ANALYZING THE IMPACT OF BLACKHOLE ATTACKS ON AODV AND DSR ROUTING PROTOCOLS' PERFORMANCE IN NS-2

Ferdinand Alifo[1], Mustapha Awinsongya yakubu[2], Martin Doe[3] and Michael Asante[4]

[1]MIS/Computer Dep., Ministry of Local Government, Local Gov't Service.
[2]University of Cincinnati Ohio, USA
[3]Computer Science Department, University of Business and Integrated Development Studies, Ghana
[4]Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are wireless networks characterized by their lack of a fixed infrastructure, allowing nodes to move freely and serve as both routers and hosts. These nodes establish virtual links and utilize routing protocols such as AODV, DSR, and DSDV to establish connections. However, security is a significant concern, with the Blackhole attack posing a notable threat, wherein a malicious node drops packets instead of forwarding them. To investigate the impact of Blackhole nodes and assess the performance of AODV and DSR protocols, the researchers employed the NS-2.35 ns-allinone-2.35 version for simulation purposes. The study focused on several metrics, including average throughput, packet delivery ratio, and residual energy. The findings revealed that AODV demonstrated better energy efficiency and packet delivery compared to DSR, but DSR outperformed AODV in terms of throughput. Additionally, environmental factors and data sizes were taken into account during the analysis.

KEYWORDS

Performance Analyss, AODV, DSR, MANET, Protocols, Security, Blackhole, NS2

1. INTRODUCTION

Routing protocols have a crucial role in Mobile Ad hoc Network (MANET) research, concentrating on guaranteeing efficient and secure communication. [1]. Several routing protocols have been specifically developed for MANETs, including AODV, DSR, DSDV, OLSR, among others. MANETs encounter vulnerabilities attributed to factors such as an open access medium, dynamic topology changes, absence of central administration or monitoring systems, cooperative algorithms, and transparent protective mechanisms [2]. Due to their attractive features, MANETs are vulnerable to malicious activities. Therefore, emphasizing security concerns becomes crucial to enhance network availability, data reliability, and privacy. Since MANETs function wirelessly, they are susceptible to different forms of attacks, including Blackhole attacks, saturating attacks, routing table overflow attacks, Denial of Service (DoS) attacks, Sybil attacks and impersonation attacks, [3]. These threats pose a serious risk to the availability, integrity, and confidentiality of network services. Among these threats, the Blackhole Attack stands out as one of the most dangerous attacks on MANETs. This attack has been known to have a considerable impact on MANET reactive routing protocols, such as Ad-hoc OnDemand Distance Vector (AODV) and

DOI 10.5121/ijcsea.2023.13402

Dynamic Source Routing (DSR) [4]. To ensure network services' availability and safeguard user privacy, it is imperative to address network security issues. This research utilizes the NS2 Simulator to investigate the performance of AODV and DSR protocols in Mobile Ad Hoc Networks (MANETs) using various metrics, including Average Throughput, Packet Delivery Ratio (PDR), and Residual Energy at the destination node. The primary objective of the paper is to assess how the AODV and DSR routing protocols respond to a Blackhole attack and how this security risk impacts crucial variables such as packet delivery ratio, average throughput, and residual energy. Moreover, the study analyzes the existing body of knowledge on evaluating routing protocol performance under security attacks, gaining insights into the behavior and effectiveness of AODV and DSR during a Blackhole attack.

MANETs are gaining popularity in diverse sectors due to their wireless network connectivity and cable-free convenience. However, their vulnerability to security attacks, particularly Blackhole attacks, raises significant concerns. By scrutinizing the behavior of AODV and DSR routing protocols under Blackhole attacks, this research yields valuable insights into these vulnerabilities and can potentially inform strategies to bolster MANET security.

2. RELATED WORKS

[3]discusses Mobile Ad hoc Networks (MANETs), which are dynamic, infrastructure-less wireless networks comprising mobile, self-organized nodes. Routing protocols in MANETs find routes between nodes for communication. The study highlights that numerous routing protocols are designed to handle dynamic topology changes. However, MANET's characteristics, like openness and restricted resources, make it vulnerable to security attacks, especially Distributed Denial of Service (DDoS) attacks. DDoS attacks consume system resources, affecting the efficiency of nodes and making them unavailable to legitimate users. The research aims to use a simulation model called DDoS-Sim to examine the impact of DDoS attacks on routing protocols like AODV, DSR, and DSDV. The model utilizes the NS-2 network simulator to apply DDoS attacks on the selected routing protocols and analyze their performance in terms of packet delivery fraction and end-to-end delay.

