International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 1272-1278
https://doi.org/10.70917/ijcisim-2026-3552
Article

PREVENTION AND MITIGATION OF MOBILE NODE DRAINING IN MANET

Ankita Chourasia[1], Sanjiv Tokekar[2]

[1] Computer Science & Engineering, IET-DAVV, Indore, India.
Email: **ankita.chourasia29@gmail.com**
[2] Electronics & Telecommunication, IET-DAVV, Indore, India.
Email: **stokekar@ietdavv.edu.in**

Abstract: —Mobile ad hoc networks (MANETs) are composed of mobile nodes deployed in areas that are often difficult to access. These networks are capable of dynamically discovering and utilizing various functionalities through wireless communication. Among the findings are high computational efficiency, low energy consumption, storage reduction, and increased detection capabilities. The communication is open and, hence, prone to various security threats. The limitations in power supply combined with the need to balance consumption of power for communication and computing have resulted in research efforts, establishment of security protocols, and security assault prevention becoming extensive. The mobile node is the most vulnerable component due to its limited availability and maximum usage. The energy loss in mobile nodes not only reduces their lifetime but also affects the overall network performance negatively. The objective of this study is to detect and eliminate attacks by using power consumption as the primary indicator for identifying energy-draining activity. Using the open-source simulator, the previously mentioned work has been implemented in accordance with IEEE 802.11b standards. The suggested scheme's performance has been evaluated in terms of power draining and packet delivery ratio (PDR).
Keywords: AODV, NS-2, Draining Rate, Resource Deflection, and MANET

1. Introduction

A Mobile Ad Hoc Network (MANET) comprises a heterogeneous collection of mobile devices—such as laptops, smartphones, and radios—that communicate with each other through technologies like Wi-Fi, cellular networks, or local RF links. This type of wireless network is independent of fixed wired infrastructure as it can supply the required network functionality. Moreover, they can migrate and rearrange themselves during the communication. MANETs can either be restricted to the area of a certain group of wireless devices or can be connected to the internet.

Copyright: © 2026 by the authors

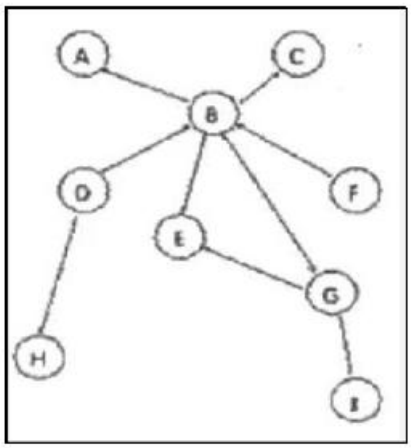

Figure 1: Mobile Ad-hoc Networks

2. ROUTING PROTOCOLS

Routing is a procedure in which a path through one or more networks is selected so that data packets can move from a source to a destination. The purpose of routing is to discover the route from source to destination. The different routing protocols for MANET can be used to identify the possible paths for the packets, which are called S and D when travelling from one node to another [12]. A few recommended techniques for routing are in the area of a MANET. This is done to enhance the

performance of the network and to utilize it properly. Routing protocols in MANETs are generally categorized into three main types: proactive, reactive, and hybrid. In proactive protocols, every node works on a routing table containing complete routing details related to the network[5].

The routes are thus created by the node ahead of time. Therefore, reactive protocols take less time to implement than finding the route techniques. On the contrary, nodes in reactive protocols only build routes when they are necessary. In contrast, a hybrid approach includes both reactive and proactive methods in the nodes. AODV is classified as a reactive routing protocol, which is based on the hop-by-hop route discovery method. One of the methods through which a node learns the way to a certain spot is through the sending of a precise address Route Request (RREQ). Subsequently, the intermediate nodes apart from following the desired route also make a return path to the ultimate destination [13] [14].

