Fuzzy Systems and Data Mining VII
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA210200

Securing Mobile Adhoc Networks from Black-Hole Attacks

Fahmina Taranum[a,1] and Khaleel Ur Rahman Khan[b]
[a]*Muffakham Jah College of Engineering and Technology, Osmania University, India*
[b]*Ace Engineering College, Jawahar Lal Nehru Technological University, India*

Abstract. MANETs are in-secure and vulnerable to attacks, as it lacks a central trusted authority. Providing security to such a network becomes an essential task and formulate the origin of the proposed work. The proposed system attempts to secure MANETs using route validation and cryptographic techniques. One of the most crucial, and primary concerns in today's times is to be able to detect an attacker at its initial stages. With this focus point in mind, the approach used is to prevent such an attacks by detecting in initial stage and preventing from network degradation. The novelty of the proposal is the use of cryptographic techniques for improving the security, along a reverse-AODV for reducing path fail correction, and machine learning concepts for validation of results. Many of the existing malware detection techniques proposed by the researchers were executed either on machine independent platform, or on an available dataset with machine dependent approaches. This drawback has been addressed in the existing proposal, where in machine learning is used with self-generated data-set, to eliminate contingent problems. The proposed system includes a network that is free from malware. Justification of the results were generated using classifier tools that were trained with the obtained dataset. For secured communication, an Elliptical curve cryptographic algorithm is applied to reverse ad-hoc on-demand distance vector with reverse multiple route replies that have been generated from the destination to the source node. An investigation to ensure the correct delivery of data can be done by diverting the traffic through the shortest alternative secured path. The metrics used for statistical analysis include average transmission-delay, overhead, packet forwarding rate and packet- delivery-rate, based on which the conclusion is theorized for the detection. The major finding includes the process of selecting an appropriate condition for detecting a malicious node, observing the network behavior with varying number of suspicious nodes and then validating the correctness. The implementation gives us varied results, both when the suspicious node is deferred for some time, and then on its complete elimination. The limitation of the proposal is that the suspicious nodes are uncoordinated.

Keywords. ECC, AODV, R-AODV, Enhanced AODV

1. Introduction

Networking is a vast domain, which deals with finite number of interconnected devices for communication through wired or wireless medium. The communication is managed by using data transmission through nodes in MANETs. A mobile adhoc network consists of mobile devices that move freely in multi-direction, while communicating among each other. MANET is a dynamically configurable system where the mobile

[1] Corresponding Author, Fahmina Taranum, Muffakham Jah College of Engineering and Technology, Osmania University, India; Email: ftaranum@mjcollege.ac.in

nodes are bridged to each other via wireless links. They do not have any definite infrastructure and is with no centralized administrative authority to monitor the network. MANET can serve as a standalone network or can also be a fragment of some larger network.

With the furtherance in mobile technology in future generation, people will have a facilely, widespread, and non-discrete access to information heading towards secure communication. In the modern society, with the advancement in technologies there is an increase in the issues to be addressed. Paucity of security is one of the major issues in MANET. Security includes the discerning of possible attacks, threats and sensitivity of the system against illicit access and alterations. The attacker may drop or access data packets with wrong intention. The attacks on the MANETs can identified based on norms like location, type, behavior, intention or on the layer onto which they befall, etc. The issues encountered like limited wireless transmission range, hidden terminal problems, and packet loss due to reasons like transmission errors, mobility-induced, route changes, and battery constraints. There has been huge amount of work done by the researchers in Manets using in-secure AODV routing Protocols. The designed strategy is novel as it highlights the new approach showing the various aspects of selecting the path using routing protocols, authentication of route and node, followed by validation process. Malicious attacks in the network need to be examined by exploring its type, aim, nature, cause and effects to handle security threats in an appropriate way. The attack could be just for an acquaintance or with fortitude to maltreatment a network. The type of attack implemented is black-hole, in which the traffic is attracted by the node using false dissemination and destination is kept deprived of the transmission. Black hole usually assimilates traffic of the network around it and tries to harm the network by reducing the performance metrics of the system.

