Computers, Materials & Continua
DOI:10.32604/cmc.2020.014094
Article

Tech Science Press

Packet Drop Battling Mechanism for Energy Aware Detection in Wireless Networks

Ahmad F. Subahi[1,*], Youseef Alotaibi[2], Osamah Ibrahim Khalaf[3] and F. Ajesh[4]

[1]Department of Computer Science, University College of Al Jamoum, Umm Al Qura University, Makkah, 21421, Saudi Arabia
[2]Department of Computer Science, College of Computer and Information Systems, Umm Al Qura University, Makkah, 21421, Saudi Arabia
[3]Al-Nahrain University, Al-Nahrain Nanorenewable Energy Research Centre, Baghdad, 70030, Iraq
[4]Department of Computer Science and Engineering, Musalair College of Engineering, Kerala, India
*Corresponding Author: Ahmad F. Subahi. Email: AFSubahi@uqu.edu.sa
Received: 30 August 2020; Accepted: 11 October 2020

Abstract: Network security and energy consumption are deemed to be two important components of wireless and mobile *ad hoc* networks (WMANets). There are various routing attacks which harm *Ad Hoc* networks. This is because of the unsecure wireless communication, resource constrained capabilities and dynamic topology. In order to cope with these issues, *Ad Hoc* On-Demand Distance Vector (AODV) routing protocol can be used to remain the normal networks functionality and to adjust data transmission by defending the networks against black hole attacks. The proposed system, in this work, identifies the optimal route from sender to collector, prioritizing the number of jumps, the battery life, and security, which are fundamental prerequisites. Researches have proposed various plans for detecting the shortest route, as well as ensuring energy conversions and defense against threats and attacks. In this regard, the packet drop attack is one of the most destructive attack against WMANet communication and hence merits special attention. This type of attack may allow the attacker to take control of the attacked hubs, which may lost packets or transmitted information via a wrong route during the packets journey from a source hub to a target one. Hence, a new routing protocol method has been proposed in this study. It applies the concept of energy saving systems to conserve energy that is not required by the system. The proposed method for energy aware detection and prevention of packet drop attacks in mobile *ad hoc* networks is termed the *Ad Hoc* On-Demand and Distance Vector–Packet Drop Battling Mechanism (AODV–PDBM).

Keywords: Wireless and mobile *ad hoc* networks (WMANet); packet drop attack (PDA); *ad hoc* on-demand distance vector (AODV); dynamic source routing (DSR); packet drop battling mechanism (PDBM)

1 Introduction

Wireless and mobile *ad hoc* networks (WMANets) are both considered free wireless frameworks. Using the communications between the WMANet and the mobile network in a system, one can frame a distinctive

system configuration or topology by using the system's ability to self-correct without hub dependency [1]. In the case of *ad hoc* networks, providing secure communication in various environments is extremely crucial. Thus, a key security concern in WMANets is routing attacks. These attacks disconnect a WMANet from its focal base station. WMANet routing protocols are uncomplicated, which makes them more vulnerable to such attacks compared with the routing protocols of framework-based networks. A type of common routing attacks on WMANets is the packet drop attack (PDA) [2]. A PDA functions as the base for launching different attacks, such as a distributed denial of service attack and a sinkhole attack, which result in numerous hubs attempting to route their traffic to the malicious hub. These attacks enable the attacker to gain control over a significant portion of the system and its related activity. Hence, steering conventions are the most researched topic in WMANet literature.

Network and security specialists have outlined various routing protocols for WMANet, such as the *ad hoc* on-demand vector, optimized link state routing, dynamic source routing (DSR), and the destination sequenced distance vector. The major concerns in relation to WMANets are saving energy and ensuring security, which affect the networks' fundamental functionality [3–5]. WMANet hubs are battery controlled, which calls for battery life extension. This is an identified issue, as is finding the shortest route to targeted hubs without massive consumption of battery power. Owing to the different quality measurements of their system, such as open access medium, the inadequacy of admins, and the insufficiency of the straightforward resistance mechanism of WMANets, the system is not frequently used by attackers, thereby preventing security attacks [6,7]. The system administration availability as well as the information integrity and confidentiality can be enhanced by addressing the identified security issues in the system. In addition, the use of wireless connection makes WMANets more vulnerable to attacks by giving the attacker access to ongoing communications. A variety of attacks on WMANets have been discovered and described [8].