In [5], a Mobile Ad Hoc Network (MANET) consists of freely and mobile nodes that form a temporary dynamic wireless network without any fixed infrastructure. These nodes act as both hosts and routers, forwarding data packets to their destinations. The communication and connectivity are facilitated by routing protocols like Ad hoc On -Demand Distance Vector (AODV).

However, due to the lack of security measures and the absence of infrastructure, MANETs are vulnerable to various security threats and attacks. This paper investigates the impact of two types of attacks, namely Blackhole and Wormhole Attacks, on the AODV routing protocol using Network Simulator version 2 (NS2) environment. The goal of these attacks is to prevent data packets from reaching their intended destinations.

Given the prevalence of mobile devices in today's world, the authors in [6] have conducted a comprehensive review to explore various routing protocol technologies applicable to MANETs. The study covers different types of routing protocols, their classifications, routing techniques, geographical coverage, route metric, route repository, and route reconfiguration strategies in detail. The [6] compares the various routing protocols discussed in the study, highlighting their respective areas of strength. Additionally, the research examines network simulators that have these protocols enabled by default to gain insights into their practical implementation.

The authors in [7] proposed a cooperative analysis method to detect malicious nodes in MANETs. The mechanism involves protocols working together to analyze and reliably identify malicious nodes. They validate their method through simulations using mobile nodes and different routing protocols such as AODV, DSR, OLSR, and DSDV. The results show that the malicious node detection rate is excellent, with low overhead, a relatively high packet delivery proportion, and quick response times, particularly when there are changes in mobility speed.

According to [8], Mobile Ad hoc Networks (MANETs), routing protocols' performance is negatively affected by various network attacks, including black hole and rushing attacks. The vulnerability to these attacks extends to all layers of mobile ad hoc networks. MANETs lack centralized administration control and infrastructure, making them less secure. The paper evaluates the Ad hoc On-Demand Distance Vector (AODV) routing protocol under rushing attacks, black hole attacks, and grayhole attacks. The study assesses the network's performance under different attack scenarios, considering various factors like speed, network size, node density, and the number of attacking nodes. Performance metrics such as average throughput, average end-to-end delay, and packet delivery ratio are used for evaluation. The results show that the attacks lead to poor throughput, increased packet dropping, and higher end-to-end delays in the network. AODV is relatively less affected by rushing attacks compared to black hole and grayhole attacks.

In [9], the authors proposed an approach called Stable-Ad hoc On Demand Distance Vector (AODV) to enhance the routing performance of AODV in mobile ad hoc networks. The approach aims to improve route stability by considering node's residual energy and link quality, estimated through received signal power, against dynamic threshold values for hop selection during route discovery. If both values exceed their thresholds, the node increases the stability factor of the route before forwarding the route request (RREQ) packet. This process continues until the destination node is reached. If a later duplicate RREQ packet with a better stability factor arrives, the node processes it. Additionally, the approach maintains local neighborhood information through hello messages. When a node receives a hello message from its neighbor, it updates the neighbor table based on its current residual energy and link connectivity status using distance and hello message delay parameters. Simulation results demonstrate that the proposed Stable-AODV algorithm outperforms traditional AODV in terms of packet delivery ratio, throughput, delay, control message overhead, and normalized routing load.

The authors of [10] proposed an enhanced trust model for securing data transfer in Mobile Ad hoc Networks (MANETs) against malicious attacks. The proposed scheme combines blind trust and referential trust to establish a more robust trust model. To achieve this, the trust relationship function is integrated with the dynamic source routing (DSR) protocol, making the protocol more secure. The authors conduct a thorough analysis of the DSR protocol and generate performance matrices for packet-related data, including packets sent, packets received, packets loss, and throughput. They also evaluate the effectiveness of the improved trust establishment scheme by implementing three algorithms in the NS2 simulator to detect and prevent various types of attacks.

