Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A REVIEW OF BLACK HOLE ATTACK STUDIES IN WIRELESS SENSOR NETWORK

[1]ALI ALDUJAILI, [2]NAJMULDEEN HASHIM, [3]NURHIZAM SAFIE

[1]Department affairs of student accommodation, University of Baghdad, Iraq
[2] Faculty of Information Science and Technology, The National University of Malaysia (UKM), Bangi, Selangor, Malaysia
[3] Faculty of Information Science and Technology, The National University of Malaysia (UKM), Bangi, Selangor, Malaysia

E-mail: [1]ali@uobaghdad.edu.iq, [2] najmuldeen@siswa.ukm.edu.my, [3]nurhizam@ukm.edu.my

ABSTRACT

The specific application of ad-hoc network is a form of the wireless sensor network, that participates to achieve "smart sensing work" where the nodes are "smart sensors". This modern technology has been used innovatively in many sensing applications and observations in various domains - medical, banking security, and industry. MANET, referred to as a Mobile ad-hoc network, is a kind of ad-hoc network which depends on a set of auto-configuring mobile wireless points that are linked to change locations. for this large range of applications, and has been a promising and innovative research scope. The objective of the present study is to analytically review the previous studies and propose a path for the future. The proposed method used in this paper to analyze previous studies uses the content analysis approach. Furthermore, the limitations of wireless sensor networks include memory storage, the power of the battery, computational work, and range of communication in their system resources, which outline their defense against threats and performance. Based on the results, the present finding was that eleven types of research discussed the black hole attack in a wireless sensor network in different case studies.

Keywords: *Black Hole Attack, Wireless Sensor Network, MANET, Ad-Hoc Network, System Resources, Review.*

1. INTRODUCTION

Wireless technology is a very significant recent invention that enables machines and users to exchange data and move freely in the place without using wires, and transmit data, during electromagnetic waves similar to radio waves on various channels [1].

There are two kinds of wireless networks (WSNs) - ad-hoc network and infrastructure network. The ad-hoc category is a decentralized network where more than two nodes are linked to each other straight, without control or central administration. Infrastructure network, on the other hand, is a centralized network that links nodes during an access point to manage the inter-node communication [2]. MANET which is called a Mobile ad-hoc network is a kind of ad-hoc network which depends on a set of auto-configuring mobile wireless points that linked for changing locations [3].

According to [1], [4] Recent years, Mobile Ad-hoc Network has gained much attention of researchers in industrial and educational fields worldwide because of its easy set-up in disaster situations, the significance of its applications and its design.

Figure 1 illustrates the diagram of MANET (Mobile ad hoc network).

Journal of Theoretical and Applied Information Technology
15th June 2019. Vol.97. No 11

