ISSN 2278-3091
Volume 8, No.1.2, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1781.22019.pdf
https://doi.org/10.30534/ijatcse/2019/1781.22019

Prevention Techniques Employed In Wireless Ad-Hoc Networks

Ravi Tomar[1], **Yogesh Awasthi**[2*]
[1]School of Engineering & Technology, Department of CS,Shobhit Institute of Engineering & Technology Meerut, India, ravistc1@gmail.com
[2]School of Engineering & Technology, Department of CS, Shobhit Institute of Engineering & Technology,Meerut, India, yogesh@shobhituniversity.ac.in
[*]Present Address: Assistant Professor, Department of Computer Engineering, Lebanese French University, Erbil,KR- Iraq, dryogeshawasthi@lfu.edu.krd

ABSTRACT

The paper emphasizes the various aspects of ad-hoc networks. The different types of attacks that affect the system and are prevented by various algorithms mentioned in this paper. Since Ad-hoc wireless networks have no infrastructure and are always unreliable, therefore they are subject to many attacks. The black hole attack is seen as one of the dangerous attacks of them. In this attack, the malicious node usually absorbs each data packets that are similar to separate holes in everything. Likewise, all packets in the network are dropped. For this reason, various prevention measures should be employed in the form of routing finding first then the optimization followed by the classification.

Key words : MANET, VANET, Artificial Bee Colony, Genetic Algorithm.

1. INTRODUCTION

Ad hoc networks are an essential factor in the evolution of wireless communications. These networks come into with usual problems of Optimization of Bandwidth, control of power and enhancement of transmission quality. Lack of proven infrastructure and multipurpose nature, such as network configuration, surveillance protection and problems related to self-reliance. In these networks, equitable nodes are included without interconnection. The attack occurs with some opponent on sensor node subset. As the data packets are not sent by the nodes, thus they are captured and re-programmed. They are sent from packages or sensor nodes generated by them, which are forwarded. It's a fresh approach towards a wireless communication for nodes known as mobile hosts. There is no fixed infrastructure in this network such as BS (Base station) or mobile switching centers. The nodes which are under the range communicate directly through links and on the flip side, the distant nodes communicate through other nodes called as routers. In the coming era, the spotlight is on the capabilities of short-range data. These networks are also used for emergency as well as rescue missions. It is a very nasty choice for most of the tasks employed by the sensor network, such as relatively low cost. Types of Ad-hoc Networks are mentioned below:

1.1 MANET

It is a network having mobile devices allied through wireless links. In this network, all nodes independently follow mobility routine and have no centralized authority. For this reason, attacker with no trouble comes into the network and hence, malicious activities are performed. To triumph over this issue various security architectures are proposed for Mobile Ad hoc Networks (MANETs). A set of nodes which move freely to communicate over a multi-hop radio network without depending upon stable infrastructure. In this type, every node behaves as a client plus the router. [1] There are two kinds of contact that are carefully monitored by the protocols for MANETS:

- Broadcast communications
- Multi-hop communications

There are two typical features associated with them are:

- Constant changing of topology.
- The unreliability of wireless links between nodes.

Each device can freely move in MANET independently in any of the direction. For this reason, it will change the link to other devices. Each should forward the unrelated traffic to be a router. Mainly based on the management of any device, the information needed for the appropriate traffic is to be maintained. Such networks can work on the locked internet or by their own. This has led to a larger growth of laptops and Wi-Fi networking. These mobile networks have the following features:

- The wireless link between the nodes is highly vulnerable. As nodes move continuously due to the repeated breakdown. The transmission power is limited.
- Nodes are constantly transmitted from the radio range. This gives you an overview of results.
- The constraint of bandwidth in the wireless networks.
- Every node is dependent on the battery which is a limited source, the operation is energy efficient.