3. SECURITY THREATS

A security threat or attack is any deliberate attempt to undermine a system or its assets—such as information or resources—by revealing, tampering with, disclosing, weakening, incapacitating, or damaging it to achieve unauthorized objectives. It is the process of revealing data privacy and reducing resource capacity without permission or authorized access. Typically, there are two types of security attacks., depending on their method of assault, which follows below;

Below is a summary of the most popular power-draining attack;

1. Denial of Service (DoS) Attack **:** This type of resource exhaustion attack occurs when a user tries to access a service or resource but is unable to do so because of excessive or invalid requests that overwhelm the system. On occasion, it could be excessively performed with any resource. One way of achieving this kind of offense in wireless networks i.e. MANET is flooding [10].
2. Distributed Denial of Service [DDoS] security threat: [10] this is an advanced DoS assault that varies the degree of resource interruption it is causing. In this case, a number of compromised nodes are sending requests to a legitimate node. Several attackers substantially affect both node lifespan and network performance. This paper includes a detailed examination of DDoS attacks and their mitigation in mobile networks.
3. Vampire Attack: This power-draining attack [4] [10] is consuming nodes' power resources. It is divided into stateless and tasteful protocols. It indirectly adds to the early death and draining of the power of mobile nodes by causing heavy packet flow in the mobile network.

4. PROBLEM STATEMENT

The analysis determined that a battery was the only power source for the single node. Its life-criticality and limited availability were the reasons why it was the most attacked by all securing measures. Recent researches on floods, vampire, DDoS and basic DoS intrusions have highlighted the critical need to address resource depletion issues in mobile nodes operating under dynamic conditions. The issue of resource depletion while employing routing protocols has been a significant focus in the field for many years. Most of the approaches as per studies conducted, either try to stop the routing table generation or reach the point where flooding starts. They are estimating the network traffic and determining the highest sequence number during the attack at the moment.

In simple words as the control of complete body depends upon heart in the same line the life of node completely proportional with remaining power of battery. Flooding helps attacker to unnecessary consume battery power in very rapid rate so that in case of ad hoc routing intermediate nods will not be available to transfer the packet and sender either need to choose longest path or will not be able to have communication with destination. The power of the flood is included in all of the previously set methods for estimating flood harm. But none of

them have dealt with the node battery's energy loss rate or any other aspects related to the remaining energy.

These tactics become pointless when the adversaries use a low-density but high-impact hybrid-flooding approach, like in a dynamic flooding case. In this scenario, attackers won't go for a large volume of packets; however, they will need a lot of computational power for packet forwarding or processing. Similarly, attackers can't be stopped by static threshold-based algorithms since they use different strategies to confuse preventive systems. Solutions have been created by differing authors who looked into those techniques and suggested mitigation measures according to the signs of an attack. This research suggested that the major part of the literature identified flooding characteristics as a means to detect a dos attack. Despite the fact that flooding is the easiest method to execute a DDoS or DoS attack, more sophisticated techniques have been created for situations where it is hard to spot the attack. Each one of these instances has been investigated, and it has become evident that such attacks focus on the network's resources rather than the routing protocols. An energy-draining assault is said to take place when a malicious node harnesses the power of other nodes, thus reducing the total power that is available to all of them. [4] Citations [7] [8] [11]

Research indicates that among the most common types of energy-draining attacks are DDOS and vampire attacks, where the last one is considered the most energy-consuming since the node sends messages which the other nodes have to process even if they are not the addressee [4]. The battery of the network node is making less energy due to very high energy demand.

There have been cases of attacks in the category of resource draining which can kill mobile nodes completely by drawing all power from them.

It is stated that energy-draining attacks do not restrict themselves to specific protocols. Attacks of this nature reroute network traffic; this could either be the result of a high rate of energy consumption

or large packet numbers. These scenarios have different impacts on the rate of energy loss in mobile networks. Energy-draining attacks do not change or interfere with recognized paths or routing table data, even when they pretend to be the real correspondents.

Energy draining attacks are known for being extremely hard to detect within networks as they do not rely on any specific protocol. According to [7], an attacker has two options for carrying out an energy-draining attack: either to introduce a rogue node into the existing configuration between the source and the destination or to compromise an insider node. It starts sending packets to other nodes in an attempt to drain their batteries as soon as it has finished altering the header data.

This research employs AODV [6] as the core routing protocol for establishing system topology and enabling data transfer. Malicious nodes may either eavesdrop on RREQs or generate unnecessary RREQs to other nodes, even when there is no actual data to be transmitted. After the destination's sequence number ceases to be valid, repeat this operation several times. By transmitting every single packet it receives, the Attacker node is also draining the energy of the other nodes. Changing the header information of the packet prior to forwarding it is yet another way an attacker can make the receiving nodes work harder. This can be achieved by notifying the new address instead of the previous one. The Attacker node has to possess a part of the detected route to do that. Such impudent behavior is pretty hard to detect. Since the Attacker [9] node aims at the batteries that are the highlight part of the nodes, the entire mobile range

is at risk. AODV is not ready to counteract the resource-draining attacks. Consequently, a wireless mobile network is more vulnerable to the attacks of the malicious actors.