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

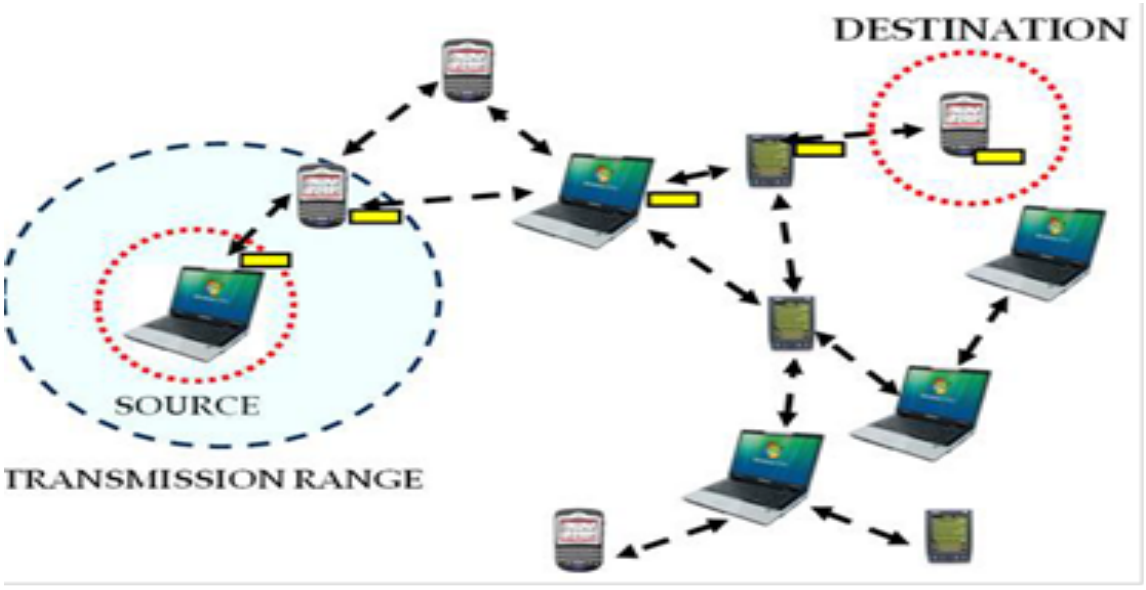

Figure1 : MANET (Mobile ad hoc network) [5]

1.1 Main challenges and attendant problems in the WSN

1.1.1 Wireless medium:

The wireless media used by the wireless sensor network is less safe than wired communication because of its nature. The opponent can easily intercept packets, inject malicious ones or simply jam the contacts [6].

1.1.2 Unfriendly environment:

In this environment, the infrastructure of the network structure and its registers are very weak and they can be captured or destroyed by attackers using the simplest means, and sensors cannot reveal the necessary information to deal with the attacks. Detecting the necessary information in this kind of environment can be difficult because sensors are helpless are exposed to physical attacks [6].

1.1.3 Enormous Scale network:

Safeguarding a sizeable network is a significant problem for security techniques. In particular, the sensor is limited in power and storage, so that no complicated mechanisms can be integrated [6].

1.1.4 Remote management:

Once installed, the sensor protection and all administrative configurations will be automatically completed and enable the administrator to keep it error-free and alive.[6]

1.2 challenges in MANET

1.2.1 Autonomous:

There is no centralized management entity available to manage the operation of the various mobile nodes.

1.2.2 Dynamic topology Nodes:

are mobile devices and can be connected dynamically in an arbitrary manner. The connections between the network differ in time and depend on the proximity of one node into another.

1.2.3 Device discovery:

Identifying newly moved nodes and informing them of their existence requires dynamic updates to facilitate automatic optimal route selection.

1.2.4 Bandwidth optimization:

Wireless connections have a much smaller capacity than wired connections, in wireless networks, routing protocols always optimally use the bandwidth by keeping the overhead as low as possible. The limited transmission range also imposes a limit on the maintenance of topological information on routing protocols, In MANETS due

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to frequent topological changes, the maintenance of topological information for all nodes should include more control overhead, resulting in the more bandwidth wastage.

1.2.5 Limited resources:

Mobile nodes depend on the power of the battery, which is a rare resource. furthermore, power and storage capacity is severely limited.

1.2.6 Scalability:

can be defined broadly as of whether the network can provide an acceptable level of service even when a large number of nodes are present.

1.2.7 Limited physical:

security Mobility entails higher security risks, such as peer to peer network architecture or a shared wireless media accessible to legitimate network users and malicious attackers alike. denial of service attacks should be taken into account, spoofing, and Eavesdropping.

1.2.8 Infrastructure less and self-operated

Self - healing feature requires MANET to redirect any node out of its range.

1.2.9 Poor Transmission Quality

This is an inherent problem of wireless technology caused by the degradation of the received signal from several error sources.

1.2.10 Ad hoc addressing

challenges to be implemented in the standard management scheme.

1.2.11 Network configuration

The entire MANET infrastructure is dynamic and is why the variable connections are dynamically connected and disconnected.

