3L-AODV: Three Layer Security Protocol for Grayhole Attack Mitigation in MANET

Mohammed B. Alshawki[1,2,3] ✉, Wisam Dawood Abdullah[4], Alaa Khalaf Hamoud[5], Dalton C. G. Valadares[6,7], Ammar Shareiyat[8,9], and Peter Ligeti[1]

[1] Department of Computer Algebra, Eotvos Lorand University, Budapest, Hungary, [2] IDACUS, Furtwangen University, Furtwangen, Germany [3] Department of Computer Science, University of Kufa, Najaf, Iraq [4] Department of Computer Science, University of Tikrit, Tikrit, Iraq [5] Department of Computer Information Systems, University of Basrah, Basrah, Iraq [6] Virtus RDI Center, Federal University of Campina Grande, Brazil [7] Federal Institute of Pernambuco, Caruaru, Pernambuco, Brazil [8] Department of CSS, University of Stockholm, Stockholm, Sweden [9] Department of Vulnerability Operations Center, Orange Cyberdefense, Sweden

alshawki@inf.elte.hu

Abstract. As the Mobile Adhoc Networks infrastructure has no centralized points of connections, the traffic from a source to a destination pass through number of intermediate nodes. When more than one neighbour node is available, the traffic pass through one of them based on some criteria. If a node behaves maliciously in all of the connections and drops the traffic, it creates a security blackhole, while a malicious node that behaves normally is some of the connections creates a security grayhole. Since the malicious node behaves normally is some connections, mitigating this attack is challenging. In this paper we proposed Three Layer Ad-hoc On Demand Vector (3L-AODV), a security protocol that uses three layers of protection and detection to mitigate the grayhole attack. As it does not require any modification on the AODV protocol, it can be implemented on any network that its routing is based on AODV. The analysis of our results shows that 3L-AODV could mitigate the grayhole attack without affecting the performance of the network.

1 Introduction

A Mobile Ad-hoc Network (MANET), also called a wireless ad-hoc network or mobile mesh network, is a wireless network without a centralized infrastructure, i.e., the nodes do not need to communicate with a central base station or access point. Thus, the mobile nodes communicate directly among themselves using wireless links. In MANET, the nodes are assumed to have both host and router roles, which allows a node to forward data to other nodes. This way, the information can pass through some nodes in communication between the source and the sink [2]. As the nodes in MANET can be producers and consumers of data without any centralized node, the communication between any two nodes is established either directly or through some intermediate nodes. In case there is

This is an Author Accepted Manuscript version of the following chapter: Alshawki et al., 3L-AODV: Three Layer Security Protocol for Grayhole Attack Mitigation in MANET, published in Proceedings of Eighth International Congress on Information and Communication Technology, edited by Xin-She Yang, R. Simon Sherratt, Nilanjan Dey, Amit Joshi, 2023, Springer reproduced with permission of Springer Nature Singapore Pte Ltd. The final authenticated version is available online at: https://doi.org/10.1007/978-981-99-3043-2_67

no direct link between the sender and the receiver, the sender passes the traffic to its neighbors to be forwarded toward the destination node [15]. While this infrastructure makes the creation and management of the network more flexible, it adds some challenges, such as security and trustiness, due to its decentralized and mobile nature.

Due to the mentioned infrastructure, the transmission starts from one of the neighbor nodes and the traffic in indirect links passes through multiple nodes to reach its destination. Choosing which node among the neighbors to send the traffic through depends on the closest and most updated path. The choice considers the path that has the higher sequence number (*Seq*) or, in the case of two equal *Seq* in two different paths, the path with the lower number of hops. In original protocols such as AODV, there is no guarantee that the information of the returned path by a node is reliable. Therefore, a malicious node can pretend to have the most updated path by setting a high *Seq* and shortest path, which leads to being chosen by the sender node. Then, later the malicious node can drop all the incoming traffic instead of forwarding it to the destination node. This attack is called *Blackhole attack* [7, 14]. The attack will be harder to detect and prevent if the node forwards some of the traffic as any other normal node and drops the rest of the traffic. In this case, the attack is called *Grayhole attack*.