The several types of attacks identified to date include worm-gap attacks, PDAs, hurrying attacks, asset consumption attacks, sybil attacks, flooding attacks, denial of service attacks, and mocking attacks. The minimum total transmission power routing calculates the power generally required for moving the packets of data via various routes, the route that requires the least energy consumption is selected. However, the power remaining with hubs is not ascertained, this can be a cause of the destruction of a few hubs and thus damage transmitted packets during transmission. Thus, a method for selecting the most energy-conserving hub among these base controlled hubs is required [9]. Max–min battery capacity routing expands the system by using the remaining energy of a hub, but it disregards the aggregated energy of transmission and the cause of power consumption. The conditional max–min battery capability directly joins the components that are added to the transmission energy and the remaining vitality of hubs under consideration. The least drain rate uses a metric depletion proportion, registered for a hub as a ratio of its remaining energy and the proportion of its power consumption rerarding the current activity conditions. The route with the lowest deplete ratio and least battery control is selected [10].

This paper also considers the problem of energy efficient routing to increase WMANets life. The efficient use of battery energy has become particularly important because the mobile hosts in use currently are powered by battery. The energy resources of actively participating nodes are depleted faster than those of other nodes, which in some cases, may lead to the partitioning of the network and consequently decrease its life. For this reason, reducing energy consumption in *ad hoc* wireless networks is a critical issue.

The remainder of this paper is organized as follows. Section 2 outlines the research background and related literature. Section 3 explains the PDA. Section 4 presents the proposed *Ad Hoc* On-Demand Distance Vector (AODV) Packet Drop Battling Mechanism (PDBM); that is, the AODV–PDBM. Section 5 presents the results. Section 6 provides a summary of this study and recommendations for future research.

2 Related Works

PDA is considered a calculated attack on security during routing. Significant attention is required to manage this issue. Security experts have proposed different solutions to manage such attacks. The review presented in this study discusses some of the available solutions and highlights the research conducted in the current decade. Recently, a solution has been proposed to prevent packet dropping through the theorem of anodes by using the Bayesian and the prior likelihood techniques. At the point when a hub is found to drop packets, it is disposed of from the system. Utilizing this heuristic scientific model, secure routing is feasible through an autonomous environment [11]. A mechanism has been advanced to detect agreeable PDA based on crosschecking with a clock-based mechanism termed True Link in the AODV routing protocol. Similarly, the network designers have conducted a simulation to demonstrate the base steering overhead, the deferral, and the most extreme throughput with an increment in the number of attacker hubs and in the interruption time. They have recommended a strategy to detect and prevent PDAs based on reliable data estimations. The researchers monitored the information conveyed to the recipient and examined the causes for packet drops in the middle of the packet transmission from the source hub to the target, based on which a hub functioning as a packet drop hub may be considered malicious. A trust-based mechanism has been introduced for recognizing such packet drop hubs. A boycott table is retained at each hub, and a trust estimation of its neighboring hubs is specified. The trust estimation of neighboring hubs or nodes is based on detecting whether the node is a sinkhole in the network. When the trust score of a particular node falls below the normal score of 0.5, this node is regarded as a sinkhole attack node [12,13].

A detection technique has been recommended for PDA in which the next bounce and the past jump hub of a route reply packet is checked to identify hubs during transmission. The sensor hub identifies a problem hub by investigating the data routing data packetstable it maintains. Further, analysts have proposed a trap detection approach for defending against synergistic attacks made by pernicious hubs in mobile *ad hoc* networks (MANETs) [14]. PDAs are recognized and anticipated by planning a cooperative bait detection scheme, which has the advantages of proactive safeguard structures and additionally receptive guard models that use an invert following system. A strategy has been demonstrated to recognize malicious hubs by utilizing the notion of Self-Protocol Trustiness (SPT) and another technique for opposing the PDAs as a black-gap resistance mechanism, that is implanted with all kinds of the receptive routing protocols [15–17]. The discussed techniques use neighborhood clocks and settled edge esteems for characterizing any hub as malicious [18].