The main focus of the paper is to enhance the security of data transfer in MANETs by introducing a trust-based approach and integrating it with the DSR protocol for better protection against malicious attacks. The proposed scheme is evaluated and compared against different types of attacks through simulations in the NS2 simulator.

In [11], the authors introduced the Dynamic Source Routing (DSR) Protocol to enhance quality-ofservice (QoS) by calculating path reliability and link sustainability criteria. The protocol uses node energy, centrality, degree, and link cost to select relay nodes. Qualified relaying nodes are utilized to transmit data packets from the source node to the cluster head (CH). The suggested technique outperforms other existing routing protocols in terms of packet loss ratio, energy consumption, and delay. It achieves a lower packet loss ratio of approximately 4%, which is 3% less than the existing methods.

3. METHODOLOGY

In this paper, we employ the ns-2.35 simulator on Ubuntu LINUX to simulate Blackhole attack on the AODV and DSR routing protocols using Object Tool Command Language (OTCL). This simulation enables us to examine and compare the performance metrics of both protocols when the network was exposed to a Blackhole attack. Through these simulations, we were able to assess the behaviour and effectiveness of AODV and DSR in the presence of such an attack. By utilizing ns-2.35 as our simulation tool, we were able to evaluate how the Blackhole attack affects the routing protocols and draw significant findings about their performance under the metrics.

3.1. Performance Metrics

This study employed three key metrics to evaluate the research work. The first metric, Average Throughput, measures the average data transmission rate within the network, reflecting its overall performance. The second metric, PDR (Packet Delivery Ratio), is essential as it indicates the proportion of successfully delivered packets, providing insights into reliability and minimizing data losses. The third metric, Residual Energy, assesses the energy levels of nodes, offering valuable information on network efficiency and longevity.

3.2. Simulation Parameters

Simulation parameters govern a model's actions and qualities, influencing outcomes and findings. They can be modified to examine various situations or circumstances as shown in table 2.

Table 1. Simulation Parameters

Parameter	**Settings**
Channel type	Channel/Wireless channel
Propagation Model	Propagation/TwoRayGround
Physical Type	Phy/WirelessPhysical
Mac Protocol Type	Mac/802_11
Interface queue type	Queue/DropTail/CMU/PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Maximum packet in queue	50
Number of mobile nodes	17
Routing protocol	AODV and DSR
Transmission Range	550 Meters
Interference Range	550 Meters
Start Time/Stop Time	1 Second/15 Seconds
Packet in queue	5, 10, 15, 20, 25, 30
Number of Blackholes nodes	2

3.3. Routing Topology

Routing topology is the plan arrangement of conceptual elements (nodes) in a communication network. For this study, fifteen (15) legitimate nodes and two (2) malicious nodes were set in the topography of 956m by 600m simulation environment. Two commands nam AODV.nam and nam DSR.nam were executed to invoke network animator (NAM) to show the path for AODV and DSR respectively with N

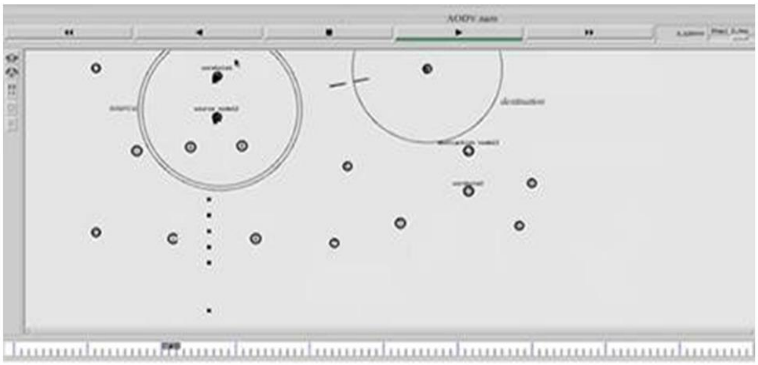

Figure 1: Screenshot of NAM with 17 nodes including two false nodes

3.4. Simulator Execution and setup

Following the successful assembly of NS-2 version ns-allinone-2.35 via Ubuntu on VMware station 16, Six (6) important files required for simulation were copied to the installation folder's home directory for execution. The Six (6) files comprises of;