1.2 VANETs

By Vehicular Ad hoc networks communication takes place through wireless communication networks between every vehicle and other vehicles. They help with more experienced roads in the future to provide timely information to drivers and relevant officials. VANETs are almost like MANETs; the major difference is that the vehicles move in an organized manner rather than moving randomly. The vehicles are in a zone and have a range of motion and it can be predicted in a shorter time as they obey traffic rules. [2] In VANETs, telecommunications are linked via wireless connections that are installed in every vehicle node. The building is not determined by nature by its organization. The VANET participating car changes every car into Beirut's node with the vehicles that drive approximately one to 300 meters of vehicles and develop a network having wide network. When the car leaves the signal range and exits the network, other cars can join and connect the vehicles to each other so that the mobile Internet can be created. This is a promising approach to the future Intelligent Transportation System (ITS).

1.3 Wireless Body Area Networks (WBAN)

WBAN is a radio frequency (RF) based wireless network technology that interconnects nodes with sensing units. This node supports several medical as well as non-medical applications within a few centimetres of the human body. Sensor uses WBAN medical tape to obtain physical information from the node. The medical band is chosen to reduce the interference and therefore, increase coexistence with sensor node devices having another network device obtainable in the medical center. Then use the Medical Gateway for Wireless Board to send information collected from the remote station to the multi-hop technology. [4]

2. RELATED WORK

Mir Athmani et.al [4] Due to its own distinctiveness, WSN are highly susceptible to malicious attacks. Black hole is the most important malicious attacks targeting sensor-guided protocols. Hierarchical routing protocols could be affected devastatingly. [5] For security, the code from this attack presented some security solutions to secure WSNs. In any scenario, a significant part of these solutions is convoluted and inefficacious in energy. In this proposal the author has mentioned a hierarchical energy efficient IDS for protecting the sensors from black hole attacks. [6] It is simple approach is dependent on the exchange of control packets among sensor node as well as base station. They evaluated our system by experimentally using an NS simulator to demonstrate their effectiveness in detecting and preventing black hole attacks. Anbuchelian. S et.al has proposed an algorithm to detect the threat of cluster headers and efficiently consume energy in WSN. A grey hole attack is taken as a black hole attack that drops the selective packets from a malicious node. Network Load Balancing between cluster and unified cluster sites and extension of WSN [7]. The potential variables used are average delay, output ratio and end-to-end delivery. The PDR (packet delivery rate) is the number of packets received to the packets that were created. In paper [8], the researchers proposed a new authentication mechanism to safely transfer messages in a VANET scenario. The author has shown that the existing message authentication technology is based on a common signature technology. The redirect node uses a common signing algorithm via RSU and produces a large text message for transmission. Because of the unified signature scheme, the RSU sometimes sends fake authentication messages towards the contract. To avoid such problems, the authors proposed the technique of the aggregated message authentication code that confirm the honesty and credibility of the messages. [9] Kyung Yang, et al. [10] The design was performed together with the On-Board Units application in VANET for highways known as V2V connections. On-Board Units consists of four modules, human and machine interface module, central controller module (CCM), GPS unit and wireless communications unit. The hardware part includes, the ARM11-based chipset, the DCMA86P2 module, and the GPS. [11, 37] The software part includes embedded linux program. Following to the testing, the results proves that On-Board Units (OBU) are ready to send and receiving of the information to command the safety aid of the vehicle, besides achieving all the essential functioning and can work securely.

3. CLASSIFICATION OF ATTACKS

3.1 Black Hole Attack

It is defined as an attack which usually occurs with some adversary on sensor node subset. A subset in the network is called, like a black hole attack, an external opponent attack. As the data packets are not sent by the nodes, thus they are captured and re-programmed. They are sent from packages or sensor nodes generated by them, which are forwarded.

