INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 3, Issue - 10, Oct – 2019
Monthly, Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 4.526
Received on : 12/10/2019 Accepted on : 29/10/2019 Publication Date: 31/10/2019

An Analysis on Various Attacks in MANET and Machine Learning Classification Algorithms

[1] K. Gayathri, [2] Dr.R. Vidyabanu,
[1] Ph.D Scholar (Assistant Professor), [2] Assistant Professor
Department of Computer Science,
[1] Shri Kumaran College of Arts and Science, Karamadai,
[2] L.R.G. Government Arts College for Women, Tirupur.

Abstract: *Wireless networks are picking up fame to its pinnacle today, as the clients need wireless availability independent of their geographic point. There is an expanding risk of assaults on Mobile Ad-hoc Networks (MANET). It is a self-sufficient accumulation of mobile devices. They have the features of infrastructure less network, flexibility, Random mobility and they do not require any base station (or) centralized device for the communication process. In this system, each device acts as a client and server. Communication between nodes is done by intermediate nodes. Sometimes the intermediate nodes act as a malicious node by implementing any abnormal function. So, the vulnerabilities of Mobile Ad Hoc Networks (MANETs) are subject of numerous kinds of attacks. The main reason for security issues in MANET is that there is no physical link between the nodes and the nodes are mobile in nature. Consequently, there is no fixed topology. This paper investigated various approaches to analyze the attacks in MANET.*

Key Words: *Attacks, Classification, MANET, Machine Learning.*

1. INTRODUCTION:

Wireless ad-hoc network is a decentralized wireless network which comprises of a large number of sensor nodes. The system is specially appointed in light of the fact that it doesn't depend on a prior foundation, for example, switches in wired systems or passages in oversaw (framework) remote systems. Rather, every node takes an interest in steering by sending information for different nodes, thus the assurance of which nodes forward information is made progressively dependent on the system network [1]. Every node has certain computational capacity and contains a processor, communicational module and battery supply. These nodes are little, minimal effort, low power and has functionalities, for example, impart over short separations, perform information preparing, sense ecological information, and so on. In this paper, a survey of various kinds of attacks against MANET is studied.

2. MANET:

Mobile Ad-hoc Networks (MANET) are the networks of mobile computing devices joined wirelessly without any support of fixed interactions. In MANET nodes dynamically organize themselves in temporary network topologies by automatically connecting and disconnecting from other nodes in a network at any moment [2]. The MANET differs from other wireless networks due to its multi hop routing. In multi hop routing, a node uses intermediate nodes to communicate with other nodes that are not in communication range. Thus communication is based on mutual trust. In a MANET, each node is behaving either as a host or as a router [3]. There are some characteristics of MANET [4], which are as follows:

- ***Autonomous and infrastructure-less***

  MANET does not rely on any pre-existing infrastructure or centralized administration. Every node works in conveyed distributed mode, goes about as a free switch and creates data itself. Appropriation of system the executives ought to be over various nodes, which prompts trouble and flaw discovery.

- ***Distributed operation***

  The focal control of the system tasks has no foundation organize, the nodes have disseminated control of system.

- ***Multi hop routing***

  One or more intermediate nodes are used for forwarding the packets when the destination node is not within the communication range of sender node.

- ***Dynamic topology***

  Nodes are allowed to move quickly with various paces; therefore, the system topology may change in any capacity whenever. The nodes in the MANET powerfully set up steering among themselves as they move around, setting up their own system.

- ***Light-weight terminals***

  The nodes at MANET are portable with low power stockpiling, less CPU capacity, and little memory size.

- ***Shared Physical Medium***

  The remote communication medium can be gotten to any substance with satisfactory assets and fitting gear. No confinements can be applied to the channel.

- ***Energy constrained operation***

  Every operation performed by the mobile devices consumes energy so it limits the processing power of mobile devices.

The advancement in wireless communications are lightweight, small-size, portable computing devices and mobile computing possible. A MANET is one consisting of a set of mobile hosts which may communicate with one another. Portable hosts may speak with one another by implication through a grouping of remote connections without passing base stations. This requires each mobile host serve as a router [5]. A scenario of MANET is illustrated in Fig 1.

