scale implementation, loop-free setup, flatness, efficiency in a dynamic environment, and flexibility. AODV is one of the four prime routing protocols that are standardized by the Internet Engineering Task Force (IETF) MANET working group. AODV serves as the foundation for devising new routing protocols in the wireless networks domain [11–13]. We analyze the performance of AODV in mobile WSN and IoT under the BH attack. Further, a detailed forensic analysis of the basis of diverse parameters and aspects is performed. The main contributions of this research work are given below.

- The BH attack in WSNs and IoT with the AODV routing protocol is investigated in a rigorous and generic manner.
- A vulnerability analysis of the AODV protocol is performed, and a forensic analysis for static as well as mobile WSN and IoT for ad hoc and traditional modes under the BH attack is carried out. The traffic patterns in the network and on the nodes are examined with the assistance of various analytical tools to assess the attack damage.
- An analogy between the DF investigation of a real-life WSN/IoT and a simulated environment is devised at the device, network, and cloud levels to correlate the procedures and tools on both sides.
- The networks under mobile and static mode with variation in the number of total nodes and BH nodes are reconstructed to verify the observations of forensic analysis. Further, a damage analysis on the basis of strategical positioning and cooperation of the BH nodes is conducted.

- Suggestions powered by this study are provided to design routing protocols that will be amenable to DF investigations.

This paper is structured as follows: Section 2 describes the related work. The proposed methodology for forensic analysis, artifact collection framework, and an analogy between simulated and real-time DF investigations are presented in Section 3 followed by Section 4, which discusses the simulation environment and results. Finally, Section 5 concludes this work.

2. Literature Review

The BH is an active attack among the tremendously harmful possible attacks in WSN and IoT. An antagonist entity claims the shortest path to the destination via a route reply (RREP) packet to the source node, even if it does not have any route to the destination. The sender transmits all the data packets to this entity, and consequently, it drops the data packets instead of forwarding them to the destination [14], distressing the collective throughput and energy of the nodes. The malicious entity is called a "Blackhole Node" due to the packet-absorbing behavior.

The packet-dropping behavior can be absolute or selective and can also produce a gateway to other catastrophic attacks. In absolute packet dropping, the BH node drops all of the packets, all the time, and for all the nodes. In this case, the network nodes may sense abnormality, and alternative routes may be chosen. However, the selective BH attack is very difficult to detect because the BH node may drop the packets at a selective time period or for specific nodes. Moreover, there are two categories of BH attacks, depending on the number of malicious nodes and single and cooperative BH attacks. If a single node is involved in dropping packets, then it is called a single BH attack, and if multiple nodes are involved, then it is called a cooperative BH attack [6,15].

The insecurity of WSN and IoT can be classified into the insecurity of nodes, routers, and data traffic. The resource-constrained environment, computational capacity, and limited transmission range make it problematic to operate an entire network steadily at a time [6,9,16].The attackers usually benefit from the hop-to-hop dependency of WSN and inoculate malicious nodes in the routes [17]. Now, the research efforts devoted to mitigating the BH attacks, the vulnerabilities of WSN and IoT, DF complications, and forensics investigations studies carried out in this domain will be discussed.

An approach [15] functioning by distributing the network into several little zones of the same size, and allocating a unique ID to each zone is suggested to detect the BH attack. The nodes know their particular locations and affiliation by a localization algorithm and broadcast their energy level in the network and to the base station (BS). The highest-energy node is chosen as the cluster head (CH). Some mobile agents support the system by monitoring the network, and if they sense any abnormality, then they mark that specific node as a BH node and trigger a message to the CH and BS. In [18] a control packet (CP), comprehensive extended data routing information (EDRI) is proposed to mitigate the BH attack. The EDRI table includes the parameters of nodes. The information such as neighbor ID, FROM (source), TO (destination), and BH node is included. Binary digits specify the honesty of the node. The CP has the IDs of the source node, neighbors, and a persistent random number (RN) security value. The CP cannot be transmitted by an adverse node, so it works for detecting a single BH attack. The methodology for community attacks is powered by the next hop number (NHN), CP, and a random number generator (RNG). It operates in three phases: discovery of the routes, scrutiny of the route, and elimination of the cooperative BH nodes.

A Cluster Reputation-based Cooperative Malicious Node Detection and Removal (CRCMD&R) scheme extending the AODV protocol with additional features [19] discovers an adverse node in the route setup phase. Therefore, the information will not be transmitted through the neighbor's nodes and malicious routes. The CH reserves three tables named legitimacy value (LV) table, neighbor's table, and reputation value (RV) table to compute the trust values of the routes. In another anticipated system [20], a malicious node is

inserted into the network to manipulate the determined traffic by promoting the shortest path to destinations. An intrusion detection system (IDS) is mounted on each node to detect the packet drop behavior. A smart attack detection (SAD) scheme [21] is projected for four types of attacks. Primarily, the scheme detects the type of attack first and then deals with it. The involved attacks are wormhole, sinkhole, BH, and botnet. The identification depends upon the node axis, mobility, and node number.

An intrusion avoidance system–secure data transmission (IAS-SDT)-focused approach [22] constructed on AODV and AOMDV (multipath extension) with a presumption of established routes is proposed to mitigate BH attack. A message is fragmented and encrypted using a homomorphic encryption scheme during the route configuration phase. The identifiable routes are assigned to each cluster. Only one fragment of the message is routed through every group. If an adversary drops the fragments, the alternative route is assigned until the arrival of all fragments. A tactical mitigation technique [23] that comprehends with certainty the BH and wormhole attack in the AODV is suggested, in which the nodes in the route preserve a record for every RREP packet for a definite time with their sequence (seq) numbers. The average of all seq numbers is computed by the specified formula. To conclucde, the routes with a value greater than computed are engaged for transmission.

The critical operations of WSN and IoT and their subjected data are a significant subject for future DF. The digital evidence (DE) found in these networks is difficult compared to what the investigation community currently possesses (Table 1). Furthermore, these systems involve inventive and enhanced prospects for data [14]. The DF techniques applied are constructed using the DF process model entailing the processes of collection, examination, analysis, and reporting [14,24]. These data are crucial not only for the ongoing investigation process but for future investigations as well. The DF in these networks is challenging when it approaches accuracy issues due to the intensity of data analysis, heterogeneity, encryption, third parties, and proprietary issues bearing the risk of demolishing data integrity and granularity [24,25]. The complexities are increased due to the significance of identified and collected devices, indistinct network confinements, and edge-less networks [25,26]. The data analysis is a big challenge for the investigator's aptitude to yield rigorous, forensically sound, and admissible DE. A study determined that the growth in the number of infested entities aggravates the harm of attack [27].

Table 1. The Digital Evidence (DE) in WSN and IoT [14,24–26].

	Internal				External		
Sources of DE	**Perimeter Devices**	**The Network**	**Sensor Nodes**	**M-Area Networks**	**Web Environments**	**End Nodes**	**Cloud**
Example	AAA and NAT Servers, IPS, IDS	Network Media	IoT ware, Embedded Systems	BAN, LAN, PAN	Web Clients, Servers	Devices, Sensors	Public, Private and Hybrid
Expected DE	Admin Level Evidence	Network Logs	IP, SSID, Data	Client VMs, Logs	User activity logs	IP, SSID, Data	Network Logs

A DF study in [28] suggests the observer nodes for their specific area. Some algorithms are advised for the accumulation and forwarding of collected DE to BS and recreating the potential scenario for the wormhole attack. The simulation calculates the communication overhead and memory overhead. The approach successfully detects wormholes due to its strict monitoring system. Another DF study analyzed non-address spoofing flood (NASF) DDoS in MANET [29]. A statistical examination of flow rate information and IDS log files is used to establish detection features. The detection ratio, false detection rate, and detection time are three different parameters to evaluate the NASF attack. Network forensics is a live DF analysis of traffic and is composed of pattern recognition, correlation fusion, and network traffic disability. The DE usually composed of captured traffic and network device data. Live network traffic is also captured as mature attackers may delete log files. It involves three questions and two features: Is there an adversary in the traffic? Does it cause DDoS? and What is the time of the attack [29,30]? The detection features (Feature I and II)

are based on the statistical analysis of flow rate info and IDS log files. The detection time, rate and false detection rate are used as metrics of performance [29,30].

There are some other studies that examine the jamming attack in the WSN [31,32]. These are emphasized in the location of the clogged zone and victim nodes that damaged the network performance. A Q-learning design algorithm is used for the identification of the node location. The learning model is asynchronous and is capable of identifying the location of the the jamming area in the run-time when the attack take place. One study [33] discussed the live forensic investigation of the man in the attack (MITM). An intrusion detection system (IDS) is activated with traffic data to watch processes, packet sniffing, and log traffic with an open source IDS snort. The Snort IDS examines the entire traffic system and explores abnormalities in the network. The Live Forensic technique is implemented in a conventional manner that comprises identification, preservation, analysis, and presentation. The results of the exploration of DE are obtained in the form of the IP Address and port. The mitigation of attacks is carried out by blocking the IP Address and port used by the attacker.

Kumar et al. [34] analytically evaluated the information reclaimed from an IoT networking device to detect the elements caused by a security rupture by extracting flash and RAM objects from a sensor node. Network connectivity information is extracted and investigated by various scenarios. They projected a scheme with the help of a RAM dump analysis tool for the extraction, analysis, and correlation of forensic data for IPv6-based WSN deployments. An IPv6 Low-Power Wireless Personal Area Networks (6LoWPAN) traffic forensic scheme [35] to accomplish detection and investigation of attacks against availability in WSN was projected to construct the scenarios of potential interest. This scheme is related to the previous one.