The objective of this research is to detect any suspicious activity in the network that might turn into a grayhole attack without affecting the network performance. As a result, the proposed model has to mitigate the independent malicious detected nodes from having a successful grayhole attack. We propose 3L-AODV, a security protocol that uses three layers of detection and prevention of grayhole attacks. In first layer, an attribute verification protocol [6] is utilized. In the second layer, a bait detection technique has been implemented, while in the third layer, similar to [7] a threshold detection technique has been utilized. The proposed approach uses a *Credit Value* that is affected by the results of all three layers. 3L-AODV does not require any modification in the original control messages of the AODV protocol. Therefore, it can be implemented on any existing network without a requirement to modify the existing protocol. The contribution of this paper are as follows:

- Three layers of detection and mitigation of grayhole attack.
- Mitigating the grayhole attack without decreasing the efficiency of the network, or any modification or update in the underlying protocol.

2 Grayhole Attack

MANET is a type of network that can be used without requiring specific infrastructure. It is an unsupervised network consisting of mobile devices to communicate with each other within several hops in a distributed approach [11]. The blackhole attack can be considered a type of Denial of Service attack and is also known as a full packet drop attack [14]. The attacker node tries to attract the communication traffic, positioning itself as the router node by disclosing its *Seq* number as the maximum and its path number as the shortest. Besides disturbing the routing process, it also degrades the network performance. A grayhole attack [12] is a smarter blackhole attack in which the attacker node works appropriately as a normal node in some of the traffic while on the rest of the traffic works as a malicious one, dropping received packets selectively. This attack is also known as a partial packet drop attack [14] since the attacker node works alternatively as normal and malicious and hence does not drop all the packets.

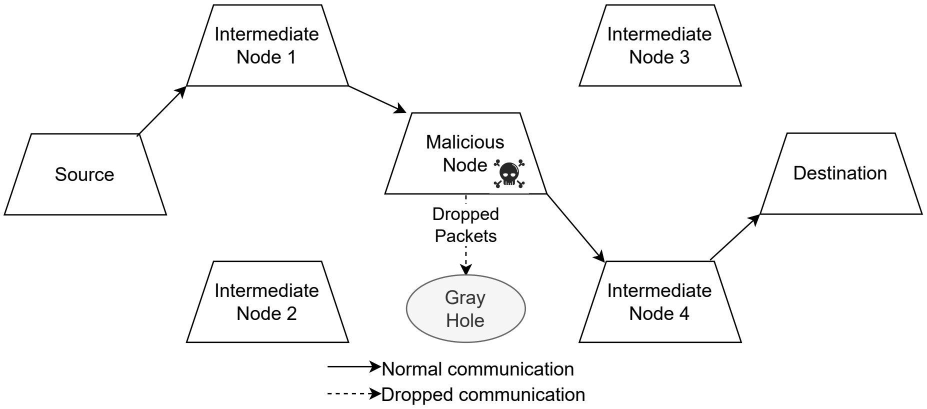

Fig. 1. Grayhole attack

Figure 1 demonstrates how a grayhole attack can happen. An attacker appears as a malicious node among the intermediate nodes responsible for forwarding the communication between the source and destination and tries to convince the sender to pass the traffic through the malicious node. Then, sometimes the malicious node will work adequately, forwarding the packets correctly, and sometimes it will drop the packets.