The simulators used for implementation includes Ns2, Qualnet and Matlab. The proposal portrays the usage of DYMO routing protocol which provide a specific and much effective route with reduced power consumption. Dymo is a power aware routing algorithm works on the concept of selecting the shortest path to destination for transmitting data. The second novelty of the system is Reverse-AODV in which a reverse route exploration works to select the path from destination to the source node for storing multicast routes that can be used in case of link or path failure. The route obtained after applying R-AODV eliminates the scope of any malicious path selection since the routing table is updated simultaneously by comparison with the highest sequence number or the shortest hop count. The path thereby prevents Black-hole nodes to participate in reverse route discovery, thereby eliminating the chances of attacker in the path. The purpose of adding encryption is to secure the data transmission. The collaboration of the strategies used is Reverse AODV with ECC and validation of the datasets is done using Matlab tool as shown in figure 1. The approach used to do the route discovery of safe path is shown in figure 2.

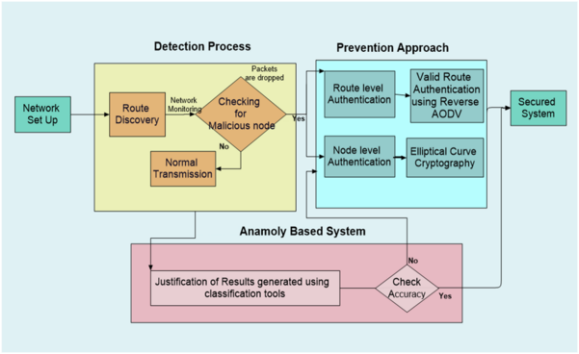

Figure 1. Architecture of the System

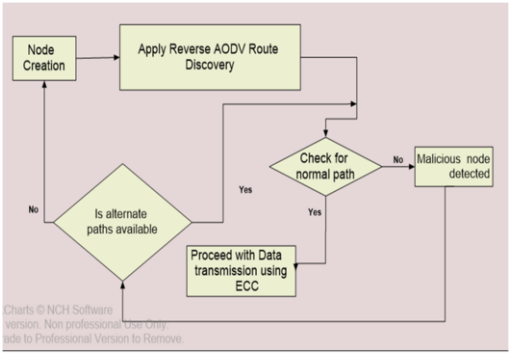

Figure 2. Malicious node detection using R-AODV

Black hole node consumes less time for packet processing and queuing delay. Packet processing here being the time for processing and extracting content from packet header, or time consumed during lookup between routing tables or to link to next node, and queuing delay refers to the time spent in queue at layers (Network and MAC) before it is forwarded to physical layer.

Q.D (Queuing delay) is the time a job waits in a queue until it can be executed, P.D (Processing delay) is the time router takes to process the packet header or time for one bit to travel, T.D (Transmission delay) is the time taken to put a packet onto link. It depends on length of packet and bandwidth of network, which can also be considered in designing.The average packet processing delay and queueing delay time threshold value is represented as ΔdTh.

Black hole attack is detected by checking the following conditions:

- If $\Delta d < \Delta dTh$, then the node is said to be authenticated, otherwise non-authenticated
- If the node is not authenticated, then the conditions (i) and (ii) mentioned below are checked for the possibility of black hole attack
- *If Th < R,* where R is the broadcasting radius of the node, H is the hop distance, *Th = distance (S, D) / H,* where distance (S, D) is the Euclidian distance
- *If DSN < (sn_{max} + μ),* where sn_{max} is the maximum SN value of all entries in routing table and μ is the number of data flows

If both the two conditions are true, then the node is said be honest, otherwise it is considered a black hole node.

2. Literature Survey

This section of the chapter presents a literature study to highlight the work explored and implemented by researchers. The idea is to fetch the limitation or area of further extension, and then to compare it with the existing approaches. The promising technological areas identified for the proposed system during the literature addresses intrusion detection, prevention and validation.

