International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

An Empirical Study of Destructive Nodes Characterization in Wireless Networks

Srinivas Aluvala

Department of CSE, KL University, Guntur, India
Department of CS & AI, SR University, Warangal, India
srinu.aluvala@gmail.com

K. Rajasekhar
Department of CSE, KL University, Guntur, India
rajasekhar_cse@kluniversity.in

Abstract— Mobile Ad hoc Networks (MANETs) are deployed in various new public and domestic environments, going up to new needs in terms of concert and effectiveness. According to the wireless dynamic nature, some needed services like security for network maintenance, trust-based routing and resource management among network nodes are not carried out as good as expected. Also, the ad-hoc networks are vulnerable to secure communications and multiple attacks can participate in various layers of a network stack. Destructive nodes have chances to change or discard routing specifications, sometimes it can send false routes to capture source data packets to pass through themselves. Some protocols have been designed to address the complication from secure data communication. Even though, a secure protocol cannot handle all kinds of attack detection and elimination in all situations. New secure data communication wireless protocols need to focus these challenges, because security care is not natively built in MANET. Therefore, in this research paper, analysis of destructive nodes characterization and impacts on wireless networks investigated the multiple attacks behaviour, activities of the attacks all through neighbour selection, path establishment from source to destination, creating awareness of attack presence detection knowledge to the normal devices during path discovery and data transmission mechanisms. Legitimate nodes need to be building with secure transmission knowledge to make sure trusted communication, ensure validation, honesty, and privacy to classify the attacks in MANETs.

Keywords- MANET Security; Destructive Nodes; Legitimate Nodes; Protocol Challenges; Awareness of Attacks; Secure Transmissions;

I. INTRODUCTION

MANET is a collection of various wireless products called as nodes, which passionately join and convey information about each other. These nodes can be laptops, desktops with wireless local area network cards, Smartphone's, tablets, Bluetooth, Personal Digital Assistants (PDA), or other model wireless communication devices. A MANET is consisting of nodes that can contact each one using wireless channels. It is also achievable to have contact with various nodes in a static infrastructure, depending on the kind of available network. Some situations where MANETs can be used are environmental and industry associate's information sharing during a disaster relief, earthquake, hurricane, official and education meeting, and defense personnel communication also other kinds of information exchange in a combat zone. Figure 1.1 demonstrates what mobile ad-hoc is, it shows the MANET communication structure both infrastructure and infrastructure less model. In common, a node can be some calculating tool that uses the air as the broadcasting medium. As described, the node may be connected to a human, a roadside vehicle, or a moving object to permit the contact among them.

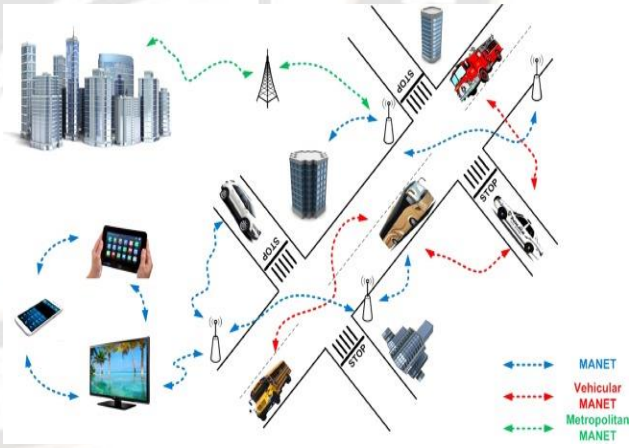

Figure 1. MANET Communications

In this atmosphere, a path between two nodes may consist of one or more hops in the MANET. A major issue in a wireless network is discovering and maintaining paths