Proposals on the Mitigation Approaches for Network Layer Attacks on MANET

Syeda Hajra Mahin, Lubna Naaz Fatima, Fahmina Taranum, Khaleel Ur Rahman Khan

Abstract— MANET is a class of network, which is customarily embracing numerous mobile nodes that do not hold any firm organization. The MANET hold peculiarities such as circumscribed battery power, bandwidth, range, security, etc, which has primarily become the reason for researchers to carry out the study. In MANETs, the transmission of the packets from the initiator to the destined nodes is regularly done via the midway nodes in the network, hence proving security to be a vital affair. There are certain categories of attacks that are prevalent in MANETs that regularly demote the system performance. In this work, the proposal is to perform comprehensive study on the numerous sorts of attacks that are prevailing in the MANETs together with their alleviation strategies put forth by numerous researchers. Post per-forming this study, there are some proposals to the studied existing alleviation strategies; which helps to provide and improve the performance and security issues.

Keywords: MANET; Peculiarities of MANET; Categories of attacks; Alleviation ideas; Security

1. INTRODUCTION

The default nodes in the MANETs routinely change their positions with respect to the presiding network while transferring the data from one end to the other. This network is outlined in such a manner that the component nodes are coupled together by some wireless association [1]. These systems do not hold the responsibility of investigating the comportment of the system. These networks can be run as individual one's or can be made a fragment of a broader one The identification of the type, intension of attack need to be explored before the preventive measures are applied.

This network possesses certain traits like the following [1]:

- Hop oriented communication
- Hassle free deployment
- Self configuring
- Dynamic topology
- Absence of base station
- Curbed security
- Recurrent link breakage

Meagerness in the network reliability has proven to become a chief subject in MANET. Soundness of the network depends upon its potential in identifying the sort of attack influencing the network and incorporation of an effective mitigation scheme against it. The concern of any attack primarily is observed to affect the confiden-tiality of the transmission and decline the overall network perfor-mance [2].

This work is to shed light upon the assorted kinds of at-tacks that exert influence on the wireless network, with an aim to perform an augmented study on the differing strategies put forth by different researchers to detect, mitigate and prevent these attacks in the network. Varying newly discovered algorithms and modifications to the existing algorithms are also scrutinized. Fur-thermore the performance of these proposals are also explored and investigated.

2. CLASSIFICATION OF ATTACKS

The figure 1 exhibits the norms upon which the attacks on MANETs could be graded.

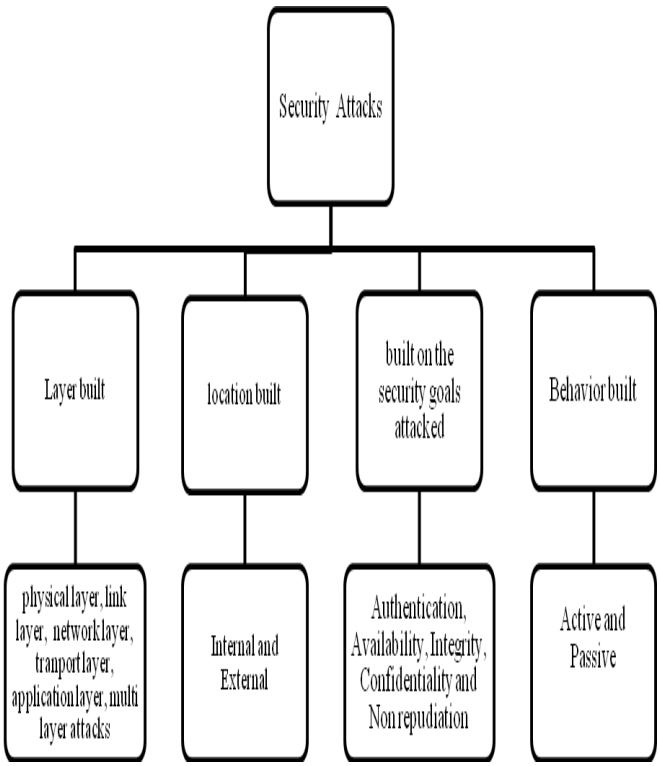

Fig. 1: Grading of attacks

Revised Version Manuscript Received on March 10, 2019.