The attack mitigation approaches and DF studies related to this research are extensively discussed in this section. Notably, these approaches lack a node-to-network relation with the fluctuations in the severity of the attack, root-level DF investigation of BH attack, and position of the BH node relative to the cumulative damage resulting from the attack. Usually, the mitigation approaches describe the number of malicious nodes directly proportional to the damage to the network. This behavior is briefly analyzed in our research. The mitigation approaches presented are fair enough for their perspective and objectives but cannot be declared perfect for every situation and network environment. There is always a need for postmortem analysis of the attack for designing advanced countermeasures and fighting precariousness. Perfect security is just an illusion, as attackers breach systems regardless of robust prevention schemes.

3. Forensic Analysis of the Black Hole Attack

This section contains strategic primitives and their discussion for this research work. Firstly, the details of research methodology for DF investigation process are discussed. The methodology works in accordance with the standard DF investigation procedure. Further, the logical analogy of the research methodology to the real-life standard DF investigation method is described. Secondly, the details of the simulation data-collection framework of NS3 are discussed. Thirdly, an analogy of DF in simulated and real-life environments is described.

Figure 1 depicts the research strategy of this work in accordance with standard DF investigation process. The tools and techniques used at specific steps in this research and the description of relevant outputs are also shown. The horizontal flow describes each step, and the vertical flow describes the methodology flow, which follows standard the DF investigation process. For example, in the simulation of the attack step in the research strategy, the NS3 tool is used for defining the network and BH attack. Now, the particulars of this research work will be discussed.

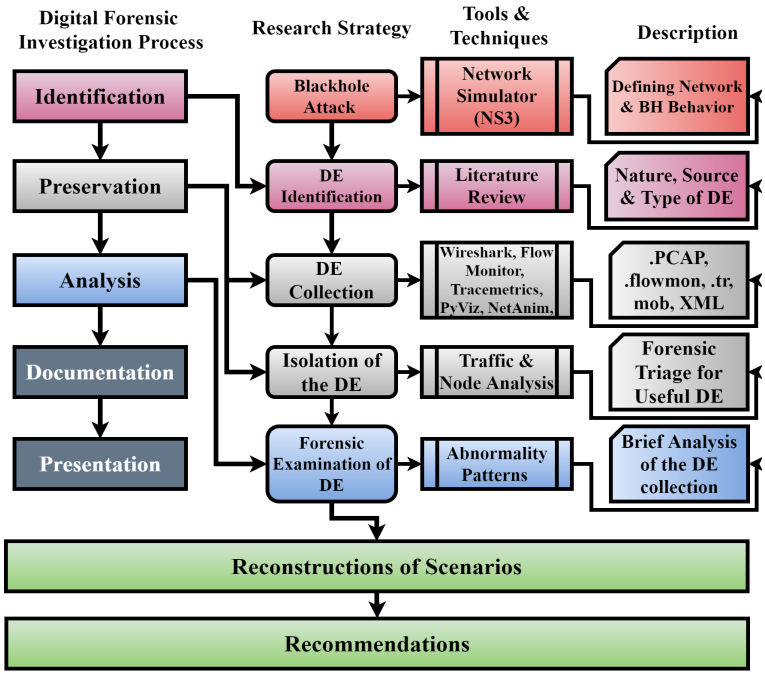

Figure 1. Strategy for forensic analysis of a BH Attack.

3.1. Digital Forensic Investigation Process

3.1.1. Attack Simulation

The simulation approach follows two scenarios. Initially, the network is executed in a normal condition, and then the BH attack starts in a random manner for forensic analysis. The identities and the number of malicious nodes are unknown. The BH attack and its effect on the network and AODV routing protocol are investigated and analyzed. Secondly, the analysis is verified by reconstructing several networks with some variations. Different scenarios with a variety of parameters are considered in the simulation of the network. This study includes scenarios such as mobile and static networks, the total number of nodes, and the total number of malicious nodes under parameters such as the total number of transmitted received and lost packets. The comprehensive performance of the network is measured from packet delivery ratio (PDR), packet loss ratio (PLR), end-to-end delay (E2E-DL), and Throughput (TH). This is briefly discussed in Section 4.1.8.

3.1.2. Digital Evidence Identification and Its Collection

The first step concerns the assessment of potential sources of relevant DE that can be found in the network. In our case, network nodes' IDs, IP addresses, and traffic logs are potential sources for the analysis. The inspection of these sources reveals insight into the attack, damage, and weakness of the network and protocol. The next step is to collect DE after the simulation ends. The useful DE is found by inspecting the live traffic of the network, traffic logs, and data maintained by the network devices. The outputs such as packet capture (.PCAP), comma-separated file (.CSV), Flow Monitor (.flowmon), mobility (.mob), Tracemetrics (.tr), and extensible markup language (.XML) files are preserved in this step for further analysis.

3.1.3. Isolation of the DE

The fourth step consists in the isolation of the DE and selection of the DE on a priority and importance basis. We have different types of output files for concerning analysis such as flowmon traces for network layer traffic analysis, PCAP traces for node-level traffic, and NetAnim traces for network routing protocol's traces. Furthermore, for example, in

flowmon traces, there are almost a thousand flow IDs. The IDs with higher packet loss ratios are points of interest.

3.1.4. Forensic Examination of the DE

This step briefly analyzes the collected DE. This analysis is multidimensional due to the types of traces. The .XML, .CSV, .flowmon, .tr, and .PCAP files are generated after the simulation ends. The tools such as Wireshark, NetAnim, Flow Monitor, and Tracemetrics are used for the analysis of remnants. The abnormalities are found by inspecting the traces files. The analysis of DE revealed some uncertainties such as the decline in network performance and, at a time, the sudden absence of data packets in the network raised questions. Specific flow IDs had 100% packet loss. The BH nodes in between the sender and receiver dropped all of the data packets. The nodes that frequently advertised routes to senders and consequently dropped the packets caused a major flood of protocol control packets in the network. A malicious node that can advertise a route to a major chunk of nodes can cause great damage. The number of total nodes in the network also has an impact on the performance of routing protocol. Therefore, some networks are reconstructed under different variations to verify the analysis. Increasing and decreasing total number of nodes and number of malicious nodes affected the scalability and variated the volume of control packets in the network.

3.1.5. Verification of Analysis

In this step, several networks are reconstructed in the mobile and static networks mode with variations in total number of nodes and number of BH nodes and the performance of the networks is observed by incorporating several parameters such as PDR, PLR, E2E DL, and TH. In comparison with the normal network, the BH attack declined the comprehensive performance of the network. The scalability of the network using AODV under variations also decreases.

3.2. Artifact Collection Framework

It is crucial to understand for the sake of good investigation how the simulator maintains and collects the statistics of networks. This research uses Network Simulator 3 (NS3), which is one of the most credible simulators for R&D. It is mainly focused on modern IPv4 and IPv6 networks, non-IP architectures, and the construction of virtual network (VN) emulations. It also facilitates the topology generation, event scheduling, random variables, and timers. There are some essential facilities of NS3 which are very important to carry out this research such as nodes, applications, channels, tracing, logging, and statistics. NS3 has the ability to emit and consume real network packets [36].

This analysis is based on the remnants that can be found in real networks and also from the NS3 simulations. The statistical framework can be used autonomously without incorporating the tracing system. It helps users to create, aggregate, and analyze data over multiple trials [37]. It can be integrated with the NS3 tracing system. In the statistical framework (Figure 2),

- Each experimental trial is piloted by each instance of the simulation program, whether in a serial or a parallel manner.
- A script executes the instances of the simulation program in a controlled manner, varying parameters as necessary.
- After this, data are composed and stored for further analysis and plotting graphs.
- The analysis may be performed by external scripts and helping tools.

One of the key objectives of the framework is to collect data and make it accessible for further operations. The network simulation tools address several design characteristics and propose numerous simulation abstractions to characterize and model real-life behavior of the networks. These tools generate the same outcomes from a practical perspective and the capacity to model communication phenomena [38]. Therefore, the DE produced from the NS3 is credible enough to pursue the DF investigations, as it is equivalent to real-life

networks. Handling DE in simulations is simple as compared to real-life networks because a small change in the operations and unavailability of electrical power can change or demolish the potential DE; i.e., the volatile memory components can be washed out. The invariability of DE is ensured through standard procedures in real-life networks such as seizing the devices, imaging the volatile and non-volatile memories, and using write-block software. However, the NS3 statistical framework carries out that task to some extent. Furthermore, the standard DF procedure is followed throughout the research. The use of simulation tools for research is widely acceptable due to its affordability, flexibility, and accessibility. Simulation is a risk-free world.