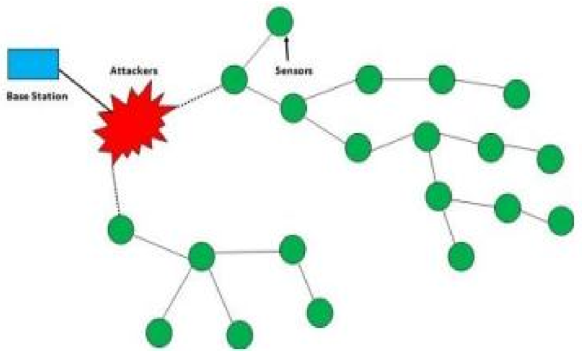

Figure 1: Black Hole

Black hole nodes to be known as reprogrammed nodes, also are known as black holes in areas that contain such nodes.

As shown in Figure 1, Sensors are held by the small green circles, and the areas they occupy are taken as the black hole of the area. If the path is specified so that the attacker's node is included in it when the passage goes through its opponent's node, the contract begins to drop packets selectively or completely. The contract known as the black hole contract is known as the area held by the black hole region. This area is the gateway to huge attacks [4]. Attacks and loss of packets greatly affect the activities within the network, and delay factors are increasing, however, network bottlenecks are reduced.

3.2 Sinkhole Attack

In this type of attack, the attacker makes an attractive compromised node for the nearby nodes by building the route data [12, 13]. The result is that the surrounding nodes will select the compromised node as the preceding node to transmit their data. This attack makes vulnerable node very simple to choose, because every transmission from the large area of the network flows through the enemy nodes.

3.3 Denial of Service (DoS)

A DDoS is type of attack in WSN which disables the server for servicing a client. In this type of attack, the attacker imparts several requests to the server and with large packets of random or invalid data so that the server is slowed down. This attack is one of the very common. [14] The simplest DoS attacks try to use the resources available to the victim node by sending unnecessary packets and preventing them from being exploited. [1] [2] DoS attacks are meant to be not only However, the opponent's efforts to destroy, destroy or destroy the network. [2] In wireless sensor networks, there may be multiple DoS attacks on multiple layers. In the physical layer, DoS attacks may cause interference and spoofing, link layers, collisions, weakness, injustice at the network layer, reject and selfishly desire, homecoming, transport layers and black holes. May be made by a dangerous flood and resynchronization.

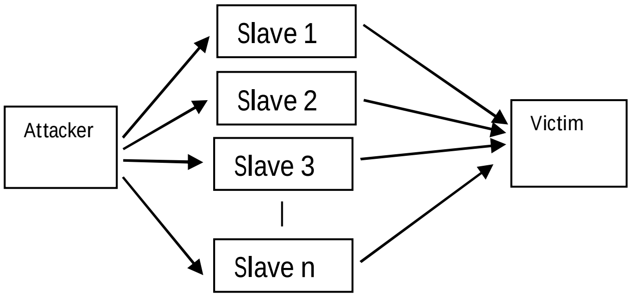

Figure 2: Illustrating DoS attacks

3.4 The Wormhole Attack

It can be defined as “An attacker prepares a low-latency, large-scale secret channel between two remote locations in a wireless sensor network. It then registers the packets in one spot, transmits them across secret tunnel, and restarts them in the other spot. The restarted packets may be new because the channel has low latency. For instance, a node (sender) in the network transfers a message towards another node (receiver node) in the network [15]. The receiving node then attempts to transfers a message to its neighbour. Then the message is sent from the sender node (generally not in range) considerably by the neighbour node, so the sender tries to forward the message to the very first specified beginner node, but it not ever approaches because it is very far away. Wormhole attacks are a crucial threatening remark for WSN because they do not require disruption of sensors in the network. Instead, they can be performed even when the sensor begins to discover the initial stages of neighbouring information [10]. Wormhole attacks are tough to combat as the information provided for routing by the nodes is hard to validate.

3.5 Eavesdropping

In the process of eavesdropping the information is gathered from a network by spying on the data transmitting through the network. Private data transmission is heard secretly illegally. Thus, the information is untouched but is no more a secret.