5. METHODOLOGY

Studies on mobile nodes have revealed that their lack of configuration tools and portability are the main factors that expose them to multiple security threats. The issue with power draining is the design of mobile node state that transducers are required

with tiny processors to make mobile node functional and network active. Remote location placement and ad hoc nature make it impossible to deploy mobile nods with live and continues power. Other part nothing can run without energy and battery power is the source of energy to mobile nodes. Attackers always aim to drain the battery intentionally so that mobile node can exhaust early-stage dead fast. The aim of this research methodology is to diagnose such situation and mitigate the attackers nod to resume the actual darning of mobile node and improvise their life. A key goal is to investigate methods that can proactively minimize or eliminate energy loss resulting from resource-draining attacks.

Among the numerous forms of resource-exhausting attacks, flooding, vampire, DOS and DDOS are the most widespread. These types of intrusions are regarded as universal since they can affect virtually any network, routing scheme, or system design, irrespective of the operational layer they target. Despite all the widespread attempts, the battle against flooding is still going on and there will always be a need for further improvements. For instance, some research departments will use maximum sequence numbers and network traffic time to launch attacks whereas others will be using flooding or hello flooding. Transitioning a security level from low to high and ascertaining the rate of depletion is an issue that no one can handle at present.

The data collection header and the estimated draining rate are depicted in Figure 4.2. The suggested technique evaluates the measured draining rate and packet count of each subset, which ranges from 1 to 1,000,000 packets. The threshold value is determined by averaging the draining rate over all subsets. The model utilizes both packet count and draining rate as predictive variables to estimate the total energy likely to be consumed and the residual energy to remain during the communication. In the next section, the algorithms used are discussed in detail. An accompanying list presents (N) packets with their respective estimated energy consumption and draining rates.

The total energy expenditure estimate is shown here.

The drainage rate for the ith subset is represented by Di.

All projected data packets meant to be sent during the communication process are signified as N.

number of sample subsets considered of total packets transmitted

Derivative= Mean Drainage Rate for n Subsets

The derivative of Dravg is the total of D1+D2+D3[...Dn] over n.

The radial gradient is responsible for the total energy expenditure at each energy level being equal to the total energy available.

Finally, TEEec is determined through the total expected residual energy (TERE) after the complete communication. This 5% additional consumption for heavy traffic or environmental problems has been considered making the network very close to the final threshold. Consequently, the final threshold will be Tr = Level of Threshold Energy.

The formula for Tr is as mentioned: TEEec + [(TEEec*5)*100] two (2)

Energy Draining Attack Implementation: To deplete resources, a long-distance attack model utilizing high-transmission nodes has been considered. The attack has been executed for both insider and outsider threats.

Long-range, high-transmission nodes constitute an external attack vector: these adversaries are equipped with elevated power and powerful transceivers, which grant them extended range and throughput. Because of their advanced configuration, they represent a serious external threat and degrade overall network performance. Internal attacks are modeled as flooding at different intensities; compromised nodes overwhelm the network with RREQs and redundant packets in modes such as heavy flooding, Simple flooding,

moderate flooding, and moderate flooding's with high consumption.

Step 1: Setting up the Mobile Network Initially, a MANET consisting of N nodes is created, each with the same initial energy level (E). The network is deployed over an area of size X × Y. All nodes implement an enhanced AODV detection and prevention mechanism. In this setup one node is designated as the sender (S) and another as the receiver (R), with the total number of packets to be transmitted denoted by Tp.

Step 2: Determining the Default Threshold Before initiating the transmission, packets are divided into multiple groups based on the required transmission volume, such as 300, 500, or 1000 units. For each node, the initial and final energy levels are measured before and after the transmission process. The average of the remaining energy across all nodes is then computed and normalized by the total node count to estimate the overall energy usage during communication. The total energy expenditure is subsequently correlated with the number of transmitted packets to determine the energy consumed per packet. This entire evaluation is carried out sequentially for all packet groups in increasing order of size to derive a weighted average depletion rate. Finally, a threshold value (Tr) is determined, incorporating a permissible deviation of 5%.

Step 3: Detecting External Energy-Depleting Attacks(First Level) In order to debar the network from resource-consuming attacks like DDoS, vampire, or DoS the system will gather ongoing intermediate energy readings from every node via the base station or mitigation server. It will compute the draining rate of each node. Power usage or draining efficiency of the nodes that are indicated as high are marked as dubious. The dubious nodes are recorded on a blacklist which bars them from any further communication. Adjacent nodes are also informed and requested to isolate the nodes on the blacklist.