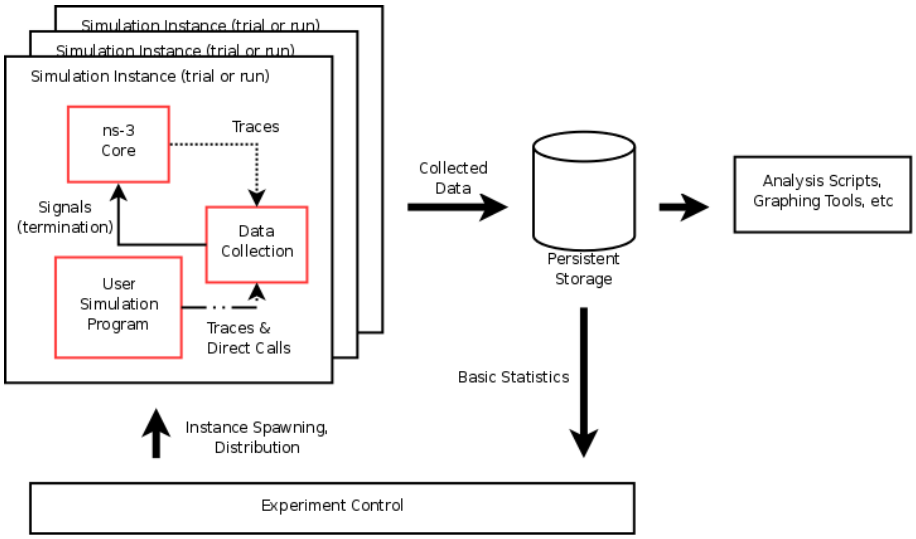

Figure 2. The statistical framework of NS3 [37].

3.3. Analogy of Real-Life DF and Simulated DF

IoT and WSN produce rich-source DE. DF investigators deal with distinct challenges, from the enormous range of IoT gadgets and different formats, to the diverse cloud infrastructure and the resulting multi-jurisdictional litigation. Therefore, a real-life DF investigation of sensor networks is very complex and involves diverse levels. Recent literature have been studied to design an analogy between the real-life and simulated DF investigation processes [14,24–26,39–44]. This analogy will help the researchers and practitioners in the DF field to relate reconstructed simulation events to real-life scenarios. Furthermore, it will enable the and practitioners to study, analyze, and investigate different BH attack scenarios in a simulation environment as compared to conducting or replicating the attack in a physical system. Figure 3 incorporates an analogy of the real-life DF investigation process and a simulated DF investigation process corresponding to the DF investigation life-cycle for WSN and IoT.

The central segment of the DF investigation life-cycle in Figure 3 contains the types of DF and corresponding types of DF operation and phases. The comparison comprises device-level, network-level, and cloud-level forensics on both sides. There are three columns included for the investigation procedure, given as expected DE, device, and media from where it can be captured, and DF tools for corresponding DE examination at three levels. The right side of Figure 3 contains a mirror image of the real-life DF investigation process in the simulated environment with their corresponding tools. A layer-to-layer relation of the TCP/IP protocol suite and NS3 simulation layer model of this research is also given in the figure. The gray boxes and circles in Figure 3 represent the relevant part of this research.

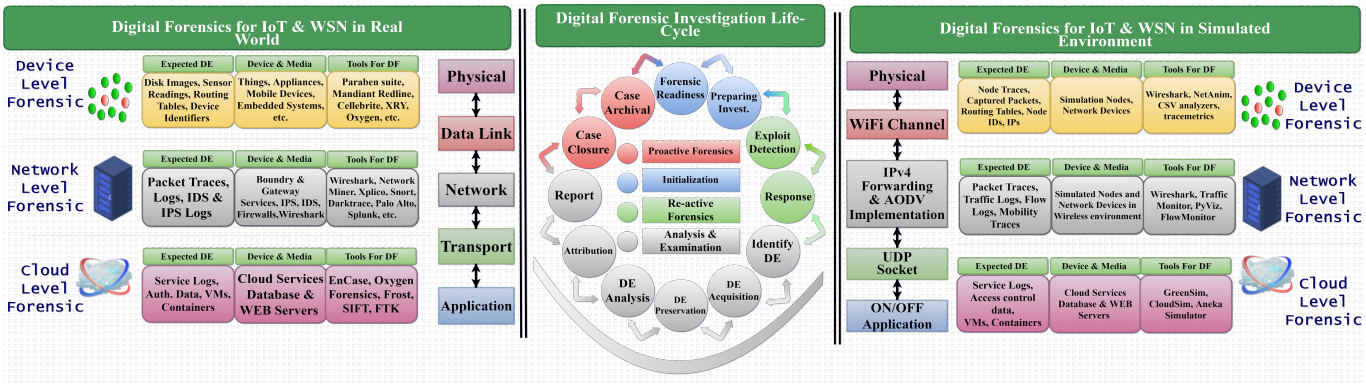

Figure 3. Analogy between real-life DF process and simulated environment.

4. Simulation and Results

This section includes the details of simulation environment, parameters, and their description. Moreover, it discusses the analysis of the outcomes of simulation. NS 3.30 on the Ubuntu 19.04 operating system on a 64-bit processor is used for the simulation of the network(s). Table 2 contains comprehensive information about the simulation environment parameters. Multiple types of networks are simulated with a variety of parameters in order to verify the findings of forensic analysis. The first value in Table 2 against every parameter is the network under the BH attack, which is briefly analyzed. The variations in the values are intended to verify the analysis. The critical point of the implementation is that it defines the behavior of the attack in the routing model of AODV. The mobile nodes in the network adopt a random way-point mobility model. The network converges in the first 100 s, and then it starts data transmission. Then the attack starts randomly. This means that the behavior of the attack is defined only in the source code of the AODV model. The random nodes in the network will drop packets. This work analyzes the traffic traces, the behavior of the AODV routing protocol, and the variations in the traffic patterns under the BH attack. This behavior of the network under the attack helps to follow the forensic activities thoroughly. At the start, it is not known which specific nodes or flows are going to be malicious. Therefore, a deep inspection is needed to reveal that what happened to the performance of the network. The point of interest is the time of the attack, the behavior of the AODV protocol under attack, the traffic variations due to the attack, the packet loss ratio, the end-to-end delay, the throughput, and the transmission volume. After the analysis of the attack, interesting facts about the behavior of the protocol under attack are discovered and verified by implementing different types of networks with variation of parameters and network environments. The network simulation runs for 200 s, and after completion of the simulation various types of output files are generated for analysis, such as CSV, Flow Monitor, trace, PCAP, and XML files of the simulation.

The graph of the simulation is plotted by the GNUPLOT of NS3. The .tr files are analyzed by Tracemetrics, which is an analysis tool for NS3. PCAP files are analyzed by Wireshark, which is a famous network packet analyzer tool. The XML trace file of the simulation and flowMon files are analyzed by NetAnim.

Table 2. Setting Simulation Environment.

	Simulation Setup
Parameters	**Values**
Nodes	50 & variable
Sink nodes	10 & variable
Mobility Model	Random WayPoint & Constant Position
Position Allocator	Random Rectangular Position Allocator
Protocol	AODV
Time	200 (s)
Loss Model	Friis
MAC Protocol	IEEE 802.11b
Bits/s	20
Mode	ad hoc Mobile & ad hoc Static & Traditional WSN
Propagation	Constant Speed Propagation Delay
Power	7.5 dBm
Wifi Rate	2 Mb/s
Area	300 × 1500 m

4.1. Analysis of Simulation Outcomes

This subsection briefly discusses and analyzes the simulation results of the BH attack. The pros and cons of AODV in terms of DF investigations are also considered. This may employ the other reactive routing protocols as well. The network simulation traces and the traffic flows between the nodes are analyzed to observe the traffic behavior. Then, a postmortem analysis of the attack and the hierarchy of packets in the network is conducted. It is of crucial importance to understand the route discovery process in the AODV protocol to analyze the traffic generated in the network. There are four kinds of packets used in the routing process: the route request (RREQ), route reply (RREP), HELLO, and route error (RERR) packets. The RREQ and RREP packets are used for route discovery. The RERR and HELLO packets are used for route preservation in case of any abnormality.

4.1.1. Analysis of the Flow Monitor Trace File

The Flow Monitor operates on the IP layer and measures several parameters. It is designed using a modular approach. The network probes for Flow Monitor are of four types.

- Packet sent by the source node (SendOutgoing IPv4 and IPv6 traces)
- The packet is forwarded by a node (UnicastForward IPv4 and IPv6 traces)
- Packet received (LocalDeliver IPv4 and IPv6 traces)
- Packet dropped (Drop IPv4 and IPv6 traces)

The data composed for every flow are given in Figure 4. The flow IDs are 6 and 7. Now, we discuss flow ID 7. It is generated from the IP address 10.1.1.12 (node 13) to the IP address 10.1.1.2 (node 3), and the UDP port used is 49,153. There are 397 packets transmitted to node 3 from node 13 and 232 packets out of 397 get dropped by the BH nodes. Only 257 packets are received by the destination node. It is observed that the summation of lost and received packets is greater than the total transmitted packets. This occurs because Flow Monitor intercepts packets at IP level, and packets queued at a lower level than IP at the end of the simulation are considered lost. Packets in this flow are forwarded 1074 times. 160 packets are dropped due to the fragment timeout, and 10 packets are dropped due to the absence of a route. Other data parameters are transmission and receive bit-rate, mean delay, packets loss ratio, the number of packets transmitted, received, and lost, time for the first and the last packet transmitted and received, etc. Two types of network devices are installed on each node: the Wifi NetDevice and the loopback NetDevice. The loopback device has the IP address 127.0.0.1 on each node and is used for testing purposes.

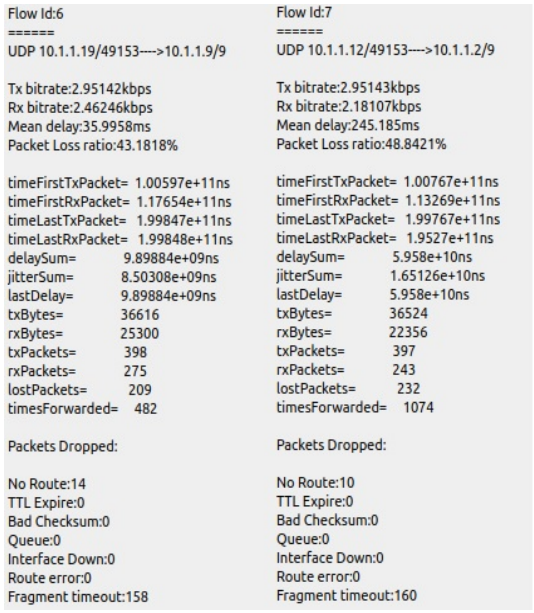

Figure 4. NetAnim Image of the Flow IDs.