3 Related Works

As it has been discussed, grayhole attack as a more complex variant of blackhole attack is a challenge for MANETs security that can cause the destruction of the networks, reducing efficiency, and losing data. [16, 4, 19]. Ahamed and Fernando [1] proposed a security mechanism that improves the data communication security between source and destination in a MANET. They also deal with the security issue of a blackhole attack. STAODV proposed by Alshawki and et al. [7] specifically protects the network against blackhole attack by proposing a model to mitigate the attack through adoption of a threshold technique. Mukul Shukla and Brijendra Kumar Joshi [17] proposed Trust-based Fuzzy AODV technique to handle the blackhole attack using a method of trust-based fuzzy based on energy auditing, neighbor node trusting, node member authenticating, and packet integrity checking. Due to using fuzzy logic, the proposed method suggests that the node is considered to be trusted by evaluating the trust value (greater than or equal to 0.6), then the communication is established between source and destination; otherwise; the node is considered as unsafe. The rethat the results are improved based on factors such as throughput, end-to-end delivery, and delivery ration context.

The blackhole and wormhole attacks were handled by Shukla et al. [18] by using a scalable-dynamic elliptic curve cryptography. They examined two types of scenarios (with and without attack). They found outstanding results according to end-to-end delay and energy consumption. Ramaprasad and Lingareddy [13] introduced a novel scheme to assess the link's legitimacy for detecting the attack of route diversion and counter-measuring the cost-effectiveness of the attack. They concluded that the process of token generation, associated with link legitimacy, will offer more secure routing than other threats' ranges. By using lightweight encryption, there is a balance between security and data transmission.

Gurung and Chauhan [4] proposed a methodology based on NS-2.35 for mitigating the attack of smart grayhole in MANET by implementing an intrusion detection for nodes. The detection nodes are deployed in MANET to prevent smart attack. The proposed mechanism suggests that the nodes overhear their neighboring nodes' transmission and block the node with malicious behavior when it drops data packets at a greater rate than the determined threshold. The nodes then notify the other nodes about the nodes with malicious behavior by broadcasting an ALERT message. Chawhan et al. [3] proposed a model to mitigate the grayhole attack in MANET by introducing a number of Intrusion Detection System (IDS) nodes, along with the intermediate nodes that are utilized to detect the malicious nodes responsible for grayhole attack. The proposed model works efficiently in terms of throughput and delay. However, it requires a modification to adopted AODV routing protocol.

4 3L-AODV

Lets $\mathcal{N}$ denotes the set of nodes in the network. We assume there is a subset of independent malicious nodes in $\mathcal{N}$ that perform a grayhole attack. A node $i \in \mathcal{N}$ in the network has a set of neighbors $\mathcal{B}_p \subset \mathcal{N}$. Each node in $\mathcal{B}_p$ is associated with a local value by the node p called *Credit Value (CV)*. Under a node p's point of view, each member $b \in \mathcal{B}_p$ is assigned with a CV_b value. The initial value of CV is fixed during the system setup. Later on, each node $i \in \mathcal{N}$ assigns the default value of CV to each new incoming neighbor node in $\mathcal{B}_p$. 3L-AODV uses three layers of detection: 1- Attribute verification, 2- Bait detection, and 3- Threshold detection. As shown in Figure 2, the results of these three techniques affect the CV parameter of each node. A zero credit value results in putting the corresponding node in a local table called *Black-list Table*.

As the first layer of malicious node detection, a node in the network can verify the hop counts of its neighbours and let only those nodes with verified attributes to involve in the process of transferring the traffic as intermediate nodes. We assume the existence of a subset of trusted nodes in $\mathcal{N}$, called *Hop Provers*. The primary duty of these nodes is to provide a proven hop distance ticket to a given node, as illustrated in Figure 3. A trusted hop prover issues a hop count ticket to a node associated with an expiry. It does not have to