1.2.12 Topology maintenance

Updating information on dynamic links among nodes in MANETs is a major challenge.[7]

1.3 Types of MANET

According to [5], there are three types of MANET that can be concluded in the figure shown below:

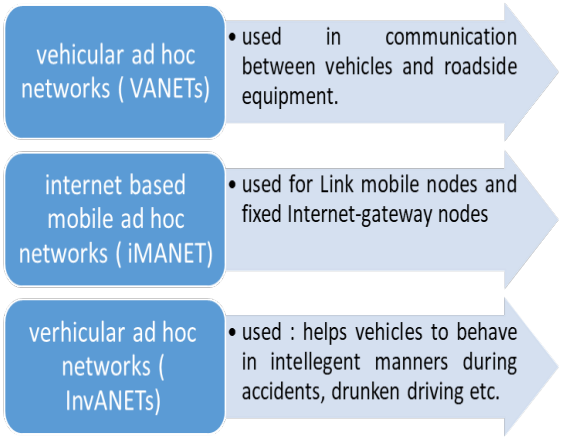

Figure2: MANET Types [5]

1.4 Security Requirements

1.4.1 Confidentiality:

This is the principle that provides protection for the data by keeping it secure from any unauthorized recipients and users. In most cases, the wireless sensor can also maintain sensitive data that need to be kept confidential and not disclosed to any neighbor sensor. The only way to ensure data are kept confidential is through encryption of such data with a secret key that alone can access the destination [8].

1.4.2 Integrity:

Even if the attacker is unable to steal the data due to the confidentiality, he can still alter them, add or remove certain fragments before they reach their destination. Data in WSN ought to be exact, regular and trustworthy. Integrity guarantees that transferring a message via nodes stays uncorrupted. [8]

1.4.3 Authentication:

This feature makes a node authenticate the other node it is communicating with to ensure that every data packet received is from the authenticated transmitter node, particularly crucial packets that contribute to a decision-making situation such as cluster election and selecting the shortest route. Hence, the trade of credentials is required to ensure authentication. [8]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1.4.4 Freshness:

Data in WSNs must be fresh and not something replayed. A timestamp choice or a time counter must accompany the packet to ensure its freshness. particularly when sensors are sensing the climate it must provide accurately-timed data [8].

1.4.5 Availability:

It is necessary to ensure that network services are continuous and not disrupted. In designing a WSN, such availability is essential and must be considered as a node that is involved in numerous computing activities as well as communication will run out of battery early, and data may not be ready [8].

1.4.6 Time synchronization:

As power is a significantly critical problem in WSN, synchronizing time is necessary to save energy. Sensors should be sleeping or deactivated when they are not needed for sensing [6].

1.5 Black hole attack

Black hole attack can be defined as a type of denial of service (DoS) using a malignant contract that disrupts the connection of the sensor network routing, forcing the nodes and the transmitter and receiver to disconnect packets instead of transmitting them [9]. In general, in this attack, the enemy listens to the path demands and responds via an announcement that it has the direct route to the goal point and the largest sequence number. Accordingly, in this way, the sender establishes the route with this malicious destination, as the more reliable. Since the attacker has arrived the packet objection aim and the routing table are altered maliciously, and it will figure out whether to forward selectively via the malicious node or delete all the packets, for instance, every type of packet or number of time slots or any random selection [10]. The enemy has two targets when running a black hole attack. The first target is in exhausting the battery of sensors and decreasing network lifetime. Second, is the dropping of all packets[10].

1.6 Layer Attacks in MANET

As indicated by [11][7], the layer attacks in MANET can be concluded in the table below:

Table 1: Layer Attacks in MANET [11], [7]