In wireless networks Eavesdropping is done by connecting the computer to the network in such a way that each transmitting data packet is intercepted and read with the help of specific software programs that allows eavesdropping over WSNs. [16]

3.6 Routing Message Flooding Attack

In Routing Message Flooding Attack the attacker inject the nodes of the network with fake control packets which are loop in the network unnecessarily and consume the network resources. [17] Thus the network is adversely affected and finally the network goes down and becomes unavailable. [18]

3.7 Rushing Attack

In this attack two coordinated attackers create a tunnel and transmit the data through it very fast over the dedicated tunnel path. The data in the tunnel moves faster than that of the data transmitting in the network. This creates a rush of data in the network and creates a rushing attack. The type of attack also increases the consumption of network resources and could result in complete denial of service. This type of attack also bypasses most of the security protocols created and implemented to secure the network from attacks, such as ARAN and Ariadne. [19]

3.8 Fabrication Attack

Fabrication attacks the authenticity of the data transmitted as the attacker injects the false data packets into the network [20]. The Fabrication attack or also known as the Link Fabrication Attack aims to pretend to the network that a direct inter-switch exists between the two networks, when there is not. The network controller thinks that there is a connection between switches by having them flood network frames from all ports. [21] Thus, the neighbouring switches gets flooded with network traffic and thinks that there is a link between them and passes the Layer Link Discovery Protocol (LLDP) and enters the network topology. Further to which the network is linked with latencies to be automatically discovered reducing the configuration burden and attracting network controllers. [22]

Table 1: WSNs Attacks Comparasion

Attack	Security Class	Attack Threat	Attacker Location	Active / Passive
Blackhole Attack	Interception	Confidentiality	Internal	Active
Sinkhole Attack	Fabrication	Integrity	Both	Active
DoS	Interruption	Integrity	Both	Active
Wormhole Attack	Fabrication	Authenticity	External	Active
Eavesdropping	Interception	Confidentiality	Both	Passive
Routing Message Flooding Attack	Interruption	Viability	Internal	Active
Rushing Attack	Interruption	Availability	Internal	Active
Fabrication Attack	Fabrication	Availability	Both	Active

4. ALGORITHMS USED FOR PREVENTION

There are numerous prevention strategies that have been presented by means of their performance and classification. It acts as a protection system for the networks. They are named as routing protocols, optimization techniques, and classification.

4.1 LEACH

The goal of the LEACH Leader Cluster is periodically replaced between the nodes of the network to share power consumption. Productivity LEACH depends on rounds. Then each cluster leader will be elected. The number of nodes and clusters of managers that are not clustering leaders is used for this choice. After the cluster, the head is detected during installation, it creates a TDMA table for messages in the group [23]. This allows you to turn off their scheduling interfaces when not using them. The cluster head is a router to the sink and responds to data fusion. When the sensor control head cluster which is located next to you, it eliminates this leader's merge data. The edition of this Protocol is LEACH-C, where C is centralized [24]. This scheme is also based on the time phases set to set the phase and phase constant. During installation, the sensors respond to the base station of their position and their energy levels. In doing so, the BS manages the cluster structures and their respective clusters. Because the BS is fully aware of the state of the network, the LEACH-C cluster structure is optimized for Lich results.

4.2 PEGASIS (Power-Efficient Gathering in Sensor Information Systems)

PEGASIS is an extended version of LEACH. The formation of chain takes place in this algorithm rather than forming nodes. The receiving takes place only from one of the close neighbours and responds to this criterion of structure. To this end, the nodes regulate the strength of their broadcasts [25]. The node collects data and sends it to the node in a row that connects to the sink. One node is identified in the circuit identified to connect with the aquarium. The series is built with a greedy algorithm.