Scientists have proposed a guard dog approach that uses a specification-based detection plot for distinguishing the packet drop and, in particular, launching attacks in wireless sensor networks. This plan practices a distributed approach in which every hub does not have a universal view. A study has recently been conducted on PDA on WMANets and on the current solutions [19]. The proposition is introduced in a chronological request and partitioned into single and cooperative PDA. A peculiarity detection searches for PDA in *ad hoc* networks and has been examined and demonstrated. They used a dynamic preparing strategy instead of a static preparing technique since WMANets are mobile and use dynamic topology. In this plan, preparing information is provisionally updated at a fixed time [9].

3 Packet Drop Attack

In a PDA, the attacker hubs misuse vulnerabilities during the route disclosure procedure of responsive steering conventions and introduce a wrong route to the target hub. On receiving a route error message, the transitional attacker hub answers with a route reply that has an over-the-top destination arrangement number that the route request message receives, which confirms the destination. If an attacker chooses to launch an attack using rapid, high power transmission, it is difficult to discover a compromised route that bypasses the

attacker hub [20–22]. Once the attacker chooses the hub as the control hub or disables some of the routes in the system, the attacker uses the hub to begin manipulating or decreasing the traffic it coordinates by creating a packet drop. This situation becomes critical when the attacker begins attacking an increasing number of routes. Fig. 1 shows the categories of attacks.

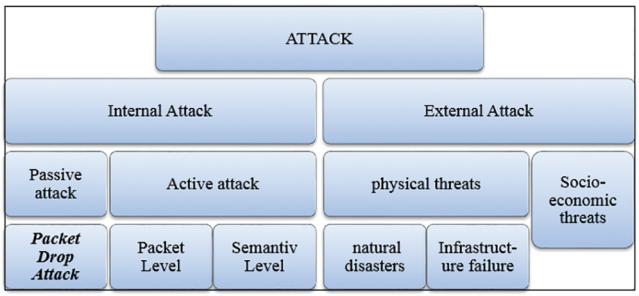

Figure 1: Categories of attacks

Fig. 2 shows the classification of PDAs. Attacks, such as internal and external PDAs, are made based on the nearness of attacker hubs. PDAs can also be classified based on the method of collaboration between attacker hubs into single or collaborative PDAs. The attacker hubs; for example, single PDA and collaborative PDA.

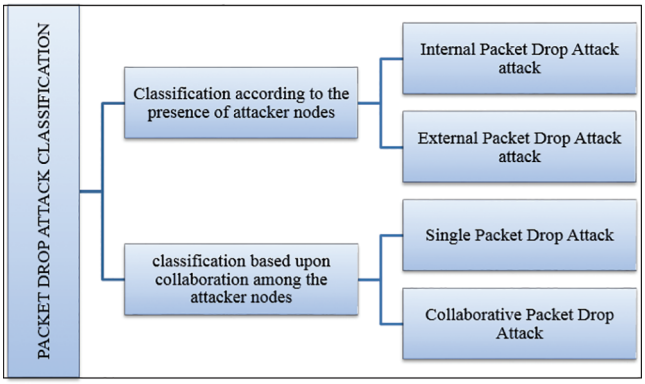

Figure 2: Packet drop attack classification

An increasingly common attack is one in which an attacker hub is transformed into a piece of the route in the network, which can be described as an unusual type of PDA since, in this type, the data packets routed through the hub are not dropped [23]. At first, the attacker hub can act as a genuine hub using trusted protocols, but later drops packets directly from some particular hubs or in some other specific instance. The identification of attacker hubs in this form of attack is particularly troublesome because these hubs drop packets routed through them for quite a while, although they may normally serve as actual hubs otherwise [18].

4 Proposed *Ad Hoc* On-Demand Distance Vector Packet Drop Battling Mechanism

Initially, during the arrangement setup of every mobile hub, data registers itself with the system, and creates a private key. In addition, it shares an open key match, which is used by the individual mobile hubs to generate computerized marks. Every hub makes a neighbor disclosure through “welcome”

messages. Route discovery is the underlying procedure performed. When two hubs need to communicate and interact with each other, and the sender hub does not have the required routing protocol, after that, the sender hub creates or instantiates a Forward Agent (FA) and connects its own particular computerized mark to it. Next, the FA broadcasts to its neighbors, and each neighbor receiving the FA confirms its advanced mark after checking that it is correct. Then, the FA is acknowledged by its neighbors. Each transitional hub that has an FA connects its own advanced mark to it and retransmits to its neighbors prior to reaching the destination hub. During its transmission toward the destination, the FA accumulates route information that is shared with neighbor hubs. On reaching the target hub, the FA is executed and a Backward Agent (BA) is created, which goes from the destination towards the source hub by using the information collected by the FA.