Step 4: Preventing Attacks (Second Level)

At this point, the system is continuously collecting

the intermediate energy levels of all mobile nodes operating. The information is forwarded to the base station for further investigation. If nothing suspicious is found, the security level of the network can be elevated for increased protection. The draining rate of each node is recalculated with respect to its residual energy and total packets sent to confirm it is functioning properly.

Step 5: Identifying and Handling Abnormal Nodes

In the event that a node expends its power at a rate much quicker than other nodes, it will be labelled as a victim node and consequently, it would be put out of action for a limited time to avoid the complete loss of its energy. The nodes that display very high or unnatural energy consumption are considered as potential attackers and thus, added to the blacklist. The blacklist is, in fact, communicated to all the connected nodes so as to provide uniform protection. Nodes that bear the signs of draining patterns that are abnormal would be excluded from access permanently, thus allowing the network to be stable and secure.

6. EXPERIMENTAL ANALYSIS

The whole evaluation process was done in a number of different environments. Initially, the NS simulator will imitate the necessary scenarios and afterwards will assess how well the proposed solution performs with the required corrections. The proposed solution was subjected to various phases during its experimental assessment. The first step in analysing the mobile network's threshold value involves building standard wireless mobile network scenarios with varying numbers of nodes.

The network's robustness and ability to grow were tested through the formation of a uniform network and exposing it to different situations with 10 and 20 nodes. Different packet transmission rates (100, 1000, 5000, 10,000, 100,000) and time

intervals (one second and one hundred milliseconds) were used in our study of battery consumption while the deployment area was kept the same. Once the battery depletion condition was

established, a threshold for each packet range was calculated by us.

Findings take into account the training data when determining the threshold. The threshold value in this work is determined using the quartile analysis. It creates a confidence interval whose width will serve as the cutoff point for judging a node's authenticity. The following four crucial criteria will be used to assess the suggested solution's performance:

1. Battery life

2. Packet Delivery Ratio

Using NS-2 simulator, scenarios were built with 10 & 20 nodes and each having the standard IEEE 802.11.b the entire simulation was conducted under both mobile and static conditions.

The entire results acquired are presented in the form of graphs as depicted in the figures below:

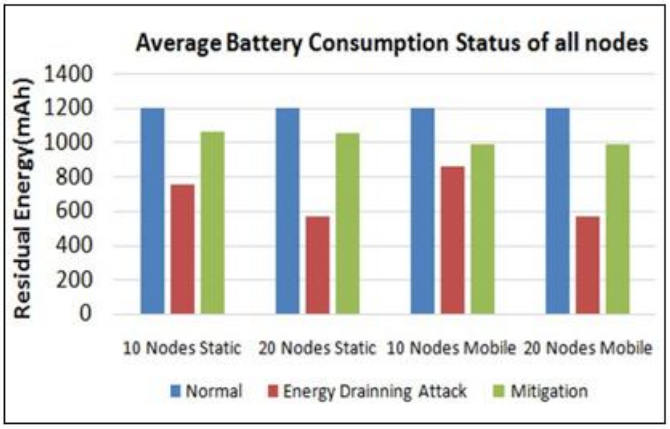

Figure 2: Average Battery Depletion of all Nodes

Fig 2 & Fig 3 demonstrate the performance of mobile ad hoc network on various situations. Fig 2 demonstrates average battery depletion and Fig 3 shows packet delivery ratio. First two comparative bar demonstrates static network performance and second two demonstrate movable state of mobile network. Green bar for all conditions demonstrates that performance after mitigation works better than attacking situation. Although security always comes with overhead but preventive approach helps to keep data safe in parallel with functional

approach. In the same manner mitigate algorithm is working better than attacking situation but lacking with actual routing protocol.