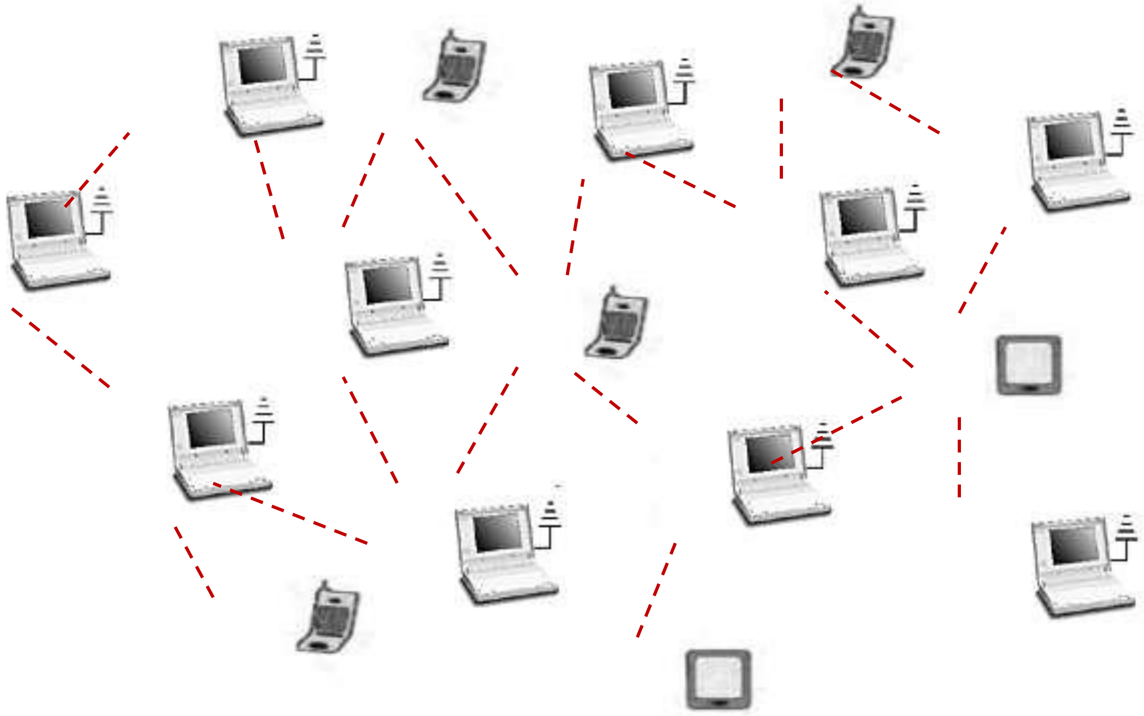

Fig1. Architecture of MANET

MANET Attacks: Attacks in MANET can be classified as Active and Passive attacks. An Active attack is one in which an attacker which is a certified node wipe out or alter the data that is being exchanged in the network. While a Passive assault aggressor hub which is an unapproved hub gets the information without upsetting or harming the system activity. Another grouping can be External and Internal assaults. In External attacks the attacker node is one which do not belong to that network while in Internal attacks the Attacker node belongs to that network. Internal attacks are more severe than External attacks since attacker knows all secret information and have privileged access rights [6].

Many security issues such as snooping attacks, wormhole attacks, black hole attacks, routing table overflow, poisoning attacks, packet replication, and denial of service (DoS) attacks, distributed DoS (DDoS) attacks have been studied in the recent years. The misconduct steering issue is one of the advanced security dangers, for example, Blackhole assaults. Some researchers propose their secure routing ideas to resolve this issue, but the security problem is still an issue.

Received on : 12/10/2019 Accepted on : 29/10/2019 Publication Date: 31/10/2019

Layered basis attacks: Attacks can also be classified on layered basis. Each layer undergoes different kind of attacks [7]. Fig 2 shows common type of attacks on various layers. Restricting on network layer in various network layer attack types is considered.