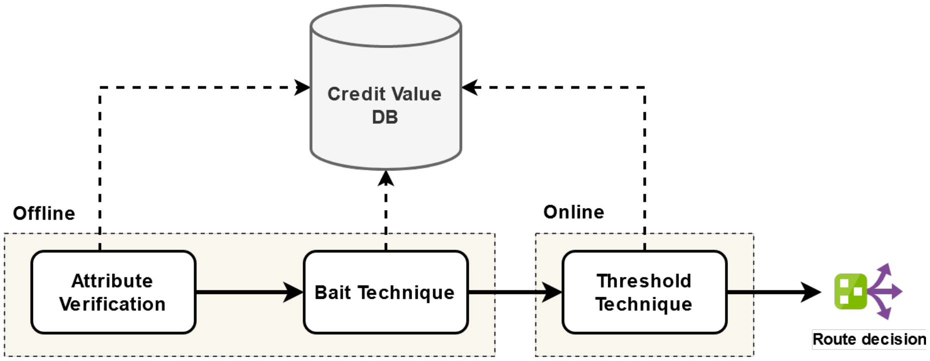

Fig. 2. 3L-AODV layers

be online later during the attribute verification process. Therefore, this layer is performed partially offline.

In order to verify the claimed attributes, specifically the number of node hops in $\mathcal{B}_p$, a node in the network applies the attribute verifier protocol [6] that is based on Attribute-based Encryption (ABE) [20] and is mainly used in the data validation networks [8]. The node utilizes *n-out-of-n* verification mode for a specific set of target attribute verification. In the case of resource-constrained nodes, lightweight protocols for encryption [9, 10] can be integrated into the attribute verification process. The inability to solve a transmitted challenge by the issuer node p and prove the attributes will reduce the corresponding CV value of a node in $\mathcal{B}_p$.

Before the traffic transmission, the sender can send a request with its address or a non-existed address as the bait address (destination address). In case a node responds to this packet, it will be detected as malicious, its corresponding CV value is set to zero, and the node is added to the black-list table. This step will filter some of the malicious nodes. Since the malicious nodes in the grayhole attack can work adequately in some periods, this technique will not detect all the malicious nodes during a grayhole attack. Finally, the traffic is sent, and the responses from different nodes are gathered together and examined to detect the safety of each response and any possible grayhole attack.

A network setup can allow the peers to perform end-to-end communication using protocols, such as Distributed Address Table (DAT) [5]. When a node p wants to send a packet to a destination node d, it sends the request RREQ to its neighbors and receives a set of replies (i.e., RREP). Each received RREP includes a Seq value and hop counts. The path through the node i that sent a RREP with higher Seq is chosen to send the packet to the destination node d. Prior to the path selection, 3L-AODV uses Seq values of the received RREPs to calculate the average threshold value as in Eq. 1.

$$threshold = \frac{1}{N}\sum_{i=1}^{N} Seq_i - Seq_d \tag{1}$$

In which N is the number of nodes in the routing table that sent an RREP, Seq_i is the *Seq* parameter of RREP received from node i, and Seq_d is the available sequence number of the destination node in the node p's routing table. The next step is to check the *RREP Validity* by defining the *Dif* value for each of the received RREPs as in Eq. 2.

$$Dif_i = |Seq_i - threshold| \tag{2}$$

In which Seq_i is the *Seq* parameter of RREP received from node i. If the Dif_i value is lower than a predefined acceptable range, the RREP is considered *Valid*. Otherwise, if the Dif_i value is higher than the predefined acceptable range, the CV parameter of the node i will be reduced by one. A zero CV parameter result in adding the corresponding node in the *black-list table*.

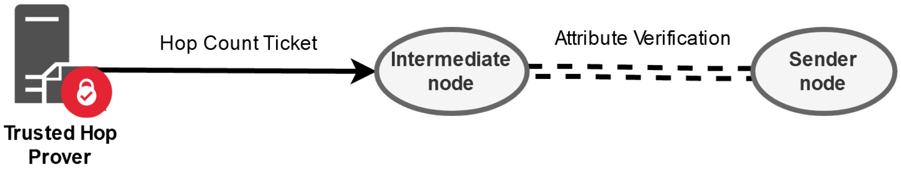

Fig. 3. Attribute verification layer

5 Evaluation

5.1 Simulation Design and Setup

To evaluate the 3L-AODV, we utilized the network simulator NS-2 to conduct experiments considering the implementation of a grayhole attack in an ad-hoc network. The purpose of these experiments was to assess how well the proposed 3L-AODV would function in a MANET in the existence of independent malicious nodes performing the grayhole attack.