Layers	Attacks	Solutions
Physical layer	Traffic Jamming	Using Spread spectrum mechanisms FHSS,DHSS
	Eavesdropping	
	Active Interference	
Data Link layer	Selfish Misbehavior of Nodes	Secure link layer protocol like LLSP using
	Malicious Behavior of nodes WPA	
	DOS	
	Traffic Misdirecting	
	Attacking neighbor sensing protocols	
Network layer	Worm Hole Attack	Securing routing protocols like SAODV, SAR, ARAN to overcome black hole attack, impersonation attacks, packet leashes, SECTOR mechanism for wormhole attack
	Black hole attack	
	Byzantine Attack	
	Information Disclosure	
	Resource Consumption	
	Routing Attack Routing Table Overflow Routing Table Poisoning Packet Replication Route Cache Poisoning Rushing Attack	
Transport layer	Session Hijacking, SYN Flooding	Securing End to End communication (SSL, TLS, SET)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Application layer	The virus, Worms Dos, Malicious code, Man in the Middle Attack, Repudiation, Impersonation	Firewalls

2. MATERIALS AND METHODS

The present study emphasizes a review of the literature in relation to the topic of this article. In addition, the philosophical concepts that that form the basis of this study are related to the previous Black hole attack studies. Additionally, the purpose of this literature review is to determine the limitations of the current Black hole attack studies [12]. Also, it is to identify the future direction of these studies. The essential source of the data given is based on recent books, online academic citation databases, and journal articles.

The primary objective aim of this study was to examine the present Black hole attack overview in Wireless Sensor Network in many case studies. The content analysis approach is applied in this study, which adopts a qualitative research strategy that has been widely used to analyze oral and written or visual communication messages [13], [14] , [15]. Table 2 illustrate the black hole attack studies in a wireless sensor network.

Table 2: Black hole attack studies

Authors	Focus of Study	Methodology	Findings	Limitations/future work
[16]	Explains simulation results, gives more rapid message verification, distinguishes a black hole attack and detects the secure routing and averting the black hole attack.	Simulation	Shows the routing security problems of MANETs. and explains the black hole attack that can happen versus a MANET.	authors intend to evolve simulations to analyze the performance of the proposed solution based on different security parameters such as the packet delivery ratio (PDR).
[17]	Proposes a watchdog mechanism to reveal the black hole attack nodes in a MANET.	Watchdog mechanism	Devises a new protocol, called “Modified AODV.”	Mobile Ad-hoc network most probably to be attacked via the wormhole and black hole attacks.
[18]	Analyzed the influence of black hole attacks on mobile ad-hoc routing protocols.	Simulation	Examines the effects of two protocols, AODV and enhanced AODV under changing pause times.	The detection of black hole attacks in ad-hoc networks is viewed as a difficult task.
[19]	This study uses an algorithmic method to concentrate on analyzing and enhancing the security of AODV.	approach	A simulation study was provided to explain the impacts of black hole attack on network performance.	The better routing protocol for reducing the black Hole Attack may be established .

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20]	This article offers an insight into the possible applications of ad hoc networks, many attacks and discusses the technological challenges that protocol designers and web developers are confronted with.	Overview	Its lack of infrastructure, intrinsic flexibility, auto-configuration, ease of deployment, low cost and potential applications make it a crucial section of the future pervasive computing environment.	Especially the need for dense deployments like sensor networks and battlefield, cheaper, more capable, the nodes in ad-hoc networks will be smaller and come in all forms.
[21]	This research paper investigates the appropriate solutions and Develops a suitable solution to prevent the network from the gray hole attack.	Survey	AODV and modified-AODV are most common and beneficial routing protocols for the establishment of mobile ad-hoc networks. It also found that they do not have any vulnerable and security policy to various security threats.	The requirement to identify the vulnerabilities and raise its growth. The complete work considers Gray-hole attack as a crucial threat and will suggest a solution to overcome its issue.
[22]	The authors suggest the detection and reduction technique prevent black hole attacks and enhance network performance.	Study	Adversely affects the performance of AODV routing protocol when black hold attacks happen on it. The complete work concludes that the suggested solution successfully detects and alleviates the black hole attack in the mobile ad-hoc network.	Still, it is necessary to avoid the Black Hole attack in mobile ad-hoc networks.
[23]	The researchers suggest a new strategy to discover collaborative and single black hole attacks, with reduced routing and computational overhead.	Algorithm	Suggest two algorithms for the detection of collaborative and single black hole attacks.	Algorithms can be evolved to detect the existence of gray holes, which sometimes act like black holes, in mobile ad hoc network.
[24]	This study proposes a new method to discover the black hole attack utilizing a quality control chart.	Statistical Process Control (SPC).	We presented a procedure based on statistical process control. It allows us to observe the activity of the network in real time by dependence a single metric.	future work will concentrate on other methods to discover such attacks and making sure better communication.
[25]	The researchers implement Cache-based IDS on AODV	CBIDS-AODV protocol.	It concludes that the proposed method shows better performance	In the future, the performance of the proposed routing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	Routing Protocol with black hole attack.		against the AODV in terms of the packet loss ratio, throughput, and packet delivery ratio.	protocol can be extended for better scalability using fuzzy logic and neural networks.
[5]	This research focuses on preventing black hole attacks by utilizing the AODV routing protocol.	AODV routing protocol.	This study discusses the mitigating and detecting of black hole attacks in mobile ad hoc network.	Many studies have been done on the detection of black hole attacks but they did not utilize routing protocol for the betterment of the results.