A large number of flows are observed in the flowMon file. The total number of flows is 950. The details of each flow cannot be discussed due to the restriction of space, so the data of each flow is fetched one by one to compose a table and CSV files to plot that data. The graphs show the variations of traffic patterns regarding their Flow IDs. Table 3 contains some of the flows selected upon the basis of the variations in the loss ratio and colored with respect to the PLR variations. The dark red flows depict a loss ratio greater than 70%, blue flows depict loss ratio less than 70% and greater than 40%, and green flows depict loss ratio less than 40%. The cumulative packets loss ratio is 28.789% for all flows. Some flows have 100% packets loss, some have 0% packets loss, and some have a packets loss in between these numbers. The total number of packets transmitted was 10,693, the total number of received packets was 7621, and the total number of lost packets was 3072. We calculate the cumulative loss of the flows and compose CSV files of the data to plot the graph. Python is used to plot graphs of the data.

Table 3. Table of Flow IDs data.

Flow ID	Nodes	Txpackets	Rxpackets	Lost Packets	PLR (%)
1	14 to 4	399	159	240	60.15%
2	10 to 0	398	125	273	68.60%
3	13 to 3	398	114	284	71.35%
4	12 to 2	398	51	347	87.18%
…	…	…	…	…	…
23	18 to 8	397	194	203	51.34%
24	18 to 8	396	108	288	72.72%
25	18 to 8	396	112	284	71.71%
…	…	…	…	…	…
948	40 to 9	4	3	1	25%
949	30 to 29	2	2	0	0.0 %
950	25 t0 32	3	3	0	0.0 %
Total	————	**10,693**	**7621**	**3072**	**28.729%**

Figure 5 depicts the statistics of all 950 flow IDs concerning their number of packet transmissions. The initial bars show that the packets transmission rate is up to 400 packets per flow ID. However, it then severely declines due to the BH attack.

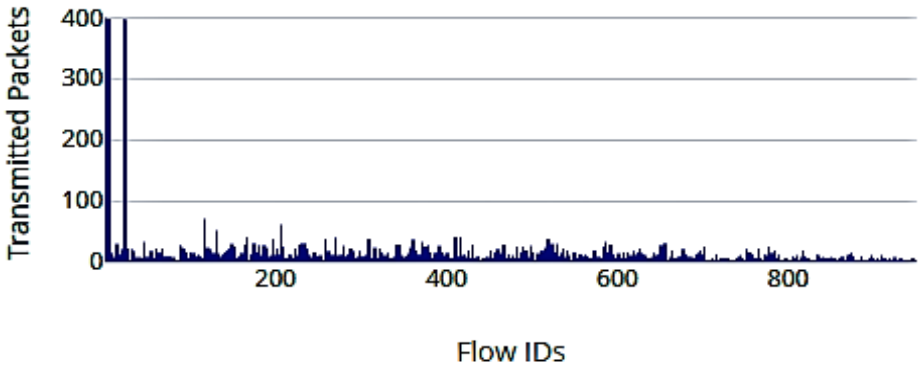

Figure 5. Packets transmitted.

Figure 6 contains the information about the received packets from all flow IDs. Due to the directly proportional relationship to transmission rate, the number of received packets is up to 200 for initial flow IDs, and then this number also declines. We can see that it keeps varying throughout the process but never touches the highest again.

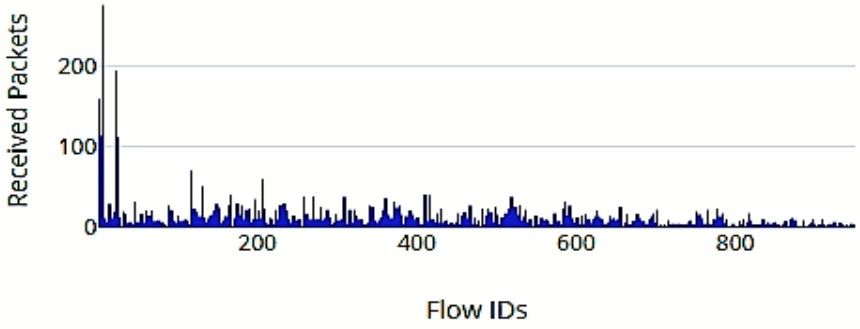

Figure 6. Packets Received.

Figure 7 depicts the number of lost packets. At the start, the packet loss is high in terms of the number of packets. It almost hit 400 packets per flow at the worsening state of attack. As we have observed, the pattern of the traffic in the past two graphs, the number of packets declines in the network communication but the ratio of sent to lost packets does not decline as per the pattern, which is depicted in the next graph. Therefore, when the transmission packets number declines, the received packets and lost packets numbers also decline.

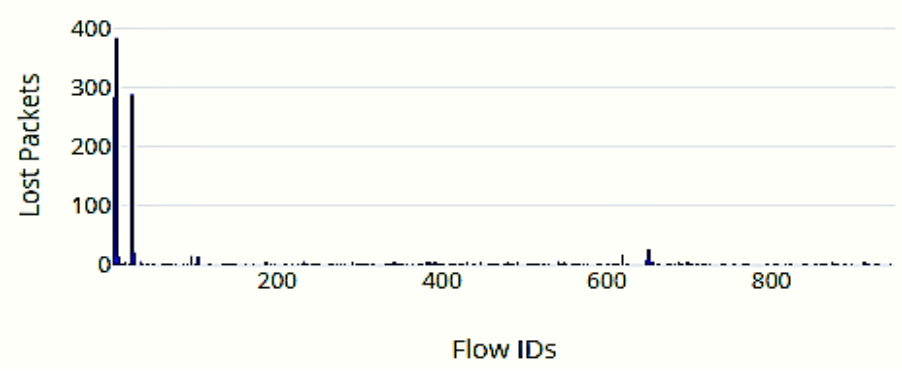

Figure 7. Number of packets lost.

Figure 8 shows the packet loss ratio (PLR) of all flow IDs from ID 1 to 950. The line graph frequently touches the maximum, when there is a 100% packet loss for a flow ID. The PLR is given as a percentage. We have many flows in which not even a single data packet is received by the destination IP. The PLR is 100% repeatedly throughout the axis. Furthermore, some of the flow IDs have PLR 0%. From the previous graphs, it is observed that the number of packet transmissions declines when the attack starts. Although the number of packets declines, but the damage scale of the BH remains the same until the end. In some flows, the number of the transmitted packets is very low, and they are all dropped by the BH nodes and lost. Therefore, the PLR hits the hundred-percent scale-point for several flow IDs. An excessive decline in the number of transmitted packets created a flood of AODV control packets in the network. We analyze the behavior of the attack on the IP layer of the network.

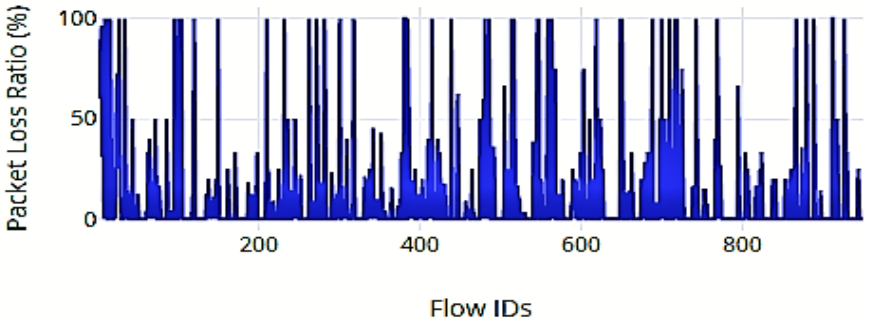

Figure 8. Packets Lost Ratio.

The number of all flows is 950, but when we run the network simulation without an attack in the normal state, the flows are only 371, and the total number of the transmitted packets is 2316. The BH attack caused a massive boost in the control traffic of the network and choked the network traffic, so the number of flows increased exponentially. AODV is an on-demand and reactive protocol, and the routes are demolished after use or due to some abnormality. Therefore, the attack caused the extensive flow of AODV control packets in the network, affecting the cumulative performance and energy.

4.1.2. Analysis of the PCAP Files

Wireshark works by putting the network interface card (NIC) into a promiscuous mode, and it tells NIC to accept every packet it receives. It helps to analyze the traffic patterns in real-time.

Figure 9 shows the packets captured at node number 5 and their sender and receiver IP addresses. We can observe that the senders broadcast RREQs to 10.1.1.255 (Network) and other packets to the nodes. We have included communication of only one node due to the restriction of space.