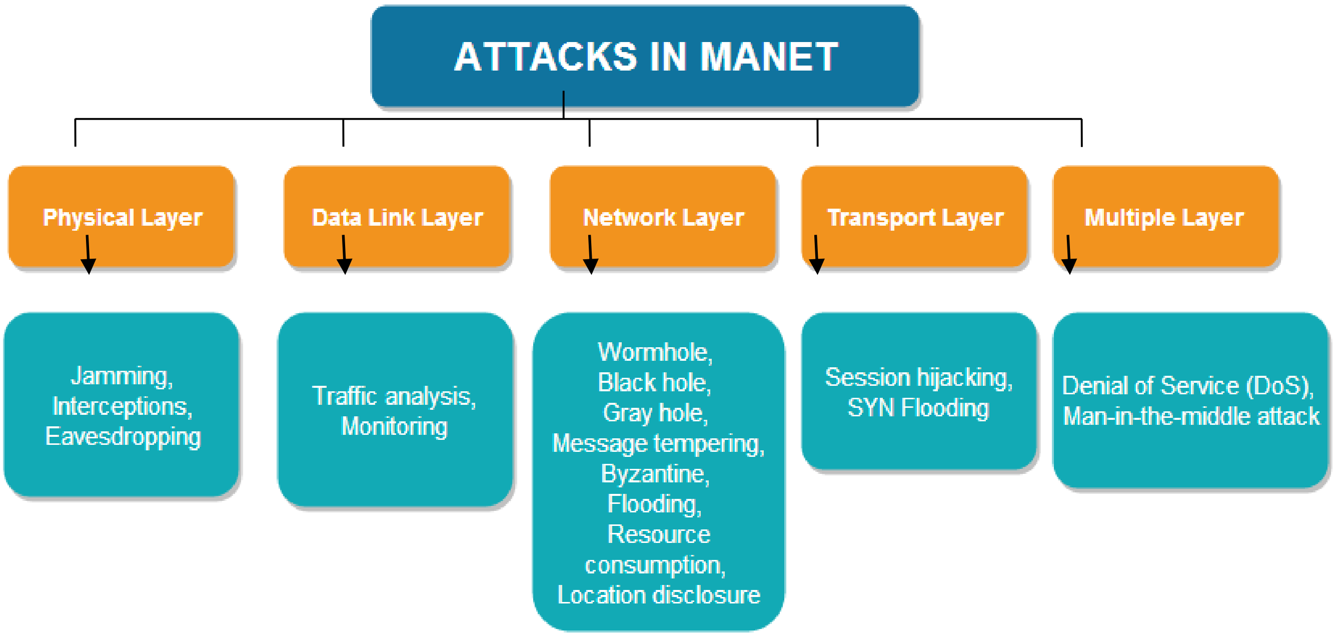
ATTACKS IN MANET
Physical Layer
Data Link Layer
Network Layer
Transport Layer
Multiple Layer
Jamming, Interceptions, Eavesdropping
Traffic analysis, Monitoring
Wormhole, Black hole, Gray hole, Message tempering, Byzantine, Flooding, Resource consumption, Location disclosure
Session hijacking, SYN Flooding
Denial of Service (DoS), Man-in-the-middle attack

Fig2. Type of attacks on layers

3. Classification of Attacks:

As previously discussed, attacks are classified based on the layers of network. But, attacks are commonly categorized into two broad categories:

i. DATA traffic attacks
ii. CONTROL traffic attacks.

This order depends on their basic qualities and assault objectives. For instance, the Black-Hole assault drops parcels inevitably, while the Gray-Hole assault additionally drops bundles yet its activity depends on two conditions: time or sender hub. However, from a system perspective, the two assaults drop bundles and Gray-Hole assault can be considered as a Black-Hole assault when it starts dropping packets. So they can be categorized under a single category. There are few attacks that have implications on both DATA & CONTROL traffic, so they cannot be classified into these categories easily [8].

i. DATA Traffic Attack

This attack bargains either in node dropping information bundles going through them or in deferring of sending of the information parcels. A few kinds of assaults pick unfortunate casualty parcels for dropping while some of them drop every one of them regardless of sender hubs. This may exceptionally corrupt the nature of administration and expands start to finish delay. This additionally causes a huge loss of significant information [8].

- ***Black-Hole Attack:*** In this kind of attack a hateful node participate in route discovery mechanism by sending RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination [9]. The source at that point begins to convey its information parcels to the dark opening believing that these bundles will arrive at the goal. As soon as the data transmission starts, hateful node drops the data packets that are needed to be forwarded to destinations. Black hole attack is increasingly damaging when contrasted with the dark opening assault.

- ***Gray Hole Attack:*** In this kind of attack a hateful node does not participate in route discovery mechanism that is initiated by other nodes and is therefore not a part of active route. Such hateful nodes would increase the route discovery failure and harm the overall network performance [10]. Another intention of such attackers is to conserve their energy by interpreting the message intended for them only and otherwise they do not cooperate with other nodes, which ultimately degrade the performance of the network.