In [1] the Fuzzy logic is used to define rules for filtering an attacker. It is a way of representing information as it appears in human mind. In [2] the proposal is to de active the attacker in its worst effecting period and outcomes are justified using Anomaly based method. The Authors in [3] have worked on validating the accuracy of the results generated. Author in [4] has worked on multiple traffic generators and has evaluated performance in normal and malicious scenarios, the extension to the work would be to coordinate the attackers. In [5] Rmayti et al. accords a scenario of using a coordinated behavior through tunnel for worm hole attack, which is adapted here to check the performance degradation in coordination. Poongothai et al. in [6] aimed at designing an Anomaly based detection system for Routing attacks in MANETs to identify the normal or attacker nodes in the system using different values in the class, i.e. class with different values to represent behaving nodes. V.Saranya et al. in [7] aimed to eliminate a misbehaving node by using a reverse route tracing algorithm and the data is routed through an alternate path. ECC algorithm is used for authentication and integrity. Thanh Tu and Thai et al in [8] has worked on the threshold of the formula for distance and hop count to get the shortest path. Ningrinla et al. in [9] has used the concept of monitoring the behavior using neighbors to detect and eliminate a malicious node from transmission. This idea is applied in the proposal to take a node in a loop of deactivation upon detecting its anomalous nature. Nagendranath and Ramesh et al. in [10] has used a packet leash mechanism to detect the intruder, but the system was prone to fake replies too. This drawback is catered by using multicast approach for route reply in our proposal. Opinder et al. in [11], proposed that for each node with public and private key used for encrypting and decrypting transmitted data with ECC. Dhiraj et al. in [12] has proposed a detection and mitigation approach against Black-hole attacks using DYMO routing protocol.

3. Proposed System

The overview of the proposed approach is depicted in figure 1. Algorithm 1 is used for route level authentication and algorithm 2 for secure data transmission.

Algorithm 1 (EA-AODV)

Step 1: Route Discovery Process: Source sends RREQ towards Destination
Step 2: If intermediate node Nin receives RREQ, Forwards to Nin + 1, end if;
Step 3: If Destination is reached, then it responds with RREP end if;

Step 4: Source gets RREP from various paths Pm, m=1, 2, ... N
For each path Pm
For each intermediate Nin along Pm source computes the per hop time
S computes Euclidian distance between every two nodes
Calculate Th=Euclidian Distance/No. of Hops end for; end for;
Step 5: If Threshold< per hop time then Nin is authenticated else
If (Th < R) and DSN < (snmax + μ) then Nin is a non-poisonous
else Nin is a malicious
Remove Nin from the routing table of Pm end if; end if;
Step 6: Fetch an alternate path for valid shortest route from routing table or
invoke new route discovery process.
Step 7: Use the validation techniques to test the results

Algorithm 2 (Elliptical Curve Cryptography for Secured Data Transmission)

Step 1: Point Compression for Y, Y= Y%2 //selecting a point on curve
Step 2: Point Decompression for y using x and y
Z= (X3+ X +6) %p, Dy= Z3, Dy= dy % p, If (y- dy) % 2 ==0
then dy=dy else Dy=p-dy end if;
Step 3: Encryption using public key//Selecting co-ord for data enc/dec
kp = rand % endseq; //Identifying point kP's and kQ's seq. No.
kq = (rand*q) % end seq; (where q is the quotient =4) Calling the point compress on x and y coordinate of kp Cipher text is ((kpx), compress(kpy), quo, kqx %p)
Step 4: Decryption
i. Decrypted point is mx, my, pdy =ptdecomp(x,y);
ii. Intmedpt = (key*arr[x][pdy]) % 13;//calc seq no. of intermediate Pt
iii. qu=quo; for i, j in 0.10 if(arr[i][j] == medpt) then
mx=i; my=j; end if, end for;

The security to data transmission is applied by data encryption and decryption using logarithmic functions at the multiple points on the curve. ECC is difficult to broken down and even harder to assume. It is based and generated using mathematical logic and hence difficult to predict by an intruder. Finally, the result-set is imported to Matlab for justification of correct detection.