According to [16], the authors explained the simulation results, which give faster message verification, distinguish a black hole attack and identify the secure routing in averting the black hole attack. Furthermore, the authors showed the routing security problems of MANETs. and explained the black hole attack that could occur versus a MANET. The method used in this research was a simulation. The limitation of this study is the author's intention to evolve simulations to analyze the performance of the proposed solution based on different security parameters such as the packet delivery ratio (PDR).

Another research [17] by proposing a watchdog mechanism to discover the black hole attack nodes in a MANET. The study by the authors also used a Watchdog mechanism as a method for their study. On the other hand, the determination of this study was Mobile Ad-Hoc network and the probability of it being attacked via the wormhole and black.

hole attacks. Furthermore, the finding of this study was to devise a new protocol, called "Modified AODV."

As stated by [18], the authors attempted to analyze the influence of black hole attacks on mobile ad hoc routing protocols to examine the effects of two protocols of AODV and enhance AODV under changing pause time. The method used in this research was a simulation. On the other hand, the researchers found the implications for future work would be the detection of black hole attacks in ad hoc networks, which would be as a challenging task.

According to [19] the study focused on a given algorithmic method to analyze and enhance the security of AODV. Moreover, a simulation study was provided to explain the impacts of black hole attack on network performance. In addition, the implications for future work included enhancing the routing protocol for reducing the black hole attack could be determined.

According to [20], this article offers an insight into the possible applications of ad hoc networks, many attacks and discusses the technological challenges that protocol designers and web developers are confronted with. The method used was a case study in the form of an overview. Although this research lacked an infrastructure, it, however, offered intrinsic flexibility, auto-configuration, ease of deployment, low cost, and potential applications which made it a crucial section of the future pervasive computing environment.

In addition, the implications for future work included especially the need for dense deployments like sensor networks and battlefield, cheaper, more capable, and the nodes in ad hoc networks would be smaller and come in all forms.

The research study by [21], investigated the appropriate solutions and developed a suitable solution to prevent the network from gray hole attacks, using the survey as their approach. Furthermore, the researchers showed that AODV and modified-AODV are most common and beneficial routing protocols for establishing mobile ad-hoc networks. They also found that they do not have any vulnerable and security policy to counter various security threats. The authors found that this topic needed to identify the vulnerabilities and raise its growth. The complete work considers the gray hole attack as crucial threats and suggests a solution to overcome its issue.

As stated by [22], the researchers noticed that detection and reduction technique could prevent

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

black hole attacks and enhance network performance. In addition, they used the case study as their approach. On the other hand, the approach adversely affects the performance of AODV routing protocol when confronted by black hold attacks. The complete work concludes that the suggested solution successfully detects and alleviates the black hole attacks in the mobile ad-hoc network., The authors also found there were still problems to be solved to avoid Black Hole attacks on mobile ad hoc networks.