- Blackhole.tcl
- average_throu.awk
- energy.awk
- pdr.awk
- AODV.tr
- DSR.tr

Location path for these files;

```
2.35/bin:/home/ferdinand/ns-allinone-
2.35/Blackhole/home/ferdinand/ns-allinone-2.35/ns-
```

```
      #PATH
PATH=$PATH:/home/ferdinand/ns-allinone-2.35/bin:/home/ferdinand/nsallinone-
2.35/tcl11.5.0/unix:/home/ferdinand/ns-allinone-2.35/tk11.5.0/unix

LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/ferdinand/ns-allinone-
2.35/otcl-1.14:/home/ferdinand/ns-allinone-2.35/lib    NS=/home/ferdinand/ns-allinone-2.35    /ns-
2.35/

NAM=/home/ferdinand/ns-allinone-2.35 /nam-
1.14/ PATH=$PATH:$XGRAPH:$N$S:$$NAM
```

3.5. Simulation Experiment for AODV

After validating the NS-2.35 installation and modifying all of the parameters, changes were made to the Blackhole.tcl file to simulate the AODV routing protocol;

- Interface queue type was set to Queue/DropTail/PriQueue
- Routing protocol was set to AODV □ tcl file was created as Blackhole.tcl
- trace file was set to tracefile [open AODVblack.tr B]
- nam file for path was set to namfile [open AODVblack.nam B]
- node 10 and node 11 were set as Blackhole node
- packets in queue [5, 10, 15, 20, 25, and 30]

3.6. Simulation Experiment for DSR

After validating the NS-2.35 installation and modifying all of the parameters, the Blackhole.tcl file was modified to simulate the DSR routing protocol:

- Interface queue type was set to CMUPriQueue
- Routing protocol was set to DSR
- tcl file was created as Blackhole.tcl
- trace file was set to tracefile [open DSRblack.tr B]
- nam file for topology was set to namfile [open DSRblack.nam B]
- nam file for path was set to namfile [open AODVblack.nam B]
- node 10 and node 11 were set as Blackhole node

4. RESULT AND ANALYSIS

Table 3 showing Average Throughput, Packet Delivery Ratio, and Residual Energy as performance metrics and data sizes displays the simulation results for AODV and DSR.

Table 2: Results of performance metrics for AODV and DSR with data sizes

Protocol	Speed/Data Size	Average Throughput	Packet Delivery Ratio(PDR)		Residual Energy (J)
AODV	5	0.288707	0.993377		1.57784
DSR		0.327946	0.983577		1.410075
AODV	10	0.328707	0.993449		3.155679
DSR		0.367946	0.983725		2.820152
AODV	15	0.368707	0.993521		4.733519
DSR		. 0.407946	0.983871		4.230228
AODV	20	0.408707	0.99359		6.311358
DSR		0.447946	0.984014		5.640304
AODV	25	0.448707	0.993658		7.889198
DSR		0.487946	0.984155		7.05038

AODV	30	0.488707	0.993724		9.467037
DSR		0.527946	0.984293		8.460455

4.1. Average Throughput Analysis

Average throughput analysis is a technique employed to assess the mean rate at which data is transmitted within a specific time frame in a given system.

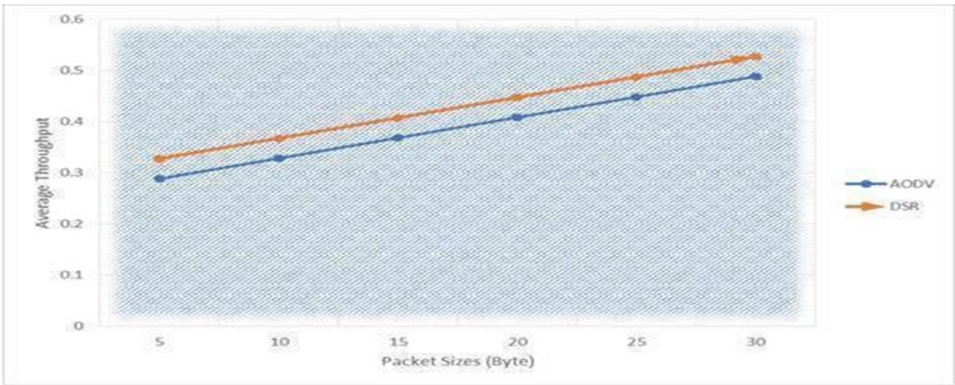

Figure 2. A graph of Average Throughput for AODV and DSR

DSR has higher throughput compared to AODV under Blackhole attack as shown in figure 2, due to its ability to detect and avoid malicious routes, enabling successful packet transmission. Additionally, DSR uses efficient routing mechanisms, reducing overhead and maintaining higher throughput even under attack.