4.3 Genetic Algorithm (GA)

GA is generally used in the applications with more search space. The benefit of GA is that the process is fully automatic and evades the local minima [15]. GA consisted of several components, namely, Crossover, Fitness function and mutation. The crossover operation is used for generating a new chromosome from parents set but the mutation operators add variation. Fitness function is utilized for executing a chromosome which is dependent on the survival chance. The population is the collection of chromosomes. The novel population is executed by using standard GA operations, like Single point Crossover, Selection operator and mutation. The procedure for the execution of the genetic algorithm is defined below and shown in Figure 3:

Step 1: Initialization of arbitrary population with chromosomes.
Step 2: Fitness function in the population to be calculated.
Step 3: Development of new population having individuals
Step 4: Selection of parent chromosomes for the better fitness function
Step 5: Calculate crossover for having a copy of parents
Step 6: Calculation of mutation for mutating the new offspring
Step 7: New population of offspring.
Step 8: Iterate the steps for the better solutions
Step 9: Stop

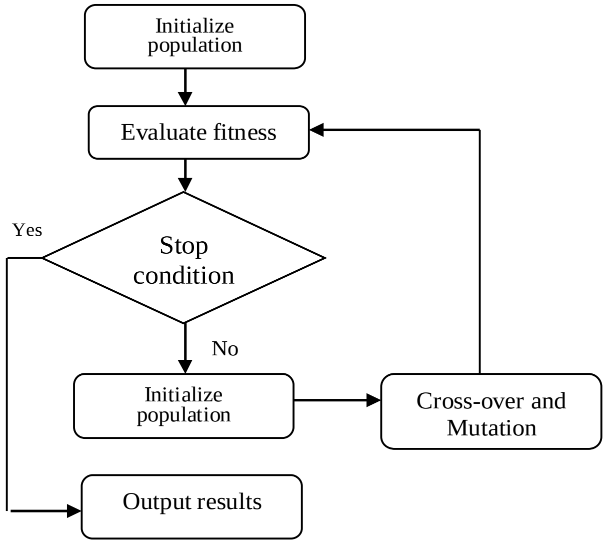

Figure 3: Flowchart of the GA working

4.4 ABC Algorithm (Artificial Bee Colony)

ABC was put forward by Karaboga in 2005 for the actual improvement of parameters, which mimics the functioning of the search for bee colonies [26]. According to algorithm, every cycle has 3 steps: first the user bees are sent to the food origin and the nectar data is checked. When the nectar data is shared, then the food origin are searched by the bees and execute the nectar consignment. Scouting bees are randomly sent to new possible food sources. In the initialization phase, the bees randomly select different food sources, and their nectars are made insistent. At the very beginning of the bee cycle, the bees reach the cell and share the nectar data with the origin with the bees, which are expecting in the dance area. The bee waiting in the dance area makes the decision to choose a food origin by a picnic and have a picnic that the food origin visited on its own before the bees are busy. After exchanging information with the audience, each Worker Bee moves to the area of the power source that she visited. Evaluated at the previous session, where the food origin is in her memory, she selects a new food source through visual data in the area where her memory is located and the amount of her nectar. In the second step, the bee viewer prefers feeding the origin area, based on the nectar data distributed by the bees working in the dance area. The greater the amount of nectar for a food source, the more likely it is to choose this food source. After reaching in a designated area, she chose a new power origin in an area that is in memory depending on visual data, as is the case with bees being used. Following in the third and final cycle step, scouts identify the bees of the novel food source when the nectar is discarded by the bees and replaced by abandoned bees. In work of prevention in most sessions, most Scouts quit to find a new power origin and the number of worker bees and the audience decided to be equal. These three steps are repeated after a certain number of cycles, called the maximum number of cycles (MCNs) [27][28].

4.5 Neural Network (NN) Algorithm

This is a mathematical model, or a specific arithmetic model based on biological neural networks. The NN workbook relies on a neural network with interconnected neurons [23]. The neurons have positive as well as negative stimuli that are a numeral value taken from another neuron and when the weighted total of stimuli is more than the provided threshold value and it gets activated. The outcome of the neurons is generally a non-linear change of stimuli sum. Neural networks are the neurons in the graphs. NN is modelled as a graph as a compilation of neurons that are integrated into an acyclic graph. It can also be said that the outcome of a few neurons can result in the input to another neuron. NN is generally connected into different neuron layers. For usual NN, the frequently utilized layer type is a fully connected layer having neurons among two distinct layers which are completely paired wise integrated, but the neurons having a single layer with no connection.