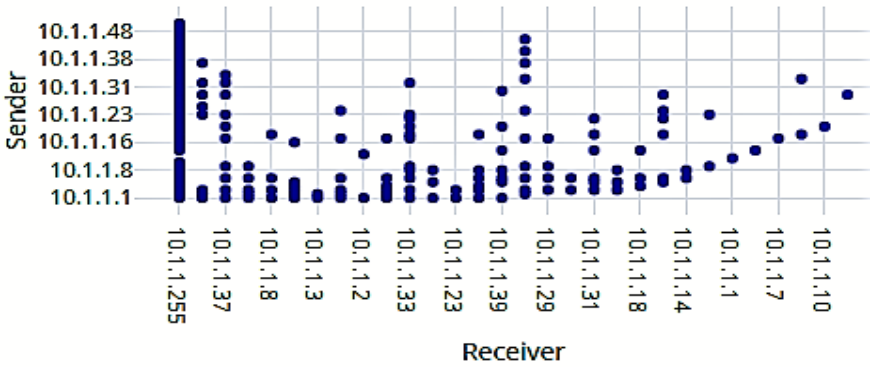

Figure 9. Communication at Node 5.

We analyzed the 50 PCAP files of all nodes and examine their network protocol hierarchy and conversations patterns. We plotted the nodes' I/O graphs over time and analyzed the behavior of attack at the nodes level. We analyzed the behavior of attack at the network IP level in the previous Flow Monitor part. All PCAP files were merged to compose one combined file and then plot a graph of that file. Another reason for doing this is the similar behavior of all malicious nodes with respect to time, because the traffic pattern at those nodes is almost the same.

We can observe the number and hierarchy of User Datagram Protocol (UDP) data and AODV packets from Figure 10. Their comparison shows that AODV control packets are far greater in numbers than data packets. The BH attack creates chaos in the network, which causes exponential growth in control packets traffic, causing damage to the cumulative performance of the network. From Figure 11, we observe traffic patterns of the packets captured at all nodes and their protocol hierarchy. The first 100 s is the network convergence time, so there is no traffic of data packets till this time except a little traffic of protocols' control packets. After that, the data packets' transmission starts and eventually tries to grow in the network. However, the BH attack starts and affects the performance of the network. Now, an interesting pattern is observed. The attack causes a major flood of AODV control packets in the network, almost threefold to the data packets. This creates an immense network overhead, and then the damage reaches its maximum at the time span from 130 to 140 s, where the data packets decline to 0 packets per s. This is the worst situation. The BH attack behaves like a smurf attack and affects the end-to-end delay and efficiency of the network. In this time period, the attack is at its extreme extent. Again, similar behavior is observed from span 160 to 170 s, where data packets declined. Therefore, the AODV protocol behaves in an "up and down" manner. It tries to re-establish routes again, but the BH again causes the same result. As the attack takes place no matter the scale, it disturbs the long-term performance of the network.

Protocol	Percent Packets	Packets	Percent Bytes
▾ Frame	100.0	456656	100.0
▾ IEEE 802.11 wireless LAN	100.0	456656	27.2
▾ Logical-Link Control	70.0	319498	71.1
▾ Internet Protocol Version 4	65.7	299827	18.1
▾ User Datagram Protocol	65.4	298837	7.2
Data	23.5	107152	20.7
Ad hoc On-demand Distance Vector Routing Protocol	42.0	191685	11.8
Internet Control Message Protocol	0.2	990	0.1
Address Resolution Protocol	4.3	19671	1.7

Figure 10. Protocol Hierarchy of all protocols' packets .

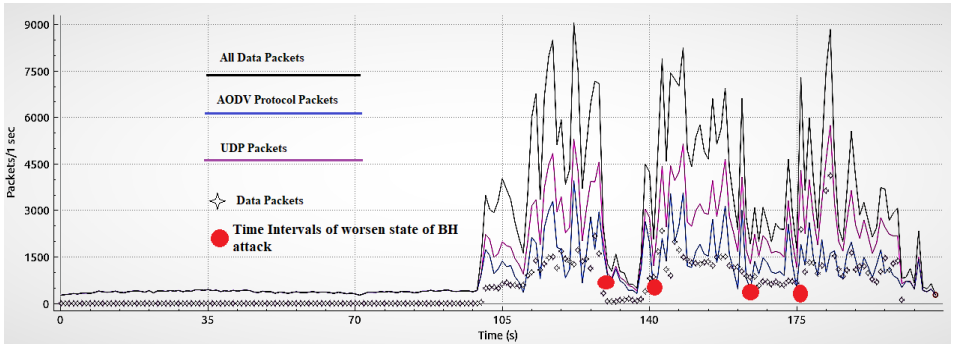

Figure 11. I/O Graph of the merged PCAP file.

4.1.3. NetAnim Traces

The NS3 network simulation is animated by NetAnim using an XML trace output file. Different sorts of statistics can be found, such as node activities regarding protocol characteristics, data transmission, and the types of data transmission. We extract the data of the UDP traffic from the animator to plot the graphs. Then we analyze the node-to-node

UDP data transmission. The graph in Figure 12 contains only the data transmissions of UDP. These flows only show the data flows that are intended from a sender to the receiver nodes.

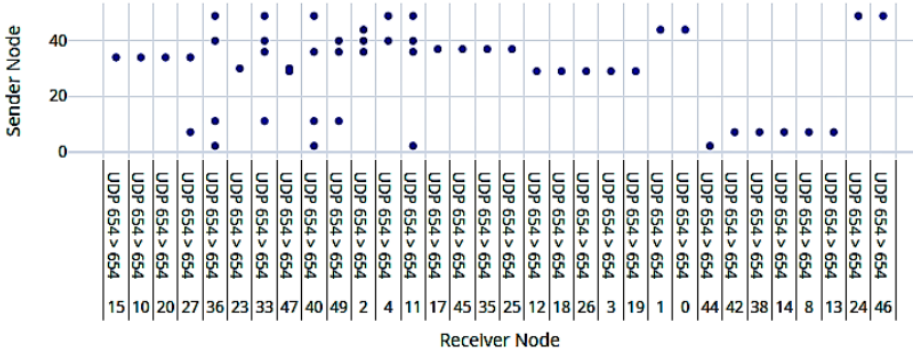

Figure 12. UDP Data Transmission.

Figure 12 shows that almost all nodes have communicated with one another by using UDP port number 654. The blue points scattered in the graph show this information. It can be observed from the graph that some nodes have not sent any data, i.e., node 20, 21, and 49, although they have received some.

Figure 13 depicts the stats of AODV RREPs of the nodes in the network. We can observe that node 49 has sent seven route replies. Now, as shown in the graph in Figure 12, it did not forward any data packet to the other nodes. Therefore, it is possible to detect the BH node from the ratio of RREP packets it publishes to the data packets it forwards.

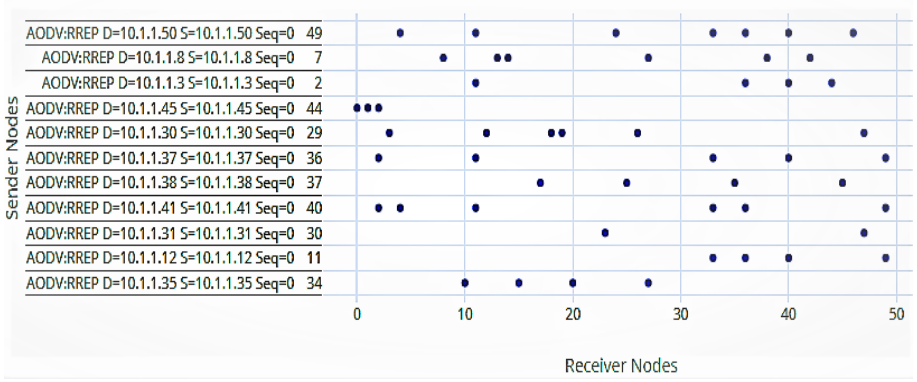

Figure 13. AODV Route Replies.

4.1.4. Little's Law Results

Tracemetrics is a useful tool to perform a rapid analysis of the trace file produced by NS3 simulations and compute useful metrics for performance measurement and research purposes. We extract Little's values from the trace (.tr) file by using Tracemetrics.

Figure 14 illustrates of the results of Little's theorem. We plot a graph of the arrival rate values of the packets at the specific nodes per unit time. This informs us about the busy nodes in the network. The X-axis contains the specific node number, and the Y-axis contains the arrival rate value of the node per unit time. The busy nodes can be easily observed in the graph.

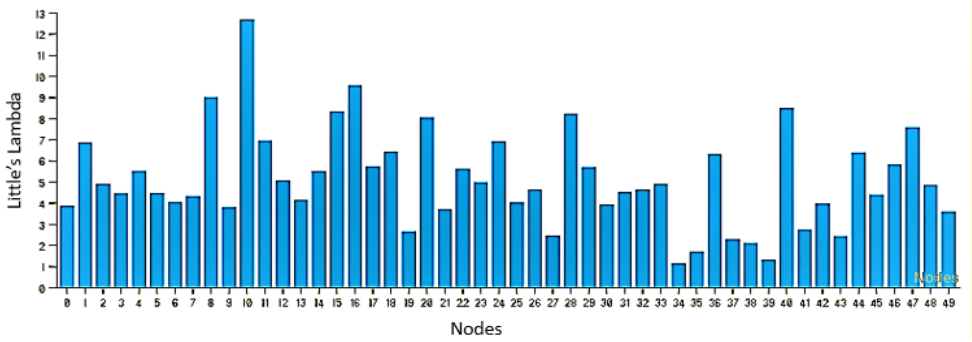

Figure 14. Little's results of the nodes

4.1.5. Throughput and Goodput of Nodes

Figure 15 contains an analysis of the throughput and goodput of the network. These results are also extracted through Tracemetrics. We can clearly observe the throughput-to-goodput ratio of the nodes. Throughput is the measurement of the amount of all data flowing through a node or link, while the goodput is the measurement of only useful data.