4. Results and Analysis

The results generated using the algorithms are statistically represented by parameters like Packet Delivery Ratio, Overhead, Throughput, Drop and Packet Forwarding Ratio.

$$\text{PDR\%} = \frac{\text{No.of collected packets}}{\text{No.of dispatched packets}} * 100 \quad (1)$$

$$\text{Overhead} = \text{No. of Routing packets} \div \text{No. of received datapackets} \quad (2)$$

$$\text{Drop} = (\text{No. of packets sent}) - (\text{No. of packets Received}) \quad (3)$$

$$\text{Packet forwarding rate} = (\text{No. of pack. received}) \div (\text{No. of pack. forwarded}) * 100 \quad (4)$$

$$\text{Throughput} = \text{No. of packets dispatched} \div \text{second} \quad (5)$$

$$Q.D = no.of\ packets * size\ of\ pqcket\ /(2 * BW) \quad (6)$$

4.1 Result Analysis with Algorithm 1

Attacks are targeted in the system to design it counteract and to provide security. The attack can be a member or an outsider, targeting the network to cause harm to it or retrieve information. The type of attack implemented, detected and avoided in the proposal is the Black hole attack. Additionally, security is added to the path through which the data is to be transmitted. In the Route Request process of route discovery, the source node initiates transmission by broadcasting a RREQ message searching for destination node, after which the destination node unicasts the route reply to the source node. This path is cached in the routing table for packet transmission from source to destination node. The route validity is checked using the destination sequence number and hop count generated in RREP. (In addition the detection of a malicious node assumes that the attacker pretends to take less propagation and queuing delay)

Authentication mechanism helps in checking the validity of the route using the following conditions,

- Actual neighbor: Two nodes Nj and Nk are actual neighbors, if d(Nj, Nk) < min(RNj, RNk);where R is the radius of coverage
- Nodes are said to be normal, if they are neighbors
- DSN ≤ max $(D.Seqno.,\mu)$,where μ represents in & out node traffic

In figure 3 throughput is analyzed for avoidance scenario with different simulation times. The inferences are EA-AODV out performs with 258 kbps, VRA-AODV with 84 kbps and AODV with 42 kbps maximum The Higher Packet forwarding ratio determines the drop and signifies that the packets are not furthered.

In figure 4 packet forwarding ratio is analyzed for detection scenario with varying simulation time. The values noted for EA-AODV is 74% maximum, VRA-AODV is 29% maximum and AODV a hike of 18%, where VRA references [8] in bibliography. The equations (1) to (6) are used in the result analysis

The figure 5 depicts a comparative analysis of all the four classifiers (Decision tree(DT), KNN (K nearest neighbor), SVM (Support vector machine) and NN (Neural networks)). From the graph it is clearly perceived that the SVM model holds high accuracy rates compared to the rest of the algorithms. The models are trained with datasets where nodes possess mobility speeds of 5, 10, 15, 20 and 25 seconds.

From the Figure 6, it is clearly interpreted that for any value of speed the SVM provides the highest accuracy rates comparatively. As this network is significantly populated with an increase number of malicious nodes, which are prone to attack network; it results in decrementing the accuracy rate of the network.