The following stage is the data flow in the system. Once the path detection is completed and productive routes are established between the sender hub and the recipient one, information begins to flow between them. During information exchange, advanced marks are likewise used with each information packet sent, to ensure secure communication.

Source hubs are able to confirm the route by sending FAs and BAs at continuous time intervals. In case of any disconnection—such as because of the removal of a malicious packet drop hub—the need to begin the discovery of another route might be addressed locally from the hub where no further routing information is accessible.

Finally, the detection of the malicious hub is achieved. When an outer attacker hub needs to take an interest in the dynamic route, it is found during the computerized signature verification stage, signalled by the lack of a mystery key, because such key is only present in the inner enlisted mobile hubs. Each mobile hub within the network has been installed with guards and a route rate mechanism to track the neighboring hubs via information exchange for recipient hubs. Each hub monitors its neighbors to identity issues such as data packet loss, slow information exchange rate, and false flooding. If any of the components of a hub fall below the corresponding base point, its neighbor hub places this hub on the malicious hub list and sends a message to inform all the legitimate hubs in the network about the hub's malicious actions.

5 Results and Discussion

WMANets can be implemented in various environments as indicated by the need of the application. We considered the issue of recognizing PDAs in WMANets by using the AODV route disclosure stage. Once the compromised hub receives a route request packet, it easily sends a route response to the originator hub by using a randomly generated high destination arrangement number and pretending that it is a destination preferably far away. The source hub waits for the route reply since it should receive such reply from either the malicious hub or the genuine destination to begin information transmission. The malicious hub sends a route reply packet with a high destination sequence number and the least number of jumps. The source expects that this route is fresh and begins transmitting information through it. An exact approach is required to recognize and eliminate an attacked hub from the system and the remaining personal hubs. A malicious hub launches different attacks, such as choosing sending and sinkhole attack in WMANets.

All the on-demand algorithms are considered. Associativity-based routing, AODV, DSR, and flow state in dynamic source routing are some of the routing protocols included in the simulation and are compared with the proposed AODV–PDBM. No routing protocol in a WMANet considers security an objective. From this AODV routing protocol, a route response is created by a destination or a transition hub that has a short route to the destination. This results in a significant flaw in the AODV route disclosure stage, which is used by the malicious hub. At the point when a route is required, the source hub broadcasts the route request to each hub within wireless range. At the point when a malicious hub receives a route

request packet, it sends a route reply immediately with a randomly produced high destination succession number with least number of jumps. The source stays in inactive for the route reply. When it receives the first route reply, it begins information transmission through the malicious hub. One conceivable solution to the examined issue is to disable the capacity of any intermediate hub to produce a route reply even if it maintains a route to the destination. Only the destination hub can produce a route reply by this technique, and thus, we can secure AODV to some degree. However, large networks will face increased routing delay

With the final goal of simulation adjustment, the current AODV steering convention is enforced in compliance with our proposed guidance and contrasting strategy and the fundamental AODV steering convention. The simulation was completed using Network Simulator (NS-2.35), which is used to run system tests. The perspective of the finished simulation environment is shown in Tab. 1. We used certain simulation parameters, such as packet conveyance proportion and number of packets lost against the number of attackers, similar to [24–26]. Parameters such as the steering overhead, arrange energy consumption, and system throughputs compared with the simulation time to evaluate the execution of our proposed algorithm compared with that of the fundamental AODV routing protocol.

Table 1: Parameters used and the corresponding statistical value

S no	Parameter name	Value
1	Number of nodes	500
2	Nodes of distribution	Random
3	MAC type	IEEE 802.11
4	Propagation	Two way reflection
5	Simulation time	500 s
6	Sensor field	100 × 100 m
7	Network type	Wireless and *ad hoc* network
8	Mobility pattern	Random
9	Network layer	Broadcast

Fig. 3 presents a graphical representation of the packet delivery ratio. This ratio is calculated as the aggregate numerous packets collected at the target hub to the many packets sent by the Constant Bit Rate source.