- ***Jellyfish Attack:*** It is to some degree not quite the same as the Black-Hole and Gray-Hole attacks. Rather than indiscriminately dropping the information parcels, it postpones them before at long last conveying them. It might even scramble the request for parcels where they are gotten and sends it in arbitrary request. This upsets the typical stream control instrument utilized by hubs for dependable transmission. Jellyfish attack can result in significant end to end delay and thereby degrading QoS [11]. It can be classified into,
    - **a.** Jellyfish Reorder Attack
    - **b.** Jellyfish periodic Attack
    - **c.** Jellyfish variance Attack

ii. CONTROL traffic attack

MANET is naturally susceptible to attack due to its primary personalities such as open medium, distributed nodes, autonomy of nodes participation in network (nodes can connect as well as leave the network on its will), lack of centralized authority which can enforce security on the network, distributed co-ordination and cooperation. Two of the most widely used routing protocols is Ad-Hoc On Demand Distance Vector routing protocol (AODV), which relies on individual node's cooperation in establishing a valid routing table and Dynamic MANET On-Demand (DYMO) , which is a fast light weight routing protocol devised for multi hop networks. As there is no constraint in joining the network, malicious node can join and disrupts the network by hijacking the routing tables or bypassing valid routes. It can also eavesdrop on the network if the node can establish itself as the shortest route to any destination by exploiting the unsecure routing protocols [8]. It can be classified as follows,

- ***Wormhole Attack:*** In this wormhole attack a hateful node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network [8].

- ***HELLO Flood:*** The attacker node floods the network with a high quality route with a powerful transmitter. So, every node can forward their packets towards this node hoping it to be a better route to destination. The attacker node need not generate a legitimate traffic; it can just perform a selective replay attack as its power overwhelms other transceivers [12].

- ***Bogus Registration Attack:*** It is a functioning assault wherein an assailant masks itself as another hub either by sending taken guide or creating such false reference points to enlist himself with a hub as a neighbor. When enlisted, it can snoop transmitted parcels or may upset the system out and out. However, this kind of assault is hard to accomplish as the aggressor needs to personally know the disguising hubs character and system topology. Encoding parcels before sending and secure verification in course disclosure (SRDP, SND, SNRP, ARAN, and so forth) will confine the seriousness of assault somewhat as aggressor hub has no past information of encryption strategy.

- ***Man in Middle Attack:*** In this attack, the assailant hub creeps into a substantial course and attempts to sniff parcels moving through it. To play out a man in the center assault, the aggressor first should be a piece of that course. It can do that by either briefly upsetting the course by deregistering a hub by sending vindictive disassociation reference point caught beforehand or enlisting itself in the following course break occasion. One method for shielding bundles coursing through MANET from prying eyes is scrambling every parcel. Despite the fact that key dissemination turns into a security issue [13].

- ***Rushing Attack:*** In this when attacker node receive any request packet for route discovery then it sends the packet in the whole network before any other node forward the request packet. Due to this if same request packet send by authorized node to already received nodes then they consider packet as duplicate and discard it. In this way attacker will always be part of the route and it is extremely difficult to identify such hateful node.

- ***Packet Replication Attack:*** In this attack the hateful node replicate the stale packet and forward to the other node on order to use the battery power and consume bandwidth and create confusion in the routing process [8].

- ***Routing Table Overflow:*** In this attacker node create routes for non relevant node with an intension that no new routes are created. This causes an overflow of routing tables.

- ***Sybil Attack:*** It shows itself by faking different personalities by claiming to comprise of various hubs in the system. So one single hub can accept the job of numerous hubs and can screen or hamper various hubs one after another. If Sybil attack is performed over a blackmailing attack, then level of disruption can be quite high. Success in Sybil attack depends on how the identities are generated in the system [14].

4. Classification of MANET attacks by using Machine Learning (ML) Techniques:

This section gives an extensive classification of few ML techniques [15]. Each of the techniques is described below. Fig3 shows the classification of Machine learning.