4.2 Results for Algorithm 2

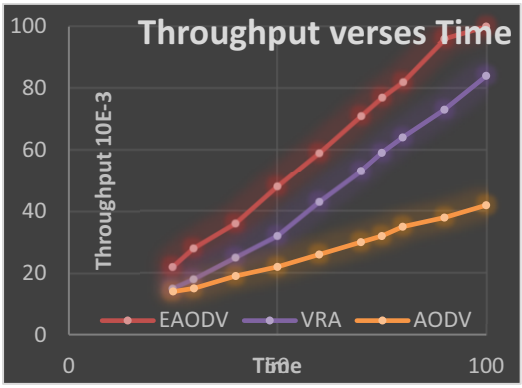

Figure 3. Comparison of Throughput

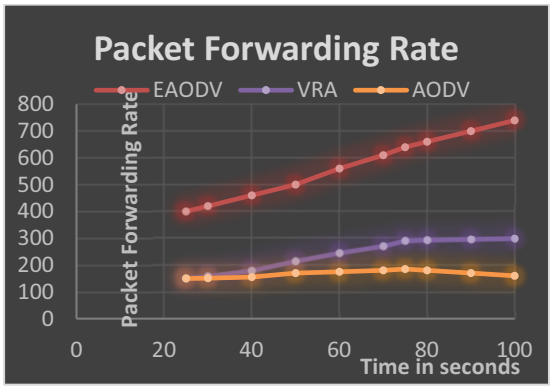

Figure 4. Packet Forwarding Rate

For both the prevention(p) and attack(a) scenario. It can be inferred from the graphs that the performance analysis is better, when a secured path is selected for data transmission. The analysis in figure 7 and figure 8 helps us to conclude that the loss rate is reduced and overhead is brought to zero after applying the prevention mechanism on selecting the sheltered path. Overhead is determined by the number of routing packets. In case of detection scenario with respect to change in simulation time in figure 8 the proposed method shows more overhead compared to the existing ones. The avoidance scenario is experimented over varying number of attackers and multiple simulation time. The reverse R-AODV end to end delay is as shown in figure 9. The delay is initially greater and later becomes linear. As the reverse path is cached at the source node in the R-AODVs, the rediscovery is not initiated unless all the reverse stored paths are used, hence the proposal is considered efficient. The throughput is compared between a Black-hole(green) and reverse AODV(red) with interpretation that after applying the reverse path algorithm, about a tremendous increase in the throughput is seen in figure 10.

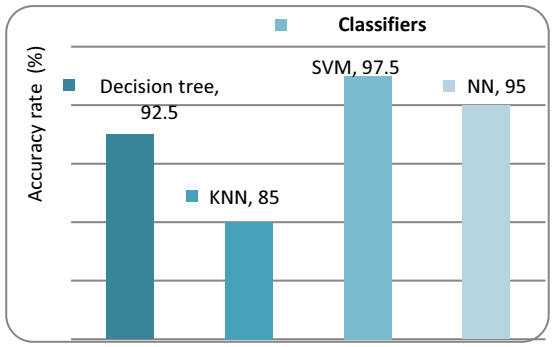

Figure 5. Accuracy verses Classifiers.

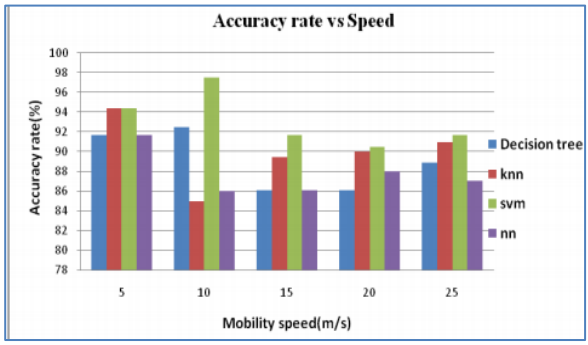

Figure 6. Accuracy verses Speed.

To design a better algorithm for prevention of malicious node, appropriate performance analysis parameters must be selected. Any malicious activity degrades the performance, but the parameters used are different for varying type of attacks. The attack type implemented in this proposal is Black hole in which the traffic sinks at the malicious node. The aim of this malicious node is to attract the traffic by making a false or fake dissemination in the network about having the short path. The node further affects the network transmission by retaining or by dropping the data, which results in the drop of packet forwarding rate. In [4] author has selected the height of antenna as ≥3 meter to capture the traffic along with increasing the storage of the buffer size of the node as parameters to inhibit malicious behavior. Figure 6 depicts the results obtained with different classifiers on varying speed of the mobile nodes to analyze the accuracy and it has been found that SVM performs the best in all the considered classifiers. The self-generated data from the network simulator is used to check the best classifier for prediction. The classes used in training are binary in nature with 0 for normal and 1 for malicious.