4.2. Packet Delivery Ratio Analysis

Packet Delivery Ratio (PDR) analysis was employed to assess the efficiency and dependability of transmitting data packets within the communication system.

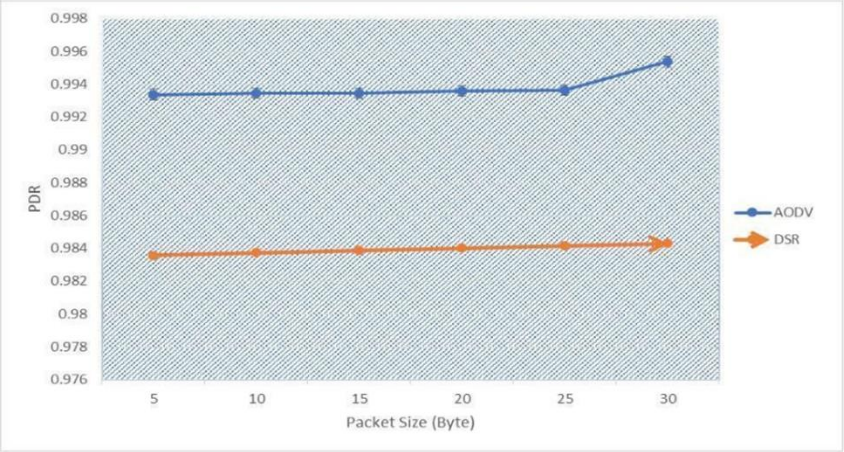

Figure 3. A graph of Packet Delivery Ratio for AODV and DSR

AODV outperforms DSR in PDR under Blackhole attack as shown in figure 3 due to better route detection and avoiding malicious node routes. AODV's efficient routing mechanisms enable lower overhead transmission, ensuring higher PDR even under attack.

4.3. Residual Energy Analysis

Residual energy analysis was utilized to evaluate the energy levels that remain in nodes within energy-constrained systems like wireless sensor networks.

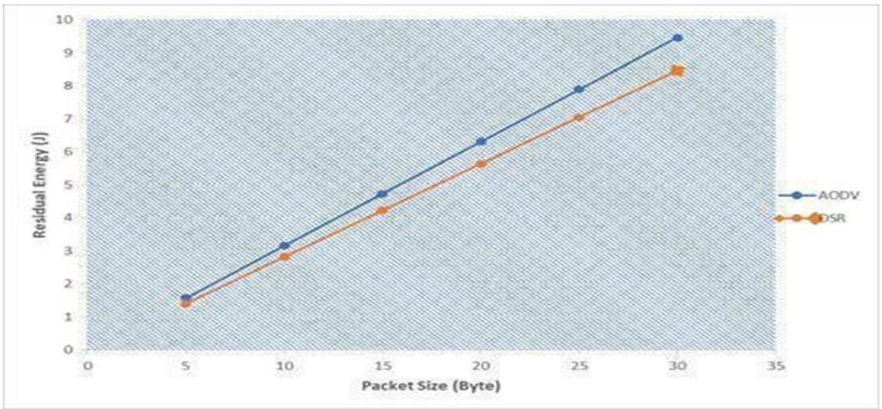

Figure 4. A graph of Residual Energy for AODV and DSR

AODV is more energy-efficient than DSR under Blackhole attack as shown in figure 4, due to its ability to detect and avoid malicious routes, while DSR is more vulnerable. AODV's efficient routing mechanisms require less energy to transmit packets, allowing nodes to conserve energy even during attacks.