Syeda Hajra Mahin, Computer Science and Engineering Department, M. J. C. E. T, Telangana, India (E-Mail: hajraziaulhussain@gmail.com)

Lubna Naaz Fatima, Computer Science and Engineering Department, M. J. C. E. T, Telangana, India

Fahmina Taranum, Computer Science and Engineering Department, M. J. C. E. T, Telangana, India

Khaleel Ur Rahman Khan, Computer Science and Engineering Department, Ace Engineering college, Telangana, India

2.1. Layer built classification of Attacks

The table 1 manifests the layer wise attacks in the network.

Table 1: layer based attacks

Layers	Example
Physical layer	Eavesdrop
Link layer	DOS
Network layer	Jellyfish
Transport layer	Flooding
Application layer	fallacious Code
Multilayer	Impersonation attack

2.2. Location built classification of Attacks

The table 2 conveys the information on the location based classification of MANET attacks.

Table 2: location based attacks

Internal attacks	An internal attack is aroused by the nodes that are pre existent of the put through network [3] [4]. The spiteful nodes in the network diffuse fallacious information in the network. These attacks are inconvenient to be discerned when juxtaposed against the external attacks.
External attacks	An external attack is aroused by the nodes that are not pre existent of the put through network [3]. The spiteful nodes in the network crucially aim to diminish the performance by muddling up the network services.

2.3. Grading grounded on security goals attacked

The table 3 manifests the details about the security goals taken into account and lists some of the examples under each security goal.

Table 3: Goals based classification

Goals	Example
Authentication: It is a mechanism of discerning individual nodes/ data packets in the network.	Session Hijacking
Availability: It is the ability to preserve the network resources for the genuine nodes in the network.	Entire of the routing based attacks compromise the availability.
Confidentiality: It is the mechanism to ensure that the data packets relayed through the network are guarded from illegitimate access by attackers.	Eavesdrop
Integrity: It refers to protecting the novelty of the data and protecting it from any alterations.	Sink Hole
Non repudiation: Ensuring that neither of the primary parties gainsays the transmission and reception of the packets.	Spoof oriented Attacks

2.4. Behavior based Attacks

The figure 2 portrays the furthermore classifications of the behavior oriented attacks.

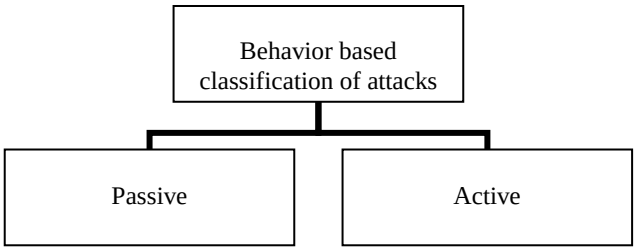

Fig. 2: Behavior based classification

Passive Attacks:

This class of attackers chiefly delves into the imparted data in the system without making any revision to it [3] [5]. The figure 3 manifests the examples of passive attacks.

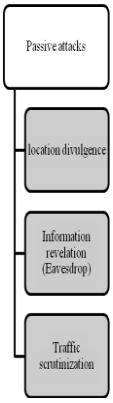

Fig. 3: Examples of passive attacks

Active Attacks:

This class of attackers yearns to transform or reorient the im-parted data in the system. The attacker is able to do this by admin-istering fallacious data into the imparting data [3] [5]. The figure 4 shows the examples of active attacks.

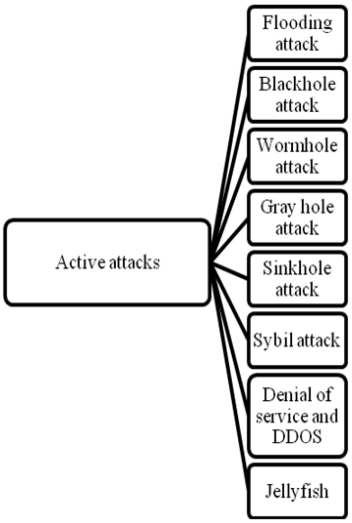

Fig. 4: Examples of active attacks

3. RELATED WORK & RESULTS

From [6], Sumaiya Vhora, et al. Suggested an approach for allevi-ating the affects of data drop attacks. An RBDR mechanism on AOMDV is brought forward. Throughout the discovery of route process the DSN is accounted and adjoined to the reply packets for all available data routing tracks in the network. After which some inflated (high) DSN merit is channeled in the network. If any route channels a much inflated value, then this replying route is concluded to have some spiteful nodes. After perceiving this, ranks are quantified for other obtainable routes grounded on hop together with sequence merits.