For the simulation, we configured the parameters accordingly, as described below. We set the simulation time for 100 seconds and a simulation area of 800m x 800m. We configured 25 for the number of nodes and zero to four malicious nodes that performed the grayhole attack. We assumed that the malicious nodes were independent. The routing protocol used the AODV protocol, whereas the MAC protocol employed the IEEE 802.11. The traffic type of simulation was Constant Bit Rate (CBR), with the source and destination being 12. The data payload was 512 bytes. Spoofed route replay generates the details of attributes concerning the malicious nodes by making a Path Replies PDU. Consequently, the hold count is assigned “1” as a value and the fake destination sequence number via incrementing 30 to 90 as a random number to arrive. Path discovery relies on Path Requests’ destination sequence number.

To compare the 3L-AODV versus the AODV, the particular setup for the simulation results was the primary point of our research concentration. The first two layers of 3L-AODV, i.e., part of the attribute verification and bait techniques, can be done prior to actual traffic transmission during the idle time. Without loss of generality, we evaluated the third layer of 3L-AODV that is fully executed during the actual data transmission.

5.2 Results and Discussion

The time it takes for a packet to be transferred from source to destination across a network is known as end-to-end delay or one-way delay. The proposed approach of 3L-AODV had fluctuating performance compared to AODV as illustrated in Figure 4.

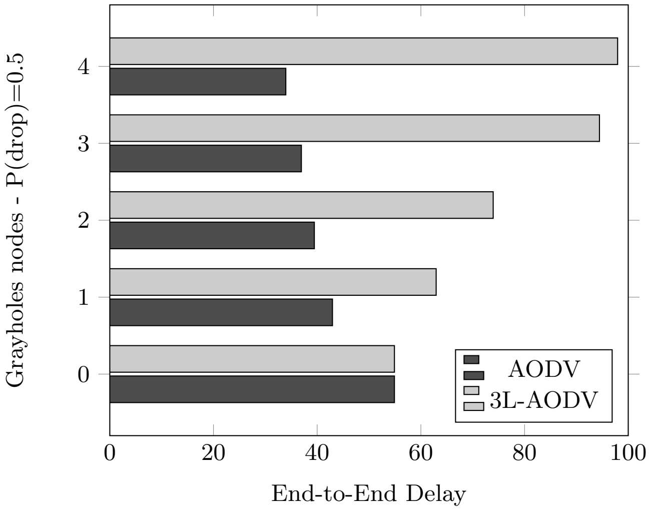

Fig. 4. Effect of delay

3L-AODV experienced an increase in end-to-end delay from 55s to 97s according to the appearance of malicious nodes sequentially. The grayhole nodes broadcasted spoofed acknowledgments containing fabricated target node sequence numbers. Utilizing 3L-AODV, these nodes might be detected in the first two layers. Additionally, 3L-AODV detected the malicious node and mitigated the grayhole attack by preventing the malicious nodes from being selected for traffic transmission. Consequently, taking this approach during the third layer of 3L-AODV impacted the end-to-end delay performance.

The throughput is recognized as a number of successful delivered packets or bits within a specific period of time. Where throughput performing high with no occurrence of malicious node, i.e., high throughput indicates good performance. The existence of a grayhole node affects the throughput by dropping some of the packets. The 3L-AODV performed 50% better than that of AODV as illustrated in Figure 5. Both AODV and 3L-AODV performed identical at initiate time. However, the performance of AODV exhibited consistent degradation. Occurrence of malicious node degrade the AODV 49 kbps for instance malicious node

1 appearing throughput preformed 66kbps while throughput scored 58 kbps to 49 kbps when node 2 and node 3 appeared correspondingly. Thus, 3L-AODV outperformed AODV in terms of throughput from the added malicious nodes. 3L-AODV exhibited a high throughput performance ranged between 98 kbps to 99 kbps respectively.