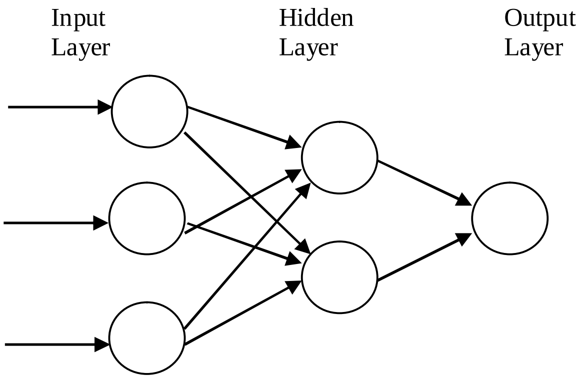

Figure 3: Neural Network

5. PREVENTION TECHNIQUES

5.1 DoS Prevention

Wood and Stankovic [29] explains how a problem can arise in different layers of any network due to DoS attack. It can over consume the network resources by injecting extra data packets into the network. Therefore, every network user should be authorized only after the verification of the user with its malicious nature.

5.2 Blackhole Attack Prevention

Blackhole is one of the most important security issues in the WSNs. Using protocols such as RREP and ADOV avoids blackhole attacks to an extent. Blackhole attack can be observed in WSNs; as it doesn’t require a sensor in the network to complete the attack and the prevention can done at the starting state when the sensor start to observe that there is a network activity in the neighboring node. [30]

5.3 Sinkhole Attack Prevention

Geographic Routing Protocols is one of the protocols used to prevent Sinkhole Attacks. This type of attacks is very tough to avoid Geographic Routing Protocols creates a temporary topology in which only local data is passed within the network, without communicating with the main station. [31] [32]

6. CONCLUSION

There have been several advancements in the field of WSNs in the past period. Keeping in mind our motive is to highlight the venerable flaws in the Ad-Hoc Networks and make them more and more secure. VANETs is a type of wireless network that is created for relaying messages between neighbouring vehicles, and also neighbouring vehicles with fixed equipment that are present on the side of the road. The most user’s concerns in VANETs is the effects of the attack on the system and the presence of security in VANETs. Because security is an important requirement in MANETs. Due to the mobility network and its wireless nature, malware nodes can enter the network at any time. It is necessary to consider the safety of the nodes. Because wireless ad hoc networks do not have the infrastructure, they are the subject to many attacks. To prevent such attacks from their impact, you need to protect your system in the early stages of the attack. Combining routing algorithms with appropriate optimization techniques as mentioned above there may be an optimal solution. I hope that this paper will encourage researchers to develop more secure WSNs.