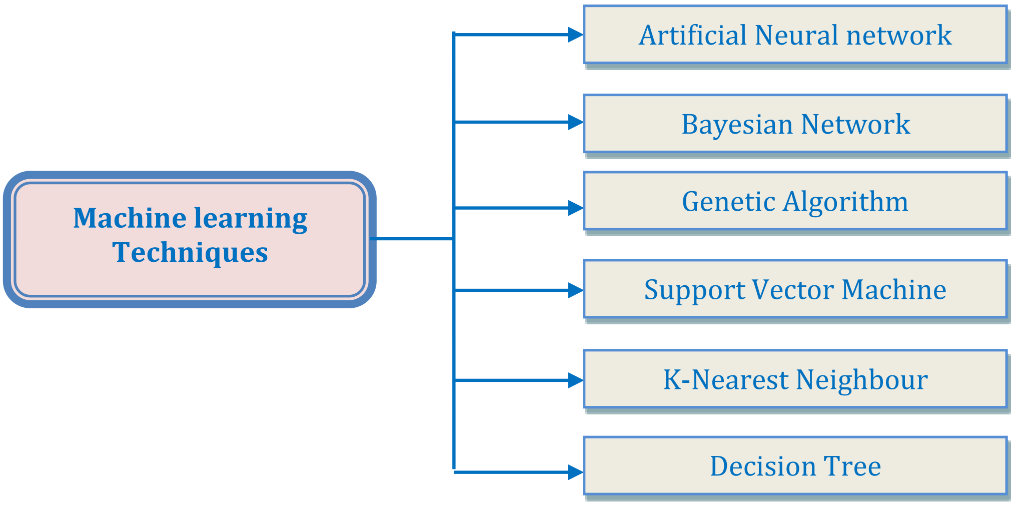

Fig3. Machine Learning Techniques

i. *Artificial Neural Network (ANN)*

ANN is a computational model inspired by biological nervous systems (e.g., human brain), which is presented as a system of interconnected “neurons” that can compute values from inputs. Roughly speaking, an ANN is a set of connected input/output units in which each connection has an associated weight. During the training phase, the network adjusts the weights to correctly predict the class label of the input tuples. Back-propagation is the most popular neural network learning algorithm. The following equation illustrates the output computation of a two-layered ANN.

$$O(x) = f\left[\sum_i \theta_i f\left(\sum_j w_{ij}x_j + b_i + b_0\right)\right]$$

Note f is the activation function, x is the input vector, w_{ij} is the weight of a hidden neuron, θ_i is a weight in the output neuron, and b_i and b_0 are biases. Many researchers have applied ANN for malware detection [16].

ii. Bayesian network (BN)

Bayesian network (BN), also called belief network, is a graphical model representing a set of variables and their causal influences. It is a graphical structure which enables the explicit representation of dependencies among variables. Different from NB, the variables in BN are not assumed to be conditionally independent. A standard Bayesian network consists of two components:

- A directed acyclic graph where random variables are represented as nodes and the edges represent probabilistic dependence between corresponding variables

- Conditional Probability Tables (CPT) for the variables. BN has also been used in malware detection [17].

iii. Genetic Algorithm (GA)

It is an adaptive search method in a class of evolutional computation using techniques inspired from convolution biological process. The principle is based on a stochastic global search method initializing with a random generation of chromosomes. The chromosomes are called population. They evolve through selection, crossover and mutation. Each chromosome represents a problem to be solved and encoded as strings. The locations of the chromosomes are usually characterized as binary (0, 1) or as a record of integers. These positions sometimes referred to as genes keep changing at each initialization. The clarification formed during every creation is based on an estimate task. The selection is thus based on the chromosome fitness level [18].

iv. Support Vector Machines

Support vector machines, or SVMs, have performed well on traditional text classification tasks, and performed well on ours. The method produces a linear classifier, so its concept description is a vector of weights, and an intercept. However, unlike other linear classifiers, such as Fisher's (1936), SVMs use a kernel function to map training data into a higher- dimensioned space so that the problem is linearly separable. It then uses quadratic programming to set the weights and the threshold such that the hyper plane's margin is optimal, meaning that the distance is maximal from the hyper plane to the closest examples of the positive and negative classes. Quadratic programming can be expensive for large problems, but sequential minimal optimization (SMO) is a fast, efficient algorithm for training SVMs. During performance, this implementation computes the probability of each class we used probability of the negative class as the rating.

v. K-Nearest Neighbour (K-NN)

K-Nearest Neighbour (K-NN) is a fundamental technique for sample classification. It evaluates the class labels of the test samples based on the majority of test sample neighbours. The parameter k is determined by the user. Based on the test sample, k numbers of training points are determined by taking the closest distance to the test sample. The prediction of the test sample is the k nearest neighbours.

vi. Decision Tree (DT)

This algorithm learns and models a data set in classification problems. It classifies new data set according to what it has learnt from previous data set [99]. It uses a well-defined criterion in the selection of best features of each node tree during their construction. A decision tree model has a root node linking to different nodes as attribute data deciding the path for each node. Decisions are made by comparison of previous data and marked as leaves [19]. A general decision tree technique is the C4.5 method.