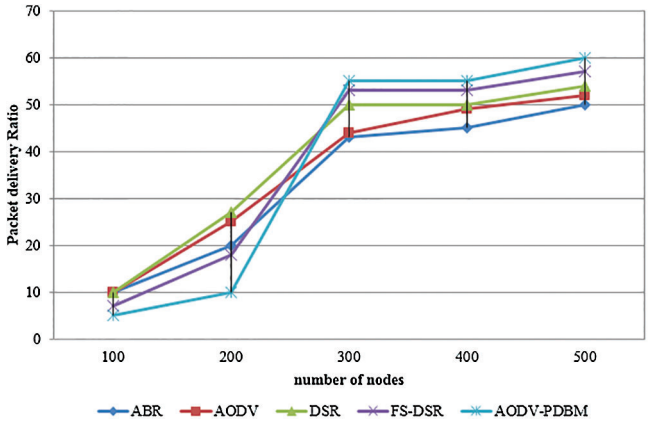

Figure 3: Graphical representation of packet delivery ratio

Fig. 4 presents a graphical representation of packet loss within a network. Packet loss can be interpreted as the fraction of the accumulated number of packets lost because of congestion or other reasons relative to the total number of packets sent during transmission. Thus, system implementation is difficult if accurate estimates of packet loss are unavailable.

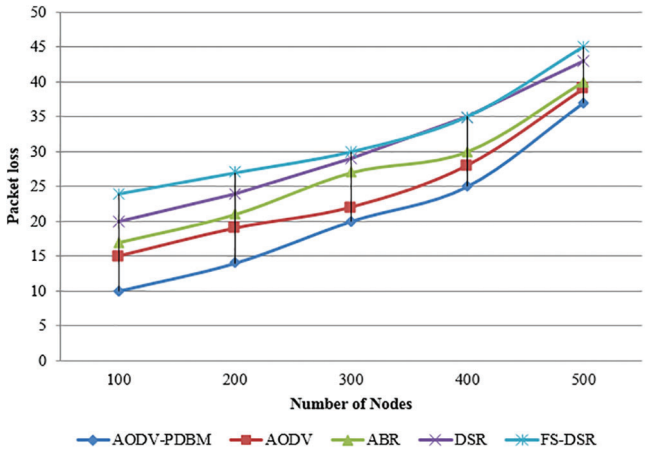

Figure 4: Graphical representation of packet loss in a network

Fig. 5 provides a graphical representation of the overhead routing within a network. Overhead routing can be interpreted as the proportion of the number of routing packets transmitted relative to the number of information packets effectively transmitted, where steering packets contain control packets used for route exploration, route repair, and for the optimization updating rule (pheromone). Implementation of the program improves with a reduction in overhead packets.

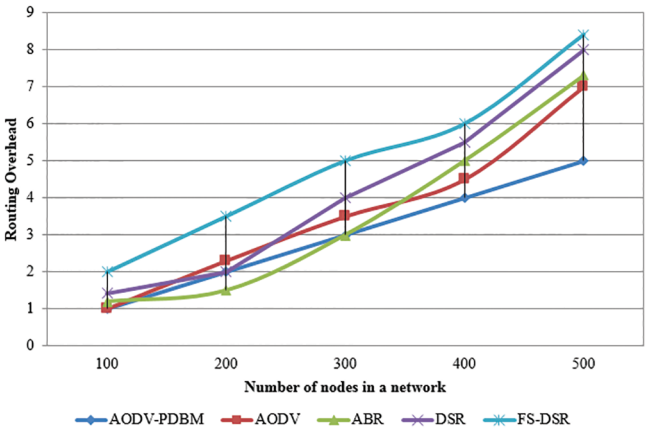

Figure 5: Graphical representation of routing overhead in a network

Fig. 6 illustrates energy use within a network. Energy consumption refers to the energy that the hubs consume in accepting packets from, and transmitting packets to, neighboring hubs. System implementation efficiency increases with decrease in energy consumption.

Fig. 7 presents a graphic representation of network performance within a network. Network throughput measures how many packets arrive at their destinations successfully during a specific period and is measured in bits per second.