From [7], Sarika U Patil worked to for the alleviation of gray hole. The routing was implemented using AODV. Spirited nodal grouping is committed. A chief is designated for each nodal group rooted on the residual energy merits. The system assurance is done by employing md5.

From [8], Mohsin Mulla, et al. Worked on an approach to avert the influence of sybil based attack. This paper utilizes RSS to tell apart between spiteful and the permissible ones. The most common con-jecture tells that the speed of the component nodes of the system would not transcend ten mtrs/sec. Rooted on this, RSS is valued. The RSS merits are juxtaposed to distinguish the spiteful nodes among the permissible ones.

From [9], the researchers Priyanka Yadav, et al. Brought forward an advancement to the most recurrent routing protocol, AODV. Themain Objective is to provision the impact of numerous sorts of attacks specifically, man in middle together with Sybil based and wormhole based attacks. Hello messages along with the usage of dc (digital certificate) are taken up to embattle against felonious activities. While channeling the data adjoining of ciphered DC is done. Pro-vided that, if the deciphering of DC is not been able to be done then that node would be regarded as the spiteful one.

From [10], the researchers Bhavin Joshi, et al. were successful to evolve a diminution scheme to protect from the impacts of DDOS. In this work, an overseer is employed rooted on the node's liveliness. The curtailment on the request packets is detailed so that no legitimate node would transcend the set limit.

From [11], Roshani Verma, et al. Brought forward an approach to alleviate the impact of wormhole sort of attack. The notion of track origination is based upon the protocol AODV. The reckoning of PDR and RTT is carried out post the channeling of the data packets. The deciding factor for the presence of this attack is solely based on the following condition, that provided the RTT barely falls below the pre set value and the PDR has fallen below 1, it is ministered as a spiteful node.

From [12], the researchers Avni Tripathi, et al. Developed a pro-cedure to protect against an active attack i.e., black hole. In this scheme the destined node post obtaining the packets consigns a special packet to the initiator where it conjoins the endmost hop merit. Provided that the conjoined value is identical to the value stacked at the initiator end, the channeling of the data would pursue.

From [13], Sakshi Garg, et al. have come up with intensified AODV to safeguard against jellyfish attack. Component nodes propagate a special packet via which the relay time of the data packets are jot down. The nodes in the system hold the responsi-bility to scrutinize the discrepancies between the relay and the reception times rooted on which the resolutions are made.

From [14], the researchers Dhiraj Nitnaware, et al. Preferred a scheme to bridle the active attack black hole employing an effective routing protocol DYMO. This protocol functions by implementing hello messages. Here, the power of transmission along with the tallness of antenna is taken into deliberation for the component nodes which are furthermore juxtaposed against some pre decided values. Those of the considered nodes having surpassed this threshold are believed to be the spiteful ones.

From [15], Alka Chaudhary, et al. advocated an approach to di-minish the affects of data drop attack. This operates in the following manner: (1) Beginning with the drawing out of fuzzy traits like data progress proportion, drop rate, and accuracy extent. (2) Deciding on the fuzzy rule: the rule considered is that provided the data progress proportion is elevated keeping the average drop rate slighter, then the accuracy extent remains elevated. (3)Resolution module: an accuracy merit is pre decided and if any node has this merit value surpassing the pre determined one, then that node is treated as the spiteful one. (4)Concluding module: based on the above module the spiteful nodes are noted and this information is channeled in the network post which the spiteful nodes are detached from the system.

From [16], Han-Chao Lee, et al. have innovated a probing plan of action for uncovering dynamic intrusions. A probing track is coined from initiator to target and at some settled time stretch the probing packets are disseminated, and presuming that if an alongside node doesn't procure it on time then the probing track should be re-fabricated. If it does procure it on time then the Degree of

Misbehavior intrusion (DMI) is reckoned and if the value is on the farther side of zero then the re-coining of probing path is to be done.

$$q1 = \frac{leaked\ no.of\ probe\ pkts}{gross\ probe\ pkts}; \quad (1)$$

$$q2 = \frac{altered\ no.of\ probe\ pkts}{gross\ probe\ pkts} \quad (2)$$

$$q3 = \frac{dispatch\ delay\ of\ probe\ pkt}{anticipated\ delivery\ time} \quad (3)$$

$$DMI(Ns, Nd, Ti) = \sum_{k=0}^{3} Wkqk, 0 \leq Wk \leq 1 \quad (4)$$

Where Ns is initiator node; Nd is destined node and Ti is the time interval. This is redone for succeeding iteration. Following this course of action the attacks are recognized and ergo can be halted.