REFERENCES

1. Gupta, N. and Singh, P. **Prevention of Gray Hole Attack in MANET using Fuzzy Logic**, 2017
2. Thilak, K. D. and Amuthan, **A. Cellular Automata-based Improved Ant Colony-based Optimization Algorithm for mitigating DDoS attacks in VANETs,** *Future Generation Computer Systems*, 82, pp. 304-314, 2018 https://doi.org/10.1016/j.future.2017.11.043
3. Mishra Binood Kumar, Nikam Mohan C and Lakkadwala Prashant, **Security Against Black Hole attack in wireless Sensor Network –A Review**, *Fourth International Conference on Communication System and Network Technologies, IEEE Computer Society Washington, DC, USA*, pp. 615-620, IEEE, 2014. https://doi.org/10.1109/CSNT.2014.129
4. Samir Athmani, Djallel Eddine Boubiche, and Azeddine Bilami, **Hierarchical Energy Efficient Intrusion Detection System for Black Hole Attacks in WSNs**, *Computer and Information Technology (WCCIT), 2013 World Congress on Sousse*, pp.1- 5, IEEE, 2013. https://doi.org/10.1109/WCCIT.2013.6618693
5. A. Manjeshwar, and D. P. Agrawal, **TEEN: A routing protocol for enhanced efficiency in wireless sensor networks**, *2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing (WPIM 2002)*, p. 195b, 2002.
6. C. Karlof and D. Wagner, **Secure routing in wireless sensor networks: Attacks and countermeasures**, *In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, May 2003.
7. S. Anbuchelian, Selvamani K and Chandrasekar. **An Energy-Efficient Multipath Routing Scheme by Preventing Threats in Wireless Sensor Network Electrical and Computer Engineering (CCECE)**, *IEEE 27th Canadian Conference*, 2014. https://doi.org/10.1109/CCECE.2014.6901163
8. H. Liu, Y. Chen, H. Tian, T. Wang, and Y. Cai, **A novel secure message delivery and authentication method for vehicular ad hoc networks**, *First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, pp. 135–139, Wuhan, China, 2016. https://doi.org/10.1109/CCI.2016.7778893
9. Xu and Liusheng Huang Quan Sun **Bandwidth Power Aware Cooperative Multipath Routing for Wireless Sensor Network**, *IEEE Transaction on wireless Communication*, Vol. 11, No.4, April 2012. https://doi.org/10.1109/TWC.2012.020812.111265
10. Baviskar B.R and Patil V.N, **Black hole attacks mitigation and prevention in wireless sensor network**, *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, Volume 1, Issue 4, pp.167- 169, May 2014.
11. Satyajayant Misr,Kabi Bhattarai, **Hole attack mitigation with Multiple base station in Wireless sensor network** , 2011
12. C. Karlof and D. Wagner, **Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures**, *Proc. First IEEE Int'l. Wksp. Sensor Network Protocols and Applications*, pp. 113–27, May 2003.
13. Adrian Perrig, John Stankovic, and David Wagner, **Security in wireless sensor networks**, *Commun.ACM*, 47(6) pp. 53-57, 2004. https://doi.org/10.1145/990680.990707
14. Khaled M. Elleithy, Drazen Blagovic, Wang Cheng, and Paul Sideleau, **Denial of Service Attack Techniques: Analysis, Implementation and Comparison**, 2006
15. Yang, Qiong, Lin Wang, Weiwei Xia and Yi Wu, and Lianfeng Shen, **Development of on-board unit in vehicular ad-hoc network for highways**, *International Conference on Connected Vehicles and Exp*, pp. 457-462, 2014. https://doi.org/10.1109/ICCVE.2014.7297589
16. M. Domenico, A. Calandriello, G. Calandriello and A. Lioy. **Dependability in Wireless Networks: Can We Rely on WiFi?**. *IEEE Security and Privacy*, 5(1):23-29, 2007 https://doi.org/10.1109/MSP.2007.4
17. Laxmi, V., Mehta, D., Gaur, M.S. and Faruki, P., **Impact analysis of JellyFish attack on TCP-based mobile ad-hoc networks**. *In Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 189-195). ACM, 2013
18. Sakshi Sachdeva and Parneet Kaur, **Routing Attacks and their Countermeasures in MANETs: A Review**, *International Journal of Advanced Research in Computer Science*, August 2016.
19. TEODOR-GRIGORE LUPU, **Main Types of Attacks in Wireless Sensor Networks**, *Recent Advances in Signals and Systems.*
20. S.K. Singh, M.P. Singh and D.K. Singh **A survey on Network Security and Network Defence Mechanism for Wireless Sensor Networks**, *International Journal of Computer Trends and Technology*- May to June Issue 2011.