Advanced routing protocol like DYMO is a popular reactive routing protocol in wireless networks, developed with aim to enhance the performance of ad-hoc network by being more energy efficient. Unlike secure protocols, DYMO lacks the security related features like authentication, integrity, and confidentiality. DYMO has certain vulnerabilities which makes security a major concern here. Outside attackers interfere and interrupt the legitimate traffic due to an open nature of wireless medium. One of such widely known attacks is the Black hole attack. As security is a major concern in wireless

networks, it is provided in the proposal at the node level and at route level by using some encryption algorithms like ECC. Open Shortest Path First(OSPF) routing protocol can also be used to apply security in networks as it includes or inherits authentication facilities as MD5 and simple authentication mechanisms to prevent against the Black hole attack. but OSPF protocol does not support wireless networks

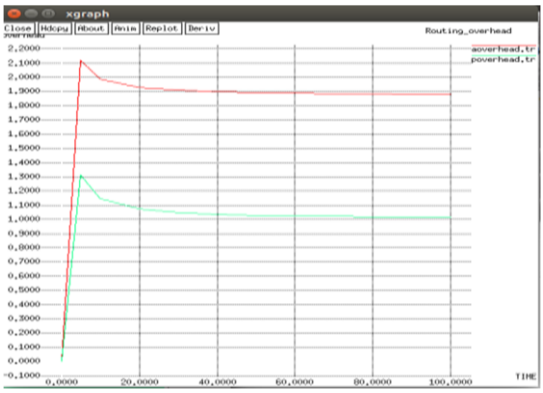

Figure 7. Loss-Ratio for Attack and Prevent.

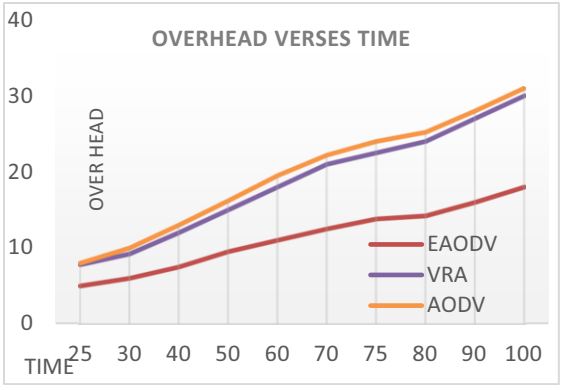

Figure 8. Overhead with Attack and prevention.

When ECC is used to make the transmission secure, it is observed that the throughput gives better values on comparison with AODV. The complete work is implemented in Adhoc wireless networks. The graphs depicted in figure 9 and 10 signifies that the results show a better analysis when the network is secured using prevention algorithm. The security can be applied at the node level or the route level. ECC helps to secure the data at the transmission level using the process of encryption and decryption based on mathematical logistics. The throughput is compared between a Black-hole (in green) and reverse AODV (in red) with conclusion that after applying the reverse path algorithm, about a tremendous increase in the throughput is noted.