From [17], Gurveen Vaseer, et al. have come up with a novel intrusion detection system on AODV protocol against probing attack, Denial of service attack, Vampire attack and user-to-root attack. A behavior table is built which contains the behavior values. The data conveyed is run through the simulation engine to inspect if its normal, if it is normal then no attack has transpired. If there is some intrusion detected then the next step is to learn which of the above 4 attacks has arose. The resolution is made based on the prevailing conditions like, If data is being seized then it is probing; if messages are relayed with no UDP, TCP standards then it is DoS attack; if there is intemperate energy depletion and disabling of path then this is believed to be vampire attack; and if the IP address is revised then this is concluded to be U2R attack.

From [18], H.Ghayvat, et al. suggested a mitigation technique for wormhole attack where the notion of tunneling time is considered to detect the attack and the notion of digital signatures is taken for its deterrence. Tunneling time gives the most recently updated posi-tion and location of each one of the nodes. A static threshold value is preserved against which the tunneling time is contrasted and resolutions are made whether a particular node is a malicious node or not.

From [19], Albandari Alsumayt, et al. have proposed a detection mechanism against DoS attack by using MrDR methodology for merging two MANETs. The MrDR has 3 stages: where Mr stands for monitoring, D for detection and R for rehabilitation which mainly focuses on the estimation of the trust value of the nodes. The merging can be in 2 ways, centralized and decentralized. In the former approach each MANET has a node accountable for calculating the trust value of all the nodes within its network using MrDR method and to make sure that there are no dissensions with the nodes of the other merging network. In such a way the attacker nodes are secluded from the newly formed larger network. In the decentralized approach no central mastery is present. Each node in the MANET has to relay and exchange information about itself and its intermediary nodes to all the other nodes in the other MANET itself.

From [20], S.B. Mohan Kumar, et al. has come up with a policy based scheme for the prevention of flooding attack in MANETs. In this work a preventive routing protocol is being put forward, where every node scrutinizes each of their adjacent nodes by keeping up a count of the relayed RREQ packets by them. When the count value goes beyond the pre-specified threshold then it is considered as the attacker node. This node is then blocked and segregated from the network.

3.1. Survey Analysis

In [6], a detailed result analysis is missed out. Hence, the en-hancements can be made by running it on the NS-2 simulator.

In [7], the evaluation has been followed out with throughput along with routing overhead, PDR and also delay. The throughput in the existence of malicious node is not so much than contrasted in its unavailability, yet superior to the prevailing condition. The propa-gation overhead is to a lesser degree than in the case of EAACK with DH-EAACK arrangement. The PDR has surpassed and the delay is minimized.

In [8], NS2 simulator is utilized with the intention to carry out inspection, and the execution variables assessed are throughput together with PDR and delay. The PDR and throughput has com-paratively refined whereas the delay has been enhanced.

In [9], the evaluation is followed through on NS 2.34. The PDR along with end-to-end delay are thought as the execution metrics. By scrutinizing the outcome it is noted that the PDR increments with inconsiderable increment in the end-to-end delay.

In [10], NS 2.35 simulator is employed for the scrutinizing need. With the put forward policy applied, end-to-end time delay has noted to dwindle and the network routing load had some inconsid-erable increment.

In [11], the assessment is carried using the NS2. The evaluation variables such as PDR, throughput, delay as well as speed are pondered. The PDR and Throughput is perceived to elevate post the application of the recommended approach, dwindling the simulation time along with delay.

In [12], QualNet 6.1 simulator has been preferred for simulation and execution survey motive. The inspection metrics contemplated are PDR together with delay and throughput. It is discerned that the average PDR has intensified from the surviving system. The average Delay is also noticed to elevate in this scheme. And the throughput is noted to rise from 3419(bits/sec) to 3553.5(bits/sec) post applying the presented scheme.

In [13], NS 2.35 simulator is operated with the intention of carrying out the inspection. The throughput along with PDR is taken as the judging variables. The throughput and PDR gain are noticed to boost when the put forth strategy is used.