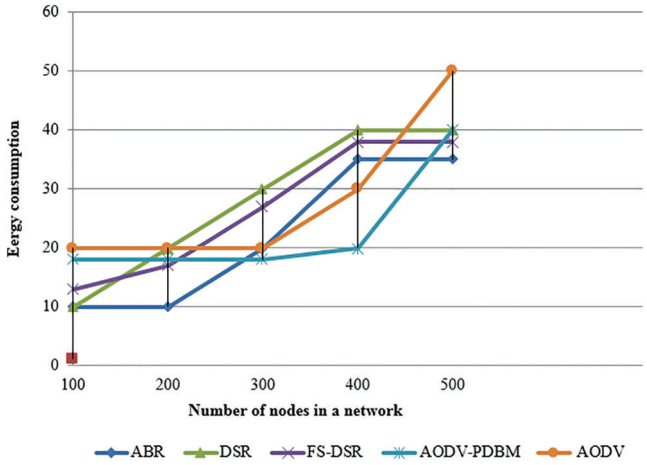

Figure 6: Graphical representation of energy consumption in a network

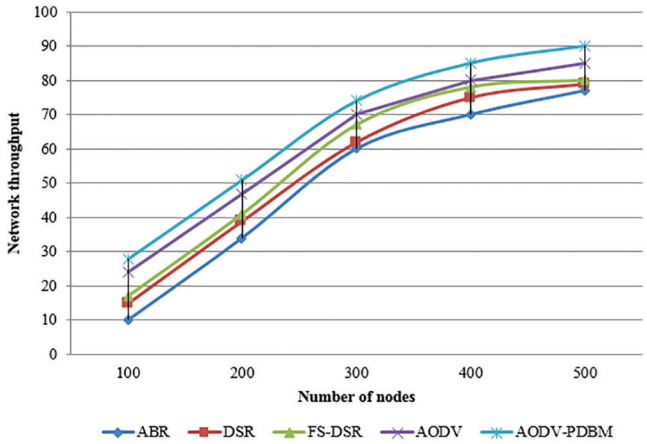

Figure 7: Graphical representation of network throughput in a network

6 Conclusions

This paper considered common security issues in a WMANet, including one of the commonly known rehashing attacks. It presented and discussed some of the solutions proposed by different network and security specialists. A multipath routing protocol was proposed to find the optimal route from sender to recipient as well as to expand system and ensure system security against attacks. We broke down the impact of these attacks by running a simulation using system parameters that organize the routing load, arrange throughput, packet conveyance proportion, packet loss and system energy consumption through the presented energy monitoring, the basic AODV and secure routing protocol. The discussed implementations demonstrate that the presented system identifies prevention measures from the attacks by comparing these with the fundamental AODV and builds a new organized execution. The AODV–PDBM was shown to be effective in the simulation environment, as it recognized malicious hubs with precision and latency. It is intended for use in WMANets, and will be a benchmark for implementation in comparative asset-constrained wireless communication gadgets/networks. The AODV–PDBM convention can be improved to add portability of the sensor hubs. Future research may include a further simulation of the proposed scheme for sparse mediums and in real-life scenarios as well as examine other metrics, such as the link layer overhead, pause time and path optimality.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Rohit, K. Taneja and H. Taneja, "Performance evaluation of manet using multi-channel mac framework," *Procedia Computer Science*, vol. 133, pp. 755–762, 2018.

[2] E. S. Kofi and K. M. Elleithy, "Real-time detection of dos attacks in IEEE 802.11 p using fog computing for a secure intelligent vehicular network," *Electronics*, vol. 8, no. 7, pp. 776, 2019.

[3] S. Hussain and M. S. Rahman, "Using received signal strength indicator to detect node replacement and replication attacks in wireless sensor networks," in *Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security, International Society for Optics and Photonics*. vol. 7344, pp. 73440G, 2009.

[4] A. Nehal, H. Kurdi and S. Al-Megren, "A hierarchical trust model for peer-to-peer networks," *Computers, Materials & Continua*, vol. 59, no. 2, pp. 397–404, 2019.

[5] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 3, pp. 1096–1101, 2019.