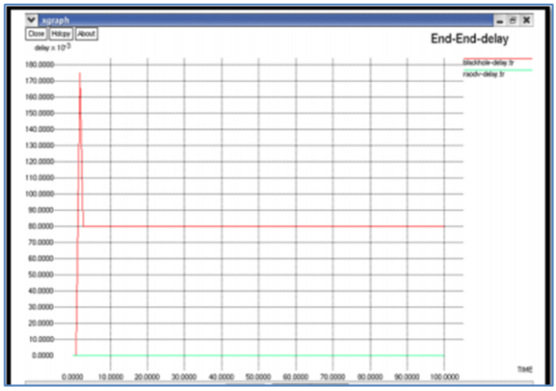

Figure 9. End to End Delay

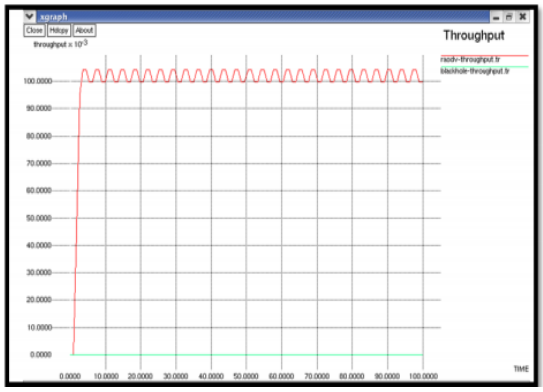

Figure 10. Throughput with ECC and R-AODV

5. Conclusion

The collaboration of two algorithms yields a secured system with good performance metrics. R-AODV helps in storing the routing information of each node thereby reducing the time taken to reinitiate the route discovery process using request retires and helps in transmitting the data at a faster rate when compared to AODV. Further the addition of ECC helps to increase the security of the data transmission, thereby making it difficult for the intruder to interpret the data. The results obtained from these algorithms are imported as data-sets to Matlab to check its efficiency and was found to give good accuracy with SVM classifier. The extension to this work could be to implement coordinated attacks.

References

[1]. Zainab, Fahmina Taranum and Khaleel Ur Rahman. Legitimate-path Formation for AODV under black hole attack in MANETs. Fourth International Conference on Electronics, Communication and Aerospace Technology; ISBN: 978-1-7281-6386-4. 2021 Dec.; p. 1489-1496.

[2]. Fahmina Taranum, Ayesha Sarvath and Noora Ali. Detection and Prevention of Blackhole node. International Conference on Electronics, Materials Engineering and Nano-Technology; IEEE Xplore. 2020 Oct.; ISBN:978-1-7281-9287-1.
[3]. Hajira, Fahmina Taranum and Khaleel Ur Rahman. Detection and Interception of Black Hole Attack with Justification using Anomaly based Intrusion Detection System in MANETs. International Journal of Recent Technology and Engineering; ISSN: 2277-3878. 2019 Sept.; 8(2s11). p. 2392-2398.
[4]. Fahmina Taranum and Khaleel Ur Rahman. Maneuvering Black hole attack using different traffic generators in MANETs. Intelligent Systems Technology and Applications; Springer Germany; 2019 Feb.
[5]. M. Rmayti, Y. Begriche, Rida Khatoun and Lyes Khoukhi. Graph-Based Wormhole Attack Detection in MANETs. 4th International Conference on Mobile and Secure Services; 2018. p. 1-6.
[6]. T. Poongothai and K. Jayarajan. Intrusion Detection System for Mobile Ad Hoc Networks using Cross Layer and Machine Learning Approach. International Journal of Computer Applications; 2018; 179(34). p. 5-13.
[7]. V. Saranya and S.Sharmila. Detection of Black-Hole Attack in MANETs using AODV & Path Tracing Algorithm. International Journal of Pure and Applied Mathematics; 2018; 119(12). p.1355-1371.
[8]. Thanh Tu and Thai Ngoc Luong. VRA-AODV- Routing Protocol Detects Black-hole& Gray Hole Attacks in Mobile Ad Hoc Network. Journal of Computers; 2018 Feb.; 13(2). p. 222-235.
[9]. Ningrinla Marchang, Raja Datta and Sajal K Das. A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology; 2017; 66(2). p. 1684-1696.
[10]. M. V. S. S Nagendranath, B. Ramesh and V. Aneesha. Detection of Packet Dropping and Replay Attacks in MANET. International Conference on Current Trends in Electronics & Commun'n; 2017. p. 933-938.
[11]. Opinder Singh, Singh J. and Singh R. Multi-Level Trust Based Intelligence Intrusion Detection System to Detect the Malicious Nodes using Elliptic Curve Cryptography in MANET. Springer; 2018. p. 51-63.
[12]. Dhiraj Nitnaware and Anitha Thakur. Black-hole Attack Detection & Prevention Strategy in DYMO for MANET. 3rd International Conference On Signal Processing & Integrated Networks, 2016; p. 279- 284.