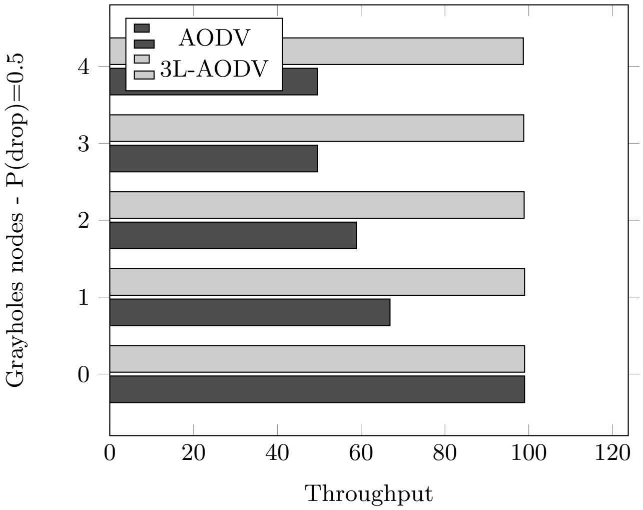

Fig. 5. Effect of throughput

The Packet Delivery Rate (PDR) is defined as the ratio of total received packets through destination node to the total sent packets by source. Where PDR performing high with no occurrence of malicious node, i.e., high PDR indicates good performance. The malicious node affected through dropping a packet resulting the total packets sent through source nodes be higher than the total received packets by the destination node. Figure 6 shows that the performance of AODV exhibited consistent degradation during grayhole attack. Both AODV and 3L-AODV performed identical at initiate time, as a result, packet deliveries are unaffected by the calculated safety status. Occurrence of malicious nodes degrades the AODV PDR ratio, which reached to 50% in case of four malicious nodes that performed the grayhole attack. Thus, 3L-AODV outperformed AODV in terms of packet delivery ratio that exhibited a high PDR between 97% to 98%.

6 Conclusion

In this paper a security protocol to mitigate the grayhole attack has been proposed. The proposed protocol, 3L-AODV, consists of three layers of protection and detection. In the first layer, the node can choose the intermediate nodes

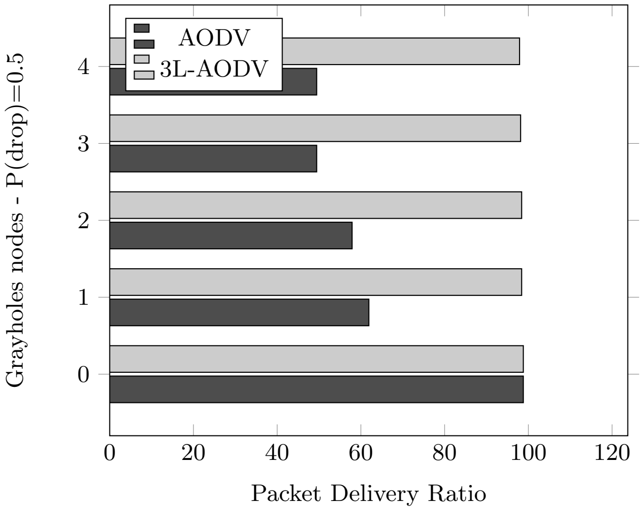

Fig. 6. Effect of packet delivery ratio

based on verified attributes, such as the hop count attribute, and a challenge-response approach to verify the attribute. In the second layer, the node uses bait technique to detect the malicious nodes. In the third layer and using threshold technique, the sender is able to mitigate the grayhole attack. The analysis showed that 3L-AODV is efficient, and does not require any modification in the original routing protocol of AODV. The future research directions include further analysis on the layer modification and integration, as well as the use of various detection techniques in the third layer that choose a valid safe path as long as it receives one, without the need to wait for other replies.

Acknowledgements. This research was partially supported by Project no. TKP2021-NVA-29 has been implemented with the support provided by the Ministry of Innovation and Technology from the National Research, Development and Innovation Fund and the project No. 2019-1.3.1-KK-2019-00011 financed by the National Research, Development and Innovation Fund of Hungary under the Establishment of Competence Centers, Development of Research Infrastructure Programme funding scheme.