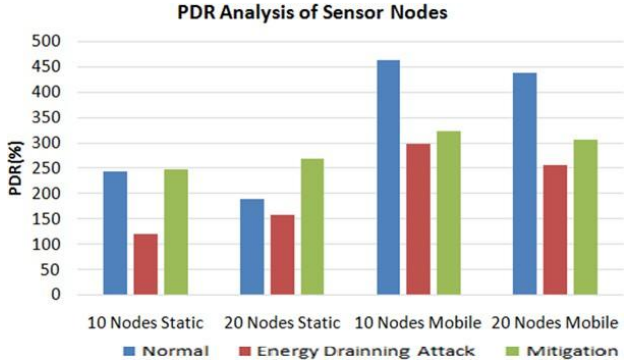

Figure 3: PDR Examination of Nodes

7. STUDY CONCLUSION AND FUTURE SCOPE

The study concluded that excessive energy consumption caused by malicious activities severely affects the efficiency and reliability of wireless mobile networks. To address this issue, it introduced a flexible approach in which the threshold value is dynamically determined based on observed energy consumption patterns and previous operational behavior. The findings show that this mechanism effectively minimizes the negative impact of energy-exhausting attacks, leading to better battery preservation in the affected nodes. Although the method was carried out using AODV, the study also indicates that the proposed technique can be combined with DSR or other protocols to improve the resilience of mobile systems against various resource-depleting threats.

Reference

1. M. Bharti, S. Rani and P. Singh, "Security Attacks in MANET: A Complete Analysis" 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, pp. 384-387, doi: 10.1109/ICDCS54290.2022.9780760.

2. K. Vanitha, AM. J. Zubair Rahamaan, “Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol ”, Cluster Computing, Page No: 1–9, 2018.
3. Chen, Joy Iong Zong, and Kong-Long Lai. “Machine Learning based Energy Management at Internet of Things Network Nodes” Journal: Journal of Trends in Computer Science and Smart Technology September 2020, no. 3 (2020): 127–133.
4. F. S., H. Kunze, J. Ernst and D. Gill, "A Novel Cross-Layer Adaptive Fuzzy-Based Ad Hoc On-Demand Distance Vector Routing Protocol for MANETs " in IEEE Access, vol. 11, pp. 50805-50822, 2023, doi: 10.1109/ACCESS.2023.3277817.
5. R. Vallikanu, A. George, S. K ," Routing and charging scheme with ferry nodes in Mobile-Adhoc networks " International Conference on Intelligent Computing and Control(I2C2), India, pp.1-4, doi: 10.1109/I2C2.2017.8321918
6. S. Chandia and M. Devapriya, "Loyalty pair neighbours selection based adaptive retransmission reduction routing in MANET" International Conference on Communication and Electronics System (ICCES), Coimbatore, India, pp. 1-6, doi: 10.1109/CESYS.2016.7889972.
7. A .Chourasia, “Reinforcement Learning based Security Policy to Mitigate Worm hole, Black hole and Gray hole Attacks in MANET ” , ISBN : 979-8-3503-8793-3 , DOI : 10.1109 / IC457434. 2024.10486553, April 2024.
8. S. Darwish, S. J. E. Ta and G. Ghinea, "Security Server-Based Architecture for Mobile Ad Hoc Networks" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 2012, pp. 926-930, doi: 10.1109/TrustCom.2012.260.
9. R. S. kumar, D. R. V and P. S. Lal, "Integrated Random Seed and Data-dependent Dynamic Key Generation for Security in Mobile Ad hoc Networks " 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023, pp. 449-453.
10. H. Amraoui, A. Habbani, A. Hajami and E. Bilal, "Security & cooperation mechanisms over mobile ad hoc networks: A survey and challenges "2017 International Conference on Electrical and Information Technologies (ICEIT) Rabat,Morocco.pp1-6,doi:10.1109/EITech.2017.8255313.
11. A. K. Bandani, M. V. Subramanyam and K. S. Prasaad, "An Efficient Residual Energy Based Routing Strategy for Mobile Nodes in MANETs using the CDROA-OSPF Protocol " 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, pp. 1-14,2024.
12. S. Tsimenidiis, T. Lagkas, and K. Rantos, “Deep learning in iot intrusion detection ” Journal of Network and Systems Management, vol. 30 , pp. 9–40, 2022.
13. J. S. Dhatterwal, M. Singh Naruka and K. S. Kaswan, “Multi-Agent System based Medical Diagnosis Using Particle Swarm Optimization in Healthcare”, International Conference on Artificial Intelligence and Smart Communication (AISC), Noida, India, 2023, pp. 889 – 893.
14. A. Chourasia, “ Improved Wireless Mobile A d Hoc Network Using Security Schemes against Black - hole Attack”, ISSN 2250-2459,vol 10,pp 61-69, IJETAE 2020.
15. Sajjaa, G. S. , Naved, M., Phasinam, K. “Various Soft Computing Based Techniques for Developing Intrusion Detection Management System”. ECS Transactions, 3335.2022