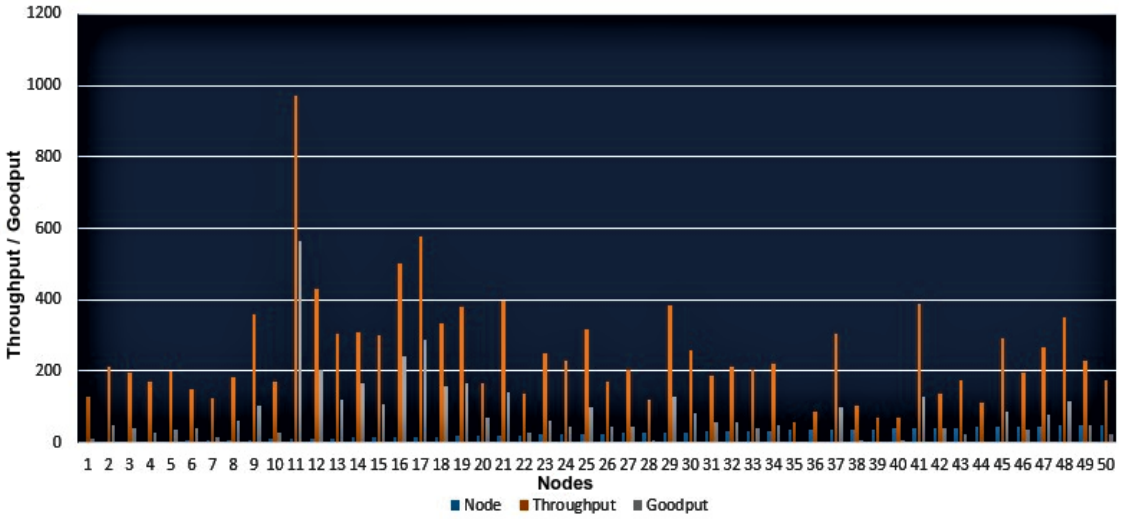

Figure 15. Throughput and Goodput.

4.1.6. Cumulative Performance Comparison of the Network with and without BH Attack

When the simulation ends, a CSV file is generated, which contains the record of the rate of packets received with respect to the simulation time, which is in seconds. We can use GNUPLOT to plot the graph of the file.

Figure 16 depicts the graph of the standard network without attack and normal functioning. We can observe the simulation unit time (in seconds) on the X-axis and the rate of packets received per unit time in the network on the Y-axis. The purple line is for the receive rate, and the green line is for the total number of the data packets received. The packets received is the cumulative number of packets received in the network till the specific time. It is always greater than the receive rate as it is the sum of the received packets at a given time.

Figure 17 is plotted from the remnants (CSV) of the same network under the BH attack. We can see that the transmission begins from the 100th second of simulation and then shows variations. However, as we have analyzed earlier from the PCAP files, the attack was most detrimental at the period of 135 s to 145 s. We can see that the receive rate of the data packets dropped to zero in that phase. The Wireshark outputs have also depicted the similar behavior for data packets, which is shown in Figure 11. Therefore, these results also validate previous ones.

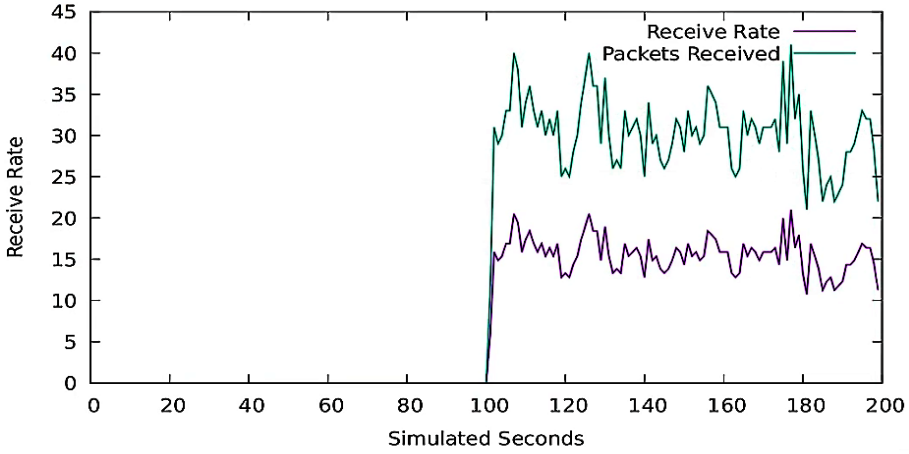

Figure 16. The stats in the normal network.

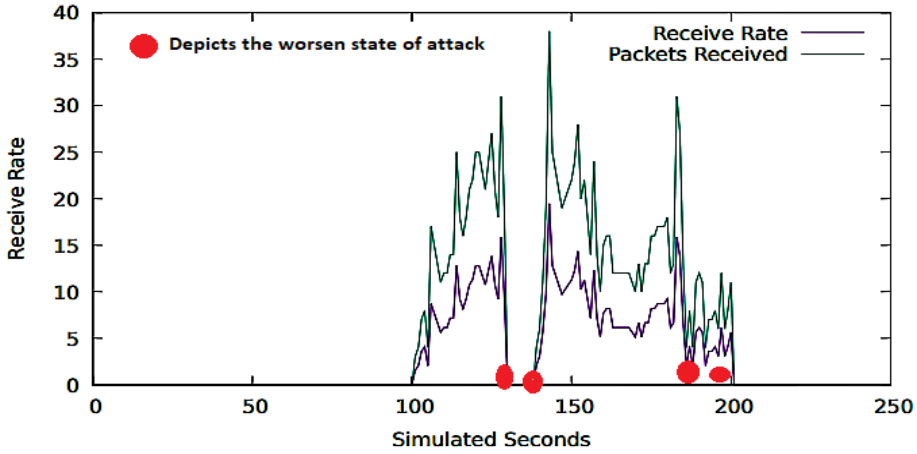

Figure 17. The stats in the network under attack.

4.1.7. PyViz Visualization Results

PyViz is an NS3 tool for live visualization, as it does not use any type of traces. It demonstrates the nodes dropping packets and the working of the mobility models in real time. We can analyze the behavior of the nodes from the number of packets the node received and the number of packets transmitted. If a node transmitted messages much less than it received, it means that there is something abnormal with it.

It can be observed from the stats of node 5 in Figure 18 that it has received 2144 data packets and transmitted only 497 packets to other nodes. This means that it discarded around about 1650 packets. The node discarded almost 76 percent of its packets. The node 22 has also shown similar behavior. We can visualize the actual network traffic pattern and positioning of nodes via PyViz and also in the live DF tools. However, we cannot identify which specific packet is being dropped due to the BH attack or any other node or network malfunction. It is observed from the live visualization that the physical and logical position of the BH nodes in the network has a great impact on the cumulative performance of the network as well. If a BH node can publish RREP to more and more nodes, it can damage the network severely. It is also observed from the PyViz that the increasing and decreasing total number of nodes and the number of malicious nodes have a great impact on the performance of the network as well. This is briefly discussed and verified in Section 4.1.8 with the reconstruction of different networks under different circumstances.

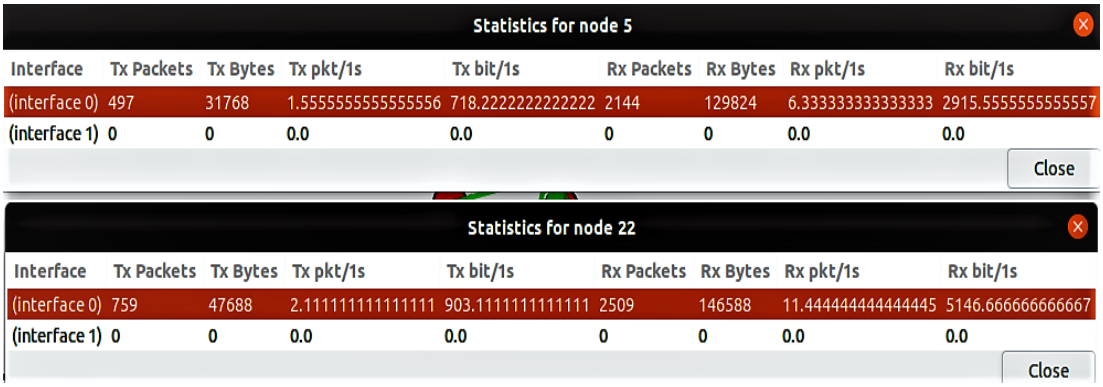

Figure 18. PyViz Visualization.

4.1.8. Discussion and Verification of Results

A mobile environment for 50 sensor nodes was simulated, and the behavior of a BH attack is defined in the model of the NS3 AODV routing class. The malicious behavior was not assigned to any node by default. Some nodes randomly acquired the malicious behavior because the approach aimed to forensically analyze the behavior of the network and the traffic in the presence of an attack. A significant portion of the network nodes were observed to behave maliciously.

The different types of traces from the simulated environment and live statistics of the simulation are analyzed and discussed in the PyViz. Some exciting challenges for this domain are discovered. For example, forensics investigations for these networks are very challenging because sound artifacts are difficult to obtain due to broadcast, resource-constrained, and fragile environments. Mobility induces data corruption. The network forensics for WSN and IoT is hideous because the DE that can be found from the data communication traces is insubstantial and can disappear quickly. The resource-constrained nature of the wireless devices may also vary the stability of traces.