In [14], QualNet 5.2 is employed to imitate and appraise the sug-gested approach. It operated using throughput and Packet delivery ratio (PDR) as the criterion for fulfilling the analysis. It is perceived that with the elevation in quantity of nodes, the throughput along with PDR and speed also elevates.

In [15], with the motive of evaluating the put forward system, Qualnet 6.1 is considered. From the outcome it is demonstrated that with the suggested approach the recognition of packet drop has improved.

In [16], with the intention of carrying out the performance scruti-nization of the suggested approach the simulator NS-2 is chosen. PDR is solely taken as the evaluation variable. The PDR value is noticed to elevate when contrasted against the existing system.

In [17], with the motivation to analyze the put forth idea NS-2 simulator has been used. The evaluation metrics taken are Normal Routing Load (NRL), Delay, throughput, Accuracy together with Confusion matrix. The results show that the proposed work has certainly improvised the existing system.

In [18], to carry out the evaluation of the proposed work NS-2.35 simulator has been chosen. The graphs are plotted against existing and proposed systems taking PDR and Throughput as the judging parameters. This mechanism is noticed to improve the overall lifespan of nodes and also

elevates the throughput, thereby reduc-ing the overall delay.

In [19], the authors have missed out performing the result analysis using simulator.

In [20], the authors carried out the performance evaluation of their proposal on NS-2.34 simulator. The evaluation metrics considered are PDR, Delay together with throughput. The PDR and Throughput values have observed to elevate with respect to the existing system.

4. CONCLUSION

Through this work, a detailed presentation on the attacks, which are vulnerable at the network layer in MANETs and its analysis is highlighted with the identification to the norms upon which these attacks could be furthermore graded. In order to safeguard the channeled data in the network an effective attack or malicious activity detection mechanism is needed to be employed. The alle-viation mechanisms put forth by numerous researchers to bridle these attacks are studied and also investigated to check for their clampdowns. The concept of tunneling is used in wormhole and its peer. To improvise the performance of the system, it is mandatory to identify the cause of the attack and thereby its prevention. Post performing this rigorous study an attempt is made with certain future enhancement proposals to the existing work which aims to overcome the clampdowns stated.

Limitations observed:

In [8], an approach to overcome Sybil attack was put forward. This paper had a clampdown that this work ended up with excessive delay.

In [14], the impediment observed is that data loss is contemplated as the sole norm in the detection of the attack.

In [15], a scheme for managing the data drop attack was formulated where the clampdown is the module of resolving the values of the judging variable or metrics. Any faults in this step could invite adverse effects on the performance.

In [19], the shortcoming noted in their proposed work is that the authors have lacked to provide a detailed analysis of their proposal and no performance metrics were discussed for evaluation.

Future work:

In [7], the upcoming improvement that can be appended is adding a safety algorithm for instance AES and MD6. The simulation can be improvised by appending more nodes to the existing network considered and by contrasting varying protocols on this proposed scheme.

In [8], the subsequent improvements can be made to dwindle the end to end delay in the propound strategy.

In [14], in time to come the selfsame suggested recognition and mitigation finding can be operated on further progressed reactive routing conventions.

In [15], in future the authors of this work plan to evolve an IDS to distinguish between the malicious and regular movements in the network.

In [16], the researchers can enhance this projected work by appending more evaluation metrics to the system. And can also aim to improvise the put forth system to lessen the message expenses.

In [17], the authors may expand the work by providing a varied preventive strategy for attacks by incorporating some light weight mechanisms. And can also re-script the algorithm so as it could handle more varied kinds of attacks.

In [19], the work to be done in near future is to evaluate and analyze the proposal using some kind of simulator. Varied kinds of evaluation metrics can be taken for getting better and clearer idea of the proposal.

In [20], the future work could be to modify the mechanism so as it can handle flooding attack when the threshold set is reduced. And also cryptography can be adopted for extending security against attacks.

ACKNOWLEDGEMENT

We thank the management of M.J.C.E.T for providing us enough resources to prepare and experiment our work. We are thankful to our faculty members and guides for their support.