[6] A. Dhaka, N. Amita and R. Dhaka, "Gray and black hole attack identification using control packets in manets," in *Procedia Computer Science*, Elsevier, Netherlands, vol. 54, pp. 83–91, 2015.

[7] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of E-Collaboration (IJeC)*, vol. 16, no. 1, pp. 16–32, 2020.

[8] P. Panda, K. K. Gadnayak and N. Panda, "Manet attacks and their countermeasures: A survey," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 11, pp. 319–330, 2013.

[9] S. Radley and J. Janet, "Novel design, implementation and accomplishment of routing virtualization (rv) for IPv4-IPv6 coexistence using real time simulation (RTS)," *Taga Journal of Graphic Technology*, vol. 14, pp. 1810–1823, 2018.

[10] S. Radley, D. S. Punithavathani and L. K. Indumathi, "Transitional survey on IPv4-IPv6," *International Journal on Information Sciences and Computing*, vol. 7, no. 1, pp. 53–59, 2013.

[11] H. Hayouni, M. Hamdi and T. H. Kim, "A survey on encryption schemes in wireless sensor networks," in *Proc. 7th Int. Conf. on Advanced Software Engineering and Its Applications*, Copenhagen, Denmark, pp. 39–43, 2014.

[12] J. A. Chaudhry, U. Tariq, M. A. Amin and R. G. Rittenhouse, "Sinkhole vulnerabilities in wireless sensor networks," *International Journal of Security and its Applications*, vol. 8, no. 1, pp. 401–410, 2014.

[13] O. I. Khalaf and G. M. Abdulsahib, "Frequency estimation by the method of minimum mean squared error and p-value distributed in the wireless sensor network," *Journal of Information Science and Engineering*, vol. 35, no. 5, pp. 1099–1112, 2019.

[14] A. Gupta, "Mitigation algorithm against black hole attack using real time monitoring for aodv routing protocol in MANET," in *Proc. 2nd Int. Conf. on Computing for Sustainable Global Development*, St. Louis, MO, USA, pp. 134–138, 2015.

[15] K. Sachan and L. Manisha, "An approach to prevent gray-hole attacks on mobile ad-hoc networks," in *Proc. Int. Conf. on ICT in Business Industry & Government*, Indore, India, pp. 1–6, 2016.

[16] A. Siddiqua, K. Sridevi and A. A. K. Mohammed, "Preventing black hole attacks in manets using secure knowledge algorithm," in *Proc. Int. Conf. on Signal Processing and Communication Engineering Systems*, Guntur, India, pp. 421–425, 2015.

[17] P. Rani, S. Verma and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, pp. 121755–121764, 2020.

[18] A. Dorri and H. Nikdel, "A new approach for detecting and eliminating cooperative black hole nodes in manet," in *Proc. 7th Conf. on Information and Knowledge Technology*, Urmia, Iran, pp. 1–6, 2015.

[19] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma *et al.,* "An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks," *Journal of Systems and Software*, vol. 83, no. 11, pp. 2188–2199, 2010.

[20] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in manet: Merits, drawbacks, and suitability," *Wireless Networks*, vol. 26, no. 3, pp. 1981–2011, 2020.

[21] J. Qin, M. Li, L. Shi and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1648–1663, 2018.

[22] T. Poongodi, M. S. Khan, R. Patan, A. H. Gandomi and B. Balusamy, "Robust defense scheme against selective drop attack in wireless *ad hoc* networks," *IEEE Access*, vol. 7, pp. 18409–18419, 2019.

[23] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65–75, 2015.

[24] G. M. Abdulsahib and O. I. Khalaf, "Comparison and evaluation of cloud processing models in cloud-based networks," *International Journal of Simulation-Systems, Science & Technology*, vol. 19, no. 5, pp. 26.1–26.6, 2018.

[25] D. Dobhal and S. C. Dimri, "Performance evaluation of proposed-tcp in mobile ad hoc networks (manets)," in *Proc. Int. Conf. on Inventive Computation Technologies*, USA, vol. 2, pp. 1–6, 2016.

[26] I. Mobin, S. Momen and N. Mohammed, "A packet level simulation study of adhoc network with network simulator-2 (ns-2)," in *Proc. 3rd Int. Conf. on Electrical Engineering and Information Communication Technology*, Dhaka, Bangladesh, pp. 1–6, 2016.