Traditional DF mechanisms may be applied at device-level investigations but not for network traffic forensic, especially in the presence of reactive routing protocols. The reactive forensic is challenging for this purpose because solid DE is difficult to obtain from the network traffic artifacts. At the routing protocol level, we have also discovered some interesting facts related to DF investigations. Reactive routing protocols are not compatible or suitable for DF investigations due to their on-demand behavior, i.e., AODV. Routes are established on demand and demolished after their use, so we cannot have any useful route information from the routing tables. The source nodes transmit HELLO packets for route preservation in AODV. The RERR message presents the unreachable destination. Message-receiving nodes inactivate the existing route toward that destination. In the case of intense and cooperative behavior of the attack, the constant growth and load of protocol control packets can jam the cumulative performance of the network, affecting the energy. As the network size grows in terms of number of nodes, the chances of collecting useful DE declines. As the BH attack goes into a worsening state, it also behaves like a smurf attack, which is also a type of DoS. We have noticed this in the PCAP analysis in Figure 11, where the data packet transmissions has fallen to 0, but the AODV control packets were not.

For the sake of argument, let us assume that if we develop a mechanism for all network nodes to submit each routing table or routing information to a third party node or a BS, then the on-demand protocols will then also produce a large amount of control traffic to find, sustain, and maintain routes, especially in mobile networks where the position of the nodes is continuously varying. Therefore, the networks using on-demand or reactive routing protocol are not suitable to produce forensically useful data, especially in the case of adverse attacks. The case may become more complicated with the increasing time-span of the attack. On the other side, the AODV self-healing quality is appreciable, as we have observed from the graphs in the Figures 11 and 17.

There are also some essential aspects of the research such as the physical topology, strategic positioning, and cooperation of the network nodes. From the past literature, especially in the mitigating schemes, the damage to the network by the attack has usually been shown to be directly proportional to the number of malicious nodes in the network, but this is not always true. We have found that a lower number of malicious nodes occupying important locations can cause more damage than a high number of malicious nodes that are randomly settled. This can be observed in Tables 4–6. A node that publishes fake routes to a significant number of source nodes can cause multiple types of damages to the network. In AODV, if we give responsibility to the nodes for detecting and preventing the attacks, it may work well for that specific aim but will cause an increased average end-to-end delay. We have found that it is challenging to analyze the selective behavior of the attack from the analysis of traffic in the network and packets captured at nodes. If the attack is aimed for an extended period but within small time intervals, we would not be able to identify if the packets are dropped due to the BH attack or transmission errors.

Table 4. Comparative Analysis of WSN (ad hoc).

Outcomes	Tx	Rx	Lx	PDR	PLR	DL	E2E DL	Th
Mobile (Normal)	2316	2106	210	90%	10%	0.01	1.03	88.03
Mobile (Attack)	10,676	7604	3072	71%	29%	0.051	6.6	31.49
Mobile (35 Nodes) (Attack)	3612	2737	875	75%	25%	0.03	14.6	13.81
Static (Attack)	7882	7137	745	90%	10%	0.03	4.67	37.95

Tx	Transmitted	E2E DL	End to End Delay (s)
Rx	Received	TH	Throughput (bps)
PDR	Packet Delivery Ratio	PLR	Packet Loss Ratio
Lx	Lost	DL	Delay (s)

Table 5. The Stats of the Static Network Under Attack.

Total	Mal	Tx	Rx	Lx	PDR	PLR	DL	E2E DL	TH
50	10	14,383	9742	4641	67%	33%	0.09	9.42	41.99
	14	17,778	12,762	5017	70%	30%	0.08	8.19	53.12
	15	13,435	9882	3553	73%	27%	0.08	8.19	42.12
	19	11,888	8865	3023	74%	26%	0.10	11.61	38.00
	20	12,844	9913	2950	76%	21%	0.09	9.71	44.01
	25	10,803	8732	2071	79%	21%	0.08	9.75	34.06
	26	11,050	8996	2054	79%	21%	0.08	9.3	35.01

We also set up networks with different modes of physical topology with the variations in the number of malicious nodes to verify the findings of our analysis.

Table 4 depicts the statistics computed from Flow Monitor for the ad hoc networks in mobile and static modes. The first network is in the normal state, and its graph of data packets is presented in Figure 16. This network has only 371 flows in a normal state, and the number of flows increases to 950 during a BH attack. The second network is the same, which we briefly analyzed under the BH attack in this paper. We can see the number of packets in the network exponentially grew due to the extensive number of control packets. The PLR, average E2E delay, and throughput are affected by the attack. The third network is the same as above, but we decreased the number of total number of nodes to 35 from 50. We did this to check the random behavior of the attack in a smaller number of nodes. Therefore, the PLR decreased and the E2E delay increased. In the end, the same ad hoc

network in the static mode under BH attack is given. The PLR is lower, but the average E2E delay, throughput, and several control packets are affected.

Table 6. Comparative Analysis of the Number of Malicious Nodes in Mobile WSN

Total	Mal	Tx	Rx	Lx	PDR	PLR	DL	E2E DL	TH
50	10	9150	7310	1840	79%	21%	0.13	19.06	39.24
	11	4654	3125	1529	67%	33%	0.16	53.71	23.08
	13	10,092	8231	1861	81%	17%	0.13	16.25	37.97
	14	5583	4166	1417	74%	26%	0.14	33.94	26.51
	15	4984	3707	1277	74%	26%	0.14	40.21	19.04
	19	4911	3601	1310	73%	27%	0.14	38.97	19.85
	20	4275	3279	996	76%	24%	0.13	39.10	18.36
	21	5081	3669	1412	72%	28%	0.14	40.75	16.95
	24	2724	2036	688	74%	26%	0.11	55.79	13.92
	25	3524	2777	747	78%	22%	0.11	40.49	16.792

We have reconstructed two other WSN environments with variation in parameters to verify the forensic analysis of this research. Tables 5 and 6 contain the statistics of static and mobile WSN under BH attack, respectively. We vary the number of malicious nodes in the network to observe the behavior of the protocol and network under BH attack. A small change in the number of malicious nodes, selection of specific nodes for malicious activity, specific position of the malicious node, specific grouping between nodes for malicious activity, and environmental mode of the network has a decisive impact on the cumulative performance of the network, which we can observe from the both tables. The variations in the number of malicious nodes in Table 5 from 10 to 14, 14 to 15, and 15 to 19 significantly impacted the total number of transmitted packets, further extending the effect on PDR and PLR. Similar behavior can also be observed from Table 6. The fluctuations in the depicted metrics with the variation of above mentioned parameters verify our analysis.

Keeping in view the analysis and discussion, we suggest designing pro-forensic network routing protocols and wireless infrastructures. Those protocols use a combined approach of reactive and proactive routing, in which abnormal criteria could be defined for traffic in the network and on the nodes according to the nature and responsibilities of the network. A DE collector can be established. Any specified abnormality detected could be submitted to the DE collector with all the records that could be helpful for DF investigations. The abnormality-driven DE collection approach would not only diminish the extra consumption of computational resources of the network, but it would also lessen the burden of a forensic investigator by presenting the useful DE in advance. This will be investigated in our future work in this domain.

5. Conclusions

The proliferation of WSN and IoT in many application domains has also triggered cybersecurity threats associated with these networks. In this paper, we have analyzed the blackhole attack in WSN and IoT by inspecting the traffic generated by these networks. We have analyzed different kinds of traces by different tools. We have simulated the attack in NS3 and performed a postmortem analysis of the internet protocol (IP)-level traffic in the network and on nodes by traffic monitoring tools such as Flow Monitor and Wireshark, and we have analyzed the XML traces by NetAnim. We have examined and explained the detrimental level of the attack for WSN/IoT, especially in the case of mobility. Finally, we have critically discussed the problem domain in light of this research and by verifying its findings. The DF for WSN and IoT still has many open challenges at the device and network levels. An important future research direction could be the investigation

of different proactive and reactive routing protocols for WSN and IoT that could help to design a pro-forensic routing protocol and DE collection framework for WSN and IoT.

Author Contributions: Conceptualization, A.H., M.A.K., B.S., A.M. and Z.A.; Data curation, A.H., B.S. and A.M.; Formal analysis, A.H.; Funding acquisition, M.A.K. and Jawad Ahmad; Investigation, A.H., B.S. and A.M.; Methodology, A.H., B.S. and A.M.; Project administration, M.A.K., B.S., A.M., A.W.M. and J.A.; Resources, M.A.K.; Software, A.H. and M.A.K.; Supervision, M.A.K., B.S., A.M., A.W.M. and Z.A.; Validation, A.H., M.A.K. and A.M.; Visualization, M.A.K.; Writing–original draft, A.H. and B.S.; Writing–review & editing, A.H., B.S. and A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: There is no data associated with this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

6LoWPAN	Low-Power Wireless Personal Area Networks
AODV	Advance On-Demand Distance Vector Routing Protocol
AOMDV	Advance On-Demand Distance Vector Routing Protocol (Multi- path)
BH	Blackhole
BS	Base Station
CH	Cluster Head
CP	Control Packets
CRCMD&R	Cluster Reputation-based Cooperative Malicious Node Detection & Removal
CSV	Comma-Separated Values
DDoS	Distributed Denial Of Services
DE	Digital Evidence
DF	Digital Forensics
DL	Delay
DoS	Denial Of Services
E2EDL	Average End to End Delay
EDRI	Extended Data Routing Information
IAS	Intrusion Avoidance System
ID	Identity
IDS	Intrusion Detection System
IDS	Intrusion detection system
IoT	Internet Of Things
IPv4/Ipv6	Internet Protocol version 4/6
LV	Legitimacy Value
MAL	Malicious
MANET	Mobile Ad hoc Networks
MITM	Man-In-The-Middle-Attack
NASF	Non Address Spoof flooding
NIC	Network Interface Card
NS3	Network Simulator 3
OS	Operating System
PCAP	Packet Captured file
PDR	Packets Delivery Ratio
PLR	Packets Lost Ratio
RAM	Random Access Memory
RERR	Route Error
RNG	Random Number Generator
RREP	Route Reply
RREQ	Route Request
SAD	Smart Attack Detection