REFERENCES

1. Wikipedia, https://en.wikipedia.org/wiki/Mobile_ad_hoc_network
2. Mr. Sachin Korde, et al., "Review on Network Layer Attacks Detection and Prevention Techniques in Mobile Ad Hoc Net-works", International Conference on Inventive Systems and Control, (2017), https://ieeexplore.ieee.org/document/8068654 .
3. Rahma Meddeb, et al., "A survey of Attacks in Mobile Ad hoc Networks", International Conference on Engineering & MIS, (2017), https://ieeexplore.ieee.org/document/8273007.
4. Sagarika Kar Chowdhury, "Attacks and mitigation techniques on mobile ad hoc network- A survey", International Conference on Trends in Electronics and Informatics ICEI, (2017), https://ieeexplore.ieee.org/document/8300907.
5. Sonia Verma, et al.,"A Study of Active and Passive Attacks In Manet", IJSRD - International Journal for Scientific Research & Development, Vol. 4, Issue 09, (2016), http://www.ijsrd.com/Article.php?manuscript=IJSRDV4I90235.
6. Sumaiya Vhora, et al., "Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", IEEE International Conference on Electrical, Computer and Communication Technologies, (2015), https://ieeexplore.ieee.org/document/7226060/.
7. Sarika U Patil, "Gray Hole Attack Detection in MANETs", 2nd International Conference for Convergence in Technology, (2017), https://ieeexplore.ieee.org/document/8226087.
8. Mohsin Mulla, et al., "Efficient Analysis of Lightweight Sybil Attack Detection Scheme in Mobile Ad hoc Networks", International Conference on Pervasive Computing, (2015), https://ieeexplore.ieee.org/document/7086988/.
9. Priyanka Yadav, et al., "A Secure AODV Routing Protocol with Node Authentication", International Conference on Electronics, Communication and Aerospace Technology ICECA, (2017), https://ieeexplore.ieee.org/document/8203733.
10. Bhavin Joshi, et al., "Mitigating Dynamic DoS Attacks in Mobile Ad Hoc Network", Symposium on Colossal Data Analysis and Networking, (2016), https://ieeexplore.ieee.org/document/7570941.
11. Roshani Verma, et al.,"New Approach through Detection and Prevention of Wormhole Attack in MANET", International Conference on Electronics, Communication and Aerospace Technology ICECA, (2017), https://ieeexplore.ieee.org/document/8212719/.
12. Avni Tripathi, et al., "Mitigation of Blackhole attack in MANET", 8th International Conference on Computational Intelligence and Communication,(2016), https://ieeexplore.ieee.org/document/8082683.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

13. Sakshi Garg, et al., "Enhanced AODV protocol for defense against Jellyfish Attack on MANETs", International Conference on Advances in Computing, Communications and Informatics, (2014), https://ieeexplore.ieee.org/document/6968588.
14. Dhiraj Nitnaware, et al., "Black Hole Attack Detection and Prevention Strategy in DYMO for MANET", 3rd International Conference on Signal Processing and Integrated Networks, (2016), https://ieeexplore.ieee.org/document/7566704.
15. Alka Chaudhary, et al., "Design an Anomaly Based Fuzzy Intrusion Detection System for Packet Dropping Attack in Mobile Ad Hoc Networks", IEEE International Advance Computing Conference (IACC), (2014), https://ieeexplore.ieee.org/document/6779330/.
16. Han-Chao Lee, et al., "A responsive probing approach to detect dynamic intrusion in a MANET", 7th International Conference on Information, Intelligence, Systems & Applications (IISA), (2016), https://ieeexplore.ieee.org/document/7785357.
17. Gurveen Vaseer, et al., "A Novel Intrusion Detection Algo-rithm: An AODV Routing Protocol Case Study", IEEE International Symposium on Nanoelectronic and Information Systems, (2017), https://ieeexplore.ieee.org/document/8293915.
18. H. Ghayvat, et al., "Advanced AODV Approach for Efficient Detection and Mitigation of WORMHOLE Attack IN MANET", Tenth International Conference on Sensing Technology, (2016), https://ieeexplore.ieee.org/document/7796286.
19. Albandari Alsumayt, et al., "Detect DoS attack using MrDR method in merging two MANETs", (2016), 30th International Conference on Advanced Information Networking and Applications Workshops, https://ieeexplore.ieee.org/document/7471316.
20. Mohan Kumar S B, et al., "A Policy based preventive measure against flooding attack in MANETs", IEEE International Conference on Recent Trends in Electronics Information Communication Technology, (2016), https://ieeexplore.ieee.org/document/7808105.