References

1. Ahamed, U., Fernando, S.D.: Lightweight security mechanism to mitigate active attacks in a mobile ad-hoc network. International Journal of Electronics and Telecommunications 68(1), 145–152 (2022)
2. Alameri, I.A., Komarkova, J.: A multi-parameter comparative study of manet routing protocols. In: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). pp. 1–6. IEEE (2020)
3. Chawhan, M.D., Karmarkar, K., Almelkar, G., Borkar, D., Kulat, K.D., Neole, B.: Identification and prevention of gray hole attack using ids mechanism in manet.

In: 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22). pp. 1–6. IEEE (2022)

4. Gurung, S., Chauhan, S.: A novel approach for mitigating gray hole attack in manet. Wireless Networks 24(2), 565–579 (2018)
5. Alshawki, M.B., Ligeti, P., Nagy, A., Reich, C.: Distributed address table (DAT): A decentralized model for end-to-end communication in iot. Peer-to-Peer Networking and Applications 15(1), 178–193 (2022)
6. Alshawki, M.B., Yan, Y., Ligeti, P., Reich, C.: Attribute verifier in internet of things. In: 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC). pp. 1–3. IEEE (2022)
7. Alshawki, M.B., Alameri, I., Onaizah, A.N.: Staodv: a secure and trust based approach to mitigate blackhole attack on aodv based manet. In: 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). pp. 1278–1282. IEEE (2017)
8. Alshawki, M.B., Ligeti, P., Reich, C.: D3vn: Decentralized abe-based distributed data validation network. In: Proceedings of Seventh International Congress on Information and Communication Technology. Springer (2022)
9. Alshawki, M.B., Ligeti, P., Reich, C.: Odabe: Outsourced decentralized cp-abe in internet of things. In: Applied Cryptography and Network Security Workshops. Springer (2022)
10. Alshawki, M.B., Ligeti, P., Reich, C.: Sdabe: Efficient encryption in decentralized cp-abe using secret sharing. In: 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET). pp. 1–6. IEEE (2022)
11. Kuo, W.K., Chu, S.H.: Energy efficiency optimization for mobile ad hoc networks. IEEE Access 4, 928–940 (2016)
12. Ourouss, K., Naja, N., Jamali, A.: Defending against smart grayhole attack within manets: A reputation-based ant colony optimization approach for secure route discovery in dsr protocol. Wireless Personal Communications 116 (01 2021)
13. Ramaprasad, H., Lingareddy, S.: A novel integrated scheme for detection and mitigation of route diversion attack in manet. International Journal of Advanced Computer Science and Applications 12(11) (2021)
14. Rani, P., Kavita, Verma, S., Nguyen, G.N.: Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. IEEE Access 8, 121755–121764 (2020)
15. Saad, H.N., Alshawki, M.B.: Weight analysis for weighted cluster algorithms in mobile ad-hoc network. Journal of Theoretical & Applied Information Technology 95(15) (2017)
16. Schweitzer, N., Stulman, A., Margalit, R.D., Shabtai, A.: Contradiction based grayhole attack minimization for ad-hoc networks. IEEE Transactions on Mobile Computing 16(8), 2174–2183 (2016)
17. Shukla, M., Joshi, B.K.: An effective scheme to mitigate blackhole attack in mobile ad hoc networks. In: Edge Analytics, pp. 149–164. Springer (2022)
18. Shukla, M., Joshi, B.K., Singh, U.: Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in manet. Wireless Personal Communications 121(1), 503–526 (2021)
19. Yan, J., Zhou, M., Ding, Z.: Recent advances in energy-efficient routing protocols for wireless sensor networks: A review. IEEE Access 4, 5673–5686 (2016)
20. Yan, Y., Alshawki, M.B., Ligeti, P.: Attribute-based encryption in cloud computing environment. In: 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE). pp. 63–68. IEEE (2020)