5. Conclusions

This study conducted a performance analysis of the AODV and DSR routing protocols under Blackhole attacks, using PDR, Residual Energy, and Average Throughput as metrics. The simulation results indicated that DSR had a higher Throughput but AODV had better PDR and Residual Energy. These findings can help MANET network designers and managers select the best protocols for their unique network requirements. .

Acknowledgements

We express our gratitude to the reviewers for their thorough examination of the paper, as well as their valuable comments and suggestions that significantly enhanced the quality of the manuscript. Also, our gratitude goes to University of Science and Technology KNUST, Kumasi and University of Cincinnati, Ohio for their support

References

[1] B. H. Khudayer *et al.*, "A Comparative Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks," *International Journal of Advanced Computer Science and Applications,* vol. 14, no. 4, 2023.

[2] S. Al-Emadi and A. Al-Mohannadi, "Towards enhancement of network communication architectures and routing protocols for FANETs: A survey," in *2020 3rd International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2020: IEEE, pp. 1-10.

[3] M. T. Sultan, H. El Sayed, and M. A. Khan, "Performance Analysis of the Impact of DDoS Attack on Routing Protocols in Infrastructure-less Mobile Networks," in *2022 5th International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2022: IEEE, pp.1-6.

[4] T. Safdar Malik, M. N. Siddiqui, M. Mateen, K. R. Malik, S. Sun, and J. Wen, "Comparison of blackhole and wormhole attacks in cloud MANET enabled IoT for agricultural field monitoring," *Security and Communication Networks*, vol. 2022, 2022.

[5] M. H. Al Rubaiei, H. S. Jassim, and B. T. Sharef, "Performance analysis of black hole and worm hole attacks in MANETs," *International Journal of Communication Networks and Information Security*, vol. 14, no. 1, pp. 126-131, 2022.

[6] A. C. Onuora, E. E. Essien, and P. Ana, "A Comprehensive Review of Routing Protocols for Mobile Ad Hoc Networks (Manets)," *International Journal of Information System and Computer Science (IJISCS) Vol*, vol. 6, pp. 1-13, 2022.

[7] K. Thamizhmaran, "Secure Analysis of Routing Protocol under Wormhole for MANET," *Journal of Advancement in Electronics Design*, vol. 5, no. 2, pp. 47-52, 2022.

[8] P. Sarao, "Performance Analysis of MANET under Security Attacks," *J. Commun.*, vol. 17, no. 3, pp.194-202, 2022.

[9] P. Pandey and R. Singh, "Efficient ad hoc on demand distance vector routing protocol based on route stability in MANETs," *International Journal of Wireless Information Networks*, vol. 29, no. 3, pp. 393-404, 2022.

[10] S. A. Syed and A. Shahzad, "Enhanced dynamic source routing for verifying trust in mobile ad hoc network for secure routing," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, p. 425, 2022.

[11] C. N. Kishore and H. V. Kumar, "Dynamic source routing protocol for robust path reliability and link sustainability aware routing in wireless communication," *Optik*, vol. 282, p. 170036, 2023.

AUTHORS

Ferdinand Alifo is the Head of ICT/MIS department with Ministry of Local Government in Ghana. He holds an MSc Information Technology from KNUST, a BSc in Computer Science, and His expertise is further validated by his certifications in Cisco Certified Network Professional (CCNP) and Cisco Certified Network Associate (CCNA). Throughout his career, Ferdinand has made significant contributions to improving IT systems and services within the government and private sectors

Mustapha Awinsongya Yakubu is a Graduate Teaching Assistant at the University of Cincinnati where he is currently studying for PhD Information Technology. His research focuses in areas of Enterprise Architecture & Security, Human Computer Interaction, and Crisis Informatics. He earned his Master's degree in Information Technology from the Kwame Nkrumah University of Science and Technology. He has over a decade experience working in both public and private sector as an IT Professional.

Martin Doe is a Ph.D student at the University of Business and integrated development Studies, Ghana. He had MPhil in Information Technology at the Department of Computer Science in the Kwame Nkrumah University of Science and Technology, Ghana. His research area includes Cyber Security, computer networks and internet of things.

Prof. Michael Asante is an Associate Professor in Computer Science at the Department of Computer Science at the Kwame Nkrumah University of Science and Technology, Ghana. His research areas include Computer Security, Cyber Security, and Network