In addition , according to [23], the authors proposed a simulation which uses a new strategy to detect collaborative and single black hole attacks, with reduced routing and computational overhead., The method used to collect the data in this study is an algorithm. Furthermore, it suggested the use of two algorithms for the detection of collaborative and single black hole attacks. In addition, the implication of this research was that algorithms could be designed to detect the existence of gray holes, which sometimes act like black holes, in mobile ad hoc network.

In another study [24] the author examined a technique for the detection of a black hole attack utilizing a quality control chart based on statistical process control. It allows the observation of the activity of the network in real time by depending on a single metric. The method used in this research was Statistical Process Control (SPC). In addition, the author added that future work would concentrate on other methods to detect such attacks and ensure better communication.

As highlighted by [25], the authors implemented Cache-based IDS on AODV Routing Protocol to handle any black hole attack. The method used in this study was CBIDS-AODV protocol. In addition, the result also showed that the proposed method exhibited better performance against the AODV in terms of the packet loss ratio, throughput, and packet delivery ratio. Moreover, in the future, the performance of the proposed routing protocol can be extended for better scalability using fuzzy logic and neural networks.

According to an investigation by [5], which illustrates the prevention of black hole attacks by utilizing the AODV routing protocol, this study used AODV routing protocol as its approach, In addition, the authors showed that several studies have been done on the detection of black hole attacks but they did not utilize routing protocol to improve the results, Furthermore, this study dealt with the mitigation and detection of black hole attacks in mobile ad hoc networks.

There are many review papers in this area of Black Hole attack where each of these previous researches examining specific features or properties and methods to solve and reduce attacks of Black Hole Attack, we review some of these related published reviews researches:

according to [26] the article discussed various techniques for detecting and preventing MANETs from black hole attacks, this study suggested different solutions and methods to overcome and prevent this attack such as modify of AODV protocol, SRD, route authentication based on the rank of nodes, a mobile agent that roams around a mobile ad-hoc network.

Another study by [27], this author presents a comprehensive survey of the known approaches to black - hole detection and prevention, and a new dimension for their classification. In addition, they suggested new solution for the black-hole attack in MANET that should be, accurate fast and lightweight. The network bandwidth or node power should also not be wasted and can handle the cooperative black - hole attack.

As stated by [28] the researches takes several types of attacks then discusses one of the most severe attack in the network is a black hole attack. Black hole attack classified into three groups: Protocol Modification, Intrusion Detection and Counter Measure and Protection based on Cryptography.

Another review research [29], the authors attempted various categories of black hole attack mitigation techniques and also presented a summary of different techniques and their drawbacks to being considered when designing an effective protocol, In addition, the researcher was helpful in the design of combating for packet dropping attack protocols in MANET.

As highlighted by [30] the authors implemented and applied the OLSR protocol and find out that some of the effects of these attacks are stopped, but the network cannot be safe from these attacks. Also found that attacking of Black hole attack is easy to detect than attacking the Grey hole. There is not much difference in both attacks at the performance level.

Another study by author [31] show security attacks in wireless sensor networks and focused on comparing and analyzing recent WSN intrusion detection schemes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Finally, as stated by [32] the author examined a review of different existing black hole detection and mitigation techniques.

This research differs from the other review researches because it is concluding a summary of most of the researches that have study the Black Hole attack in terms of focus of study, methodology, finding, limitation and future work for each.

3. RESULTS AND DISCUSSION

The discussion of the results begins with the different black hole attack studies identified in the literature featuring different case studies of the wireless sensor network. The findings of the current study show eleven types of research discussed the black hole attacks in a WSNs. Among the possible explanations for these findings is that five types of research discussed the AODV (ad hoc on demand distance vector) protocol and another study discussed MANET (a mobile ad hoc network). Another important finding was the gray hole attack. Moreover, it was also shown that two major findings belong to the algorithm detecting single and collaborative black hole attacks and the applications and ad hoc network. Another study focused on SPC (Statistical Process Control). Finally, another author also showed the use of CBIDS-AODV protocol. As mentioned above most studies examined the AODV (ad hoc on demand distance vector) but very few studies examined SPC. These studies are categorized in Table 3.

Table 3: Showing significant differences between the seven groups.

MANET (mobile ad hoc network)	1
AODV (ad hoc on demand distance vector)	5
Applications and ad hoc network	1
The algorithm to detect single and collaborative black hole attacks	1
SPC (statistical process control)	1
Gray hole attack	1
CBIDS-AODV protocol	1

4. LIMITATION AND FUTUREWORK

The limitation of this study that there are many different studies and illustrates in various attacks that made it difficult to study and understanding the black hole attack so it takes a lot of time and effort to gather this amount of data, understand the subject correctly and summarizing this topic and taking most studies over the last seven years.

Furthermore, the future work of this research, present an article that would like to conduct a more comprehensive study of the most attacks on MANET and include more years in the abstract for the benefit of researchers in knowledge and more familiar with this subject.

5. CONCLUSION

The specific application of ad-hoc network is a type of WSN, that participates in achieving "smart sensing work" where the nodes are "smart sensors". MANET can be termed a Mobile ad hoc network and is a kind of ad-hoc network depending on a set of auto-configuring mobile wireless points that are linked to change locations. The purpose of this study is to determine the limitations of the current black hole attack studies. In addition, it is to identify possible directions for future work of this research topic. Furthermore, the primary objective of this study is to examine the present black hole attack scenario in Wireless Sensor Networks in many case studies. The content analysis approach is the method that was used in this study. The present findings indicated that eleven types of research discussed the black hole attack in wireless sensor networks.

REFERENCES

[1] B. D. Shivahare, C. Wahi, and S. Shivhare, "Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property :," vol. 2, no. 3, pp. 356–359, 2012.

[2] "black hole attack." [Online]. Available: https://en.wikipedia.org/w/index.php?title=Wireless_ad_hoc_network&oldid=855160001..

[3] R. Dilli and P. C. S. Reddy, *Robust Secure Routing Protocol for Mobile Ad Hoc Networks (MANETs)*. Springer Singapore.

[4] I. Chlamtac, M. Conti, and J. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, pp. 153–158, 2003.

[5] R. Garg and V. Mongia, "Mitigation of Black Hole Attack in Mobile Ad-Hoc Network Using Artificial Intelligence

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Technique," vol. 3, no. 1, pp. 1168–1174, 2018.

[6] D. G. Padmavathi and M. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 1, pp. 1–9, 2009.

[7] M. Computing, "An Overview of MANET : Applications , Attacks and Challenges Abstract :," vol. 3, no. 1, pp. 408–417, 2014.

[8] T. Kavitha and D. Sridharan, "Security Vulnerabilities In Wireless Sensor Networks : A Survey," *J. Inf. Assur. Secur.*, vol. 5, pp. 31–44, 2014.

[9] S. N. Mohammad, R. P. Singh, A. Dey, and S. J. Ahmad, *ESMBCRT : Enhance Security to MANETs Against Black Hole Attack Using MCR Technique*. Springer Singapore, 2019.

[10] S. Om and M. Talib, "Wireless Ad-hoc Network under Black-hole Attack," pp. 1–6.

[11] J. G. Ponsam and R. Srinivasan, "A Survey on MANET Security Challenges , Attacks and its Countermeasures," vol. 3, no. 1, pp. 274–279, 2014.

[12] N. S. and M. M. Najmuldeen A. Hashim, "A Review of e-Learning Models for Deaf and Hearing Impaired People," *J. Eng. Appl. Sci.*, vol. 13, no. 21, pp. 9029–9037, 2018.

[13] N. Hashim, N. Safie, and M. Mukhtar, "Assessing the Determinates of Cloud Computing-Based E-Learning Systems for the Deaf in Iraq : a Preliminary Study," vol. 10, pp. 634–639, 2018.

[14] A. Meri, M. K. Hasan, and N. Safie, "The impact of organizational structure and system settings on the healthcare individual's perception to utilize cloud services: A theoretical literature survey," *J. Eng. Appl. Sci.*, vol. 13, no. 4, pp. 888–897, 2018.

[15] S. Omar, M. Radzani, M. Yasin, and M. Dauwed, "Validity and Reliability Questionnaire for Social, Environment and Self-Efficacy Related of Deaf Adolescents Physical Activity," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 21, 2018.

[16] P. Jaiswal, "Prevention of Black Hole Attack in MANET," vol. 2, no. October, 2012.

[17] A. A. Bhosle, T. P. Thosar, and S. Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET," vol. 2, no. 1, pp. 45–54, 2012.

[18] J. Kumar, M. Kulkarni, and D. Gupta, "Effect of Black Hole Attack on MANET Routing Protocols," no. April, 2013.

[19] R. Das, B. S. Purkayastha, and P. Das, "Security Measures for Black Hole Attack in MANET: An Approach," pp. 1–7, 2012.

[20] L. Raja and C. S. Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges," *Int. J. Comput. Sci. Mob. Comput.*, vol. 3131, no. 1, pp. 408–417, 2014.

[21] R. Sharma, "Gray-hole Attack in Mobile Ad-hoc Networks : A Survey," vol. 7, no. 3, pp. 1457–1460, 2016.

[22] M. Puray and P. College, "Black-Hole Attack in MANET : A Study," vol. 5, no. 3, pp. 597–601, 2016.

[23] K. S. Arathy and C. N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET," *Procedia Technol.*, vol. 25, no. Raerest, pp. 264–271, 2016.

[24] B. Cherkaoui, A. Beni-Hssane, and M. Erritali, "Quality Control Chart for Detecting the Black Hole Attack in Vehicular Ad-hoc Networks," *Procedia Comput. Sci.*, vol. 113, pp. 170–177, 2017.

[25] R. L. Rao, P. B. Satyanarayana, and B. Kondaiah, "Performance of CBIDS on AODV Routing Protocol against Black hole attacks in MANET," vol. 3, no. 3, pp. 1637–1644, 2018.

[26] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," *2017 Int. Symp. Wirel. Syst. Networks, ISWSN 2017*, vol. 2018–Janua, pp. 1–4, 2018.

[27] A. Sherif, M. Elsabrouty, and A. Shoukry, "A novel taxonomy of black-hole attack detection techniques in mobile ad-hoc network (MANET)," *Proc. - 16th IEEE Int. Conf. Comput. Sci. Eng. CSE 2013*, pp. 346–352, 2013.

[28] S. Mandala, A. H. Abdullah, A. S. Ismail, H. Haron, M. A. Ngadi, and Y. Coulibaly, "A review of blackhole attack in mobile adhoc network," *Proc. 2013 3rd Int. Conf. Instrumentation, Commun. Inf. Technol., Biomed. Eng. Sci. Technol. Improv. Heal.*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Safety, Environ., ICICI-BME 2013, pp. 339–344, 2013.

[29] S. Gurung and S. Chauhan, "A review of black-hole attack mitigation techniques and its drawbacks in Mobile Ad-hoc Network," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018–Janua, pp. 2379–2385, 2018.

[30] R. Kaur and P. Singh, "Review of Black Hole and Grey Hole Attack," *Int. J. Multimed. Its Appl.*, vol. 6, no. 6, pp. 35–45, 2015.

[31] A. Ezzati, "a Review of S Ecurity a Ttacks and I Ntrusion D Etection S Chemes in W Ireless."

[32] M. Mistry, P. Tandel, and V. Reshamwala, "Mitigating techniques of black hole attack in MANET: A review," *Proc. - Int. Conf. Trends Electron. Informatics, ICEI 2017*, vol. 2018–Janua, pp. 554–557, 2018.