SDT	Secure Data Transmission
TH	Throughput
Tx/Rx/Lx	Packets Transmitted/Received/Lost
UDP	User Datagram Protocol
VN	Virtual Network
WSN	Wireless Sensor Network
XML	Extensible Markup Language

References

1. Kansakar, P.; Munir, A. A Two-Tiered Heterogeneous and Reconfigurable Application Processor for Future Internet of Things. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Hong Kong, China, 8–11 July 2018.
2. Munir, A.; Gordon-Ross, A.; Ranka, S. Multi-core Embedded Wireless Sensor Networks: Architecture and Applications. In *IEEE Transactions on Parallel and Distributed Systems (TPDS)*; IEEE: Piscataway, NJ, USA, 2014; Volume 25, pp. 1553–1562.
3. Karakaya, A.; Akleylek, S. A survey on security threats and authentication approaches in wireless sensor networks. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–4.
4. Gurunath, R.; Agarwal, M.; Nandi, A.; Samanta, D. An Overview: Security Issue in IoT Network. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018; pp. 104–107.
5. Sezer, S. T1C: IoT Security:-Threats, Security Challenges and IoT Security Research and Technology Trends. In Proceedings of the 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, USA, 4–7 September 2018; pp. 1–2.
6. Ali, S.; Khan, M.A.; Ahmad, J.; Malik, A.W.; ur Rehman, A. Detection and prevention of Black Hole Attacks in IOT WSN. In Proceedings of the 2018 3rd International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; pp. 217–226.
7. Surange, G.; Khatri, P. IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; pp. 909–913.
8. Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Gener. Comput. Syst.* **2021**, *120*, 13–25. [CrossRef]
9. Sagarwal, N. IoT Forensics: Interconnection and Sensing Frameworks. In *Digital Forensics and Internet of Things: Impact and Challenges*; John Wiley & Sons: Hoboken, NJ, USA, 2022; pp. 237–254.
10. Castro, A.; Perez-Pons, A. Virtual Assistant for Forensics Recovery of IoT Devices. In Proceedings of the 2021 7th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity), Conference on High Performance and Smart Computing, (HPSC) and Conference on Intelligent Data and Security (IDS), New York, NY, USA, 15–17 May 2021; pp. 186–190.
11. Glabbeek, R.; Höfner, P.; Portmann, M.; Tan, W.L. Modelling and Verifying the AODV Routing Protocol. *Distrib. Comput.* **2016**, *29*, 279–315. [CrossRef]
12. Reddy B, P.; Reddy B, B.; B, D. The AODV routing protocol with built-in security to counter blackhole attack in MANET. *Mater. Today Proc.* **2021**, *50*, 2214–7853.
13. Anamalamudi, S.; Sangi, A.R.; Alkatheiri, M.; Ahmed, A.M. AODV routing protocol for Cognitive radio access based Internet of Things (IoT). *Future Gener. Comput. Syst.* **2018**, *83*, 228–238. [CrossRef]
14. Karabiyik, U.; Akkaya, K. Digital Forensics for IoT and WSNs. In *Mission-Oriented Sensor Networks and Systems: Art and Science*; Springer: Cham, Swizterland, 2019; Volume 164, pp. 171–207.
15. Shreenath, K.N. Black Hole Attack detection in Zone based WSN. *Int. J. Recent Innov. Trends Comput. Commun.* **2017**, *5*, 148–151.
16. Kaur, T.; Kumar, R. Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol. In Proceedings of the 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 12–15 August 2018; pp. 288–292.
17. Johnson, A.; Molloy, J.; Yunes, J.; Puthuparampil, J.; Elleithy, A. Security in Wireless Sensors Networks. In Proceedings of the 2019 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2019, Farmingdale, NY, USA, 3 May 2019; pp. 1–3.
18. Dorri, A. An EDRI-based approach for detecting and eliminating cooperative blackhole nodes in MANET. *Wirel. Netw.* **2016**, *23*, 1767–1778. [CrossRef]
19. Sharma, S.; Gambhir, S. CRCMD & R: Cluster and Reputation based cooperative malicious node Detection Removal scheme in MANETs. In Proceedings of the 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 5–6 January 2017; pp. 336–340.
20. Kaurav, A.; Kumar, K.A. Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2.35 Simulator. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2017**, *2*, 717–722.
21. Ananthi, J.V.; Vengatesan, S. Detection of various attacks in wireless adhoc networks and its performance analysis. In Proceedings of the 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 23–24 November 2017; pp. 754–757.

22. Elmahdi, E.; Yoo, S.; Sharshembiev, K. Securing data forwarding against blackhole attacks in mobile ad hoc networks. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 463–467.
23. Sbai, O.; Elboukhari, M. Simulation of MANET's Single and Multiple Blackhole Attack with NS-3. In Proceedings of the 2018 IEEE 5th International Congress on Information Science and Technology (CiSt), Marrakech, Morocco, 21–27 October 2018; pp. 612–617.
24. Kruger, J.L.; Venter, H. Requirements for IoT Forensics. In Proceedings of the 2nd International Conference on Next Generation Computing Applications (NextComp), Mauritius, 19–21 September 2019; pp. 1–7.
25. Chernyshev, M.; Zeadally, S.; Baig, Z.; Woodward, A. Internet of things forensics: The need, process models, and open issues. *IT Prof.* **2018**, *20*, 40–49. [CrossRef]
26. MacDermott, A.; Baker, T.; Shi, Q. Iot Forensics: Challenges for the Ioa Era. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
27. Bharti, D.; Nainta, N.; Monga, H. Performance Analysis of Wireless Sensor Networks Under Adverse Scenario of Attack. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 826–828.
28. Triki, B.; Rekhis, S.; Boudriga, N. Digital Investigation of Wormhole Attacks in Wireless Sensor Networks. In Proceedings of the 2009 8th IEEE International Symposium on Network Computing and Applications, Cambridge, MA, USA, 9–11 July 2009; pp. 179–186.
29. Guo, Y.; Lee, I. Forensic Analysis of DoS Attack Traffic in MANET. In Proceedings of the 2010 4th International Conference on Network and System Security, Melbourne, VIC, Australia, 1–3 September 2010; pp. 293–298.
30. Guo, Y.; Simon, M. Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks. In Proceedings of the 2010 4th International Conference on Network and System Security, Melbourne, VIC, Australia, 1–3 September 2010; pp. 128–135.
31. Osanaiye, O.; Alfa, A.; Hancke, G. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. *Sensors* **2018**, *18*, 1691. [CrossRef] [PubMed]
32. Liu, Y.; Trappe, W. Jammer forensics: Localization in peer to peer networks based on Q-learning. In Proceedings of the 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, Australia, 19–24 April 2015; pp. 1737–1741.
33. Saputra, D.; Riadi, I. Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method. *J.-Cyber-Secur. Digit. Forensics* **2019**, *8*, 66–73. [CrossRef]
34. Kumar, V.; Oikonomou, G.; Tryfonas, T.; Page, D.; Phillips, I. Digital investigations for IPv6-based Wireless Sensor Networks. *Digit. Investig.* **2014**, *11*, S66–S75. [CrossRef]
35. Kumar, V.; Oikonomou, G.; Tryfonas, T. Traffic forensics for IPv6-based Wireless Sensor Networks and the Internet of Things. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 633–638.
36. NS-3 Manual. Real Time, Chapter 2, Simulator. 2022; pp. 45–46. Available online: https://www.nsnam.org/docs/manual/html/index.html (accessed on 20 August 2022).
37. NS-3 Manual. Statistical Framework, Chapter 3, Additional Tools. 2022, pp. 96–102. Available online: https://www.nsnam.org/docs/manual/html/index.html (accessed on 20 August 2022).
38. Minakov, I.; Passerone, R.; Rizzardi, A.; Sicari, S. A comparative study of recent wireless sensor network simulators. *ACM Trans. Sens. Netw.* **2016**, 12, 1–39. [CrossRef]
39. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]
40. Alenezi, A.; Atlam, H.F.; Alsagri, R.; Alassafi, M.O.; Wills, G.B. IoT forensics: A state-of-the-art review, challenges and future directions. In Proceedings of the COMPLEXIS 2019 4th International Conference on Complexity, Future Information Systems and Risk, Crete, Greece, 2–4 May 2019; pp. 106–115.
41. Servida, F.; Casey, E. IoT forensic challenges and opportunities for digital traces. *Digit. Investig.* **2019**, *28*, 22–29. [CrossRef]
42. Mohite, K.V.; N, P.V.J. Analysis of Forensics Tools in Cloud Environment. *Int. Res. J. Eng. Technol. (IRJET)* **2019**, *6*, 1163–1165.
43. Bouchaud, F.; Grimaud, G.; Vantroys, T. IoT Forensic. In Proceedings of the 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018, pp. 1–9.
44. Hassan, M.; Samara, G.; Fadda, M. IoT Forensic Frameworks (DFIF, IoTDOTS, FSAIoT): A Comprehensive Study. *arXiv* **2022**, arXiv:2203.15705.