5. Conclusion:

This paper talks about the classification of numerous attacks on MANET. These attacks direct to concession the safety. Security in MANET network is a great risk as it has no federal power that can manage the entity nodes working in the system. The attacks can arrive from equally within the network plus from the exterior. As Ad Hoc networks are vulnerable to many types of attacks, the classification of such attacks is a challenging issue. It is possible to make accurate classification of MANET attacks through applying machine learning techniques. This paper has specified several attacks according to different layers in mobile ad hoc networks and various existing machine learning classification techniques.

REFERENCES:

1. (N. Zanoon, N. Albdour, and H. S. Hamatta, "Security challenges as a factor affecting the security of manet: Attacks, and security solutions," International Journal of Network Security & Its Applications, vol. 7, no. 3, pp. 1–13, May 2015.
2. J. G. Ponsam and R. Srinivasan, "A survey on manet security challenges, attacks and its countermeasures," International Journal of Emerging Trends & Technology in Computer Science (IJETICS), vol. 3, no. 1, pp. 274–279, February 2014.
3. R. K. Singh, R. Joshi, and M. Singhal, "Analysis of security threats and vulnerabilities in mobile ad hoc network (manet)," International Journal of Computer Applications, vol. 68, no. 4, pp. 25–29, 2013.
4. Sagarika Kar Chowdhury, Mainak Sen "Attacks and mitigation techniques on mobile ad hoc network- A survey" International Conference on Trends in Electronics and Informatics, ICEI 2017.
5. P. V. T. Rajakumar P and P. A, "Security attacks and detection schemes in manet," in Electronics and Communication Systems (ICECS). IEEE, 2014, pp. 1–6.
6. Monika Goyal, Dr. Sandeep Kumar Poonia, Dr. Deepak Goyal3 "Attacks Finding and Prevention Techniques in MANET: A Survey" Advances in Wireless and Mobile Communications, ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 1185-1195.
7. Aniruddha Bhattacharyya, Arnab Banerjee, Dipayan Bose "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques" https://www.researchgate.net/publication/51956520.
8. Gagandeep, Aashima, Pawan Kumar "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
9. Jaydip Sen, "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" Innovation Lab, Tata Consultancy Sevices Ltd.

10. G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, “Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence”, (152-156) Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 978-1-4673-5845-3/13/2013 IEEE.
11. Rekha Kaushik and jyoti Singhai, "MODSPIRITE: A credit Based Solution to Enforce Node Cooperation in an Ad-hoc Network",IJCSI, International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.
12. Rupinder Singh, Dr. Jatinder Singh and Dr. Ravinder Singh, "HELLO FLOOD ATTACK COUNTERMEASURES IN WIRELESS SENSOR NETWORKS", International Journal of Computer science and Mobile Applications, Vol.4 Issue. 5, May- 2016, pg. 1-9.
13. Marti S, Giuli TJ, Lai K, Baker M, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks” 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August 2000. International Journal of Comp.
14. R. K. Singh, R. Joshi, and M. Singhal, “Analysis of security threats and vulnerabilities in mobile ad hoc network (manet),” International Journal of Computer Applications, vol. 68, no. 4, pp. 25–29, 2013.
15. Z. Zhang, C. Manikopoulos "Investigation of neural network classification of computer network attacks” International Conference on Information Technology: Research and Education, 2003. IEEE, Proceedings. ITRE2003.
16. Elike Hodo, Xavier Bellekens, Andrew Hamilton, Christos Tachtatzis and Robert "Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey" https://arxiv.org/ftp/arxiv/papers/1701/1701.02145.pdf
17. T. Subbulakshmi, S. M. Shalinie, and A. Ramamoorthi, “Detection and Classification of DDoS Attacks using Machine Learning Algorithms”, European Journal of Scientific Research, ISSN 1450-216X, Volume 47, No. 3, pp. 334 – 346, 2010
18. N. Lu, S. Mabu, T. Wang, and K. Hirasawa, “An Efficient Class Association Rule-Pruning Method for Unified Intrusion Detection System using Genetic Algorithm”, in IEEJ Transactions on Electrical and Electronic Engineering, Vol. 8, Issue 2, pp. 164 – 172, January 2, 2013.
19. M. Barreno et al., “The security of machine learning”, Journal Machine Learning, Vol. 81, Issue 2, pp. 121-148, November 2010.