21. S. Hong, L. Xu, H. Wang, and G. Gu, **Poisoning network visibilityin software-defined networks: New attacks and countermeasures.,** *in NDSS*, 2015. https://doi.org/10.14722/ndss.2015.23283
22. Dylan Smyth, Sean McSweeney, Donna O'Shea and Victor Cionca, **Detecting Link Fabrication Attacksin Software-Defined Networks**, *ICCCN*, July 2017. https://doi.org/10.1109/ICCCN.2017.8038435
23. Singh, I., **Detecting Sinkhole Attack In Manet Using Olsr Routing Protocol With Artificial Intelligence,** *International Journal of Advanced Research in Computer Science*, 9(3), 2018. https://doi.org/10.26483/ijarcs.v9i3.6020
24. Bansal, S. K., Bisen, A. S., and Gupta, R., **A secure hashing technique for k-means based cluster approach in VANET,** *In Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016 International Conference on pp. 2037-2041. IEEE, October 2016. https://doi.org/10.1109/SCOPES.2016.7955806
25. Lin, X., Sun, X., Ho, P. H. and Shen, X. **GSIS: A secure and privacy-preserving protocol for vehicular communications.** *IEEE Transactions on vehicular technology*, 56(6), pp. 3442-3456, 2007. https://doi.org/10.1109/TVT.2007.906878
26. Bi X and Wang Y, **An improved artificial bee colony algorithm.** *In: 2011 3rd international conference on computer research and development (ICCRD)*, vol 2, pp 174–177, 2011
27. Akay B and Karaboga D., **A modified artificial bee colony algorithm for real parameter optimization**., *Inf Sci 2012*, 192(1):120–42, 2012. https://doi.org/10.1016/j.ins.2010.07.015
28. Xiang WL and An MQ., **An efficient and robust artificial bee colony algorithm for numerical optimization**, *Computer Res 2013*, 40(5) pp. 1256–65, 2013. https://doi.org/10.1016/j.cor.2012.12.006
29. A.D. Wood and J.A. Stankovic, **Denial of Service in Sensor Networks Computer**, vol. 35, no. 10, 2002, pp. 54-62, 2002. https://doi.org/10.1109/MC.2002.1039518
30. Pranjul Sarathe and Neeraj Shrivastava, **A Review on Different Methods to Prevent Black Hole Attack in MANET**, *International Journal of Computer Sciences and Engineering* Vol.-6, Issue-6, June 2018. https://doi.org/10.26438/ijcse/v6i6.11491156
31. M. Zorzi and R. R. Rao, **Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance,** *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 337-348, 2003. https://doi.org/10.1109/TMC.2003.1255648
32. Sampada A. Khorgade and Namrata D. Ghuse, **Attacks and Preventions in Wireless Sensor Network**, *International Journal of Engineering Research and General Science Volume 3*, Issue 2, Part 2, March-April 2015.
33. Saravanan S., Hailu M., Gouse G.M., Lavanya M., Vijaysai R., **Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip.** *In: Zimale F., Enku Nigussie T., Fanta S. (eds) Advances of Science and Technology. ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol 274. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-15357-1_34
34. Amin Salih Mohammed, D Yuvaraj, M Sivaram and V Porkodi, **Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol**, *International Journal of Advanced Research in Computer Science*, Vol. 10, Issue 6, 2018. https://doi.org/10.26483/ijarcs.v9i6.6335
35. Mathiyalagan R, Saravana Balaji B and Josephine P, **An Efficient Routing and Distributed Denial of Service (DDOS) Attack Detection Technique for Centralized Control Plane**, *International Journal of Engineering Research and Technology*, Vol. 12, issue 1, pp. 124-130, 2019.
36. V.Porkodi and V.Manikandan, **Cooperative data dissemination via roadside WLANS using caching and transmission**, *International Journal of Innovative Research in Engineering Science and Technology*, Vol. 1, Issue 2, 52-57, 2013.
37. B. Buvaneswari , T. Kalpalatha Reddy, **ELSA- A Novel Technique to Predict Parkinson's Disease in Bio-Facial Recognition System**, International Journal of Advanced Trends in Computer Science nad Engineering, Volume 8, no 1, 2019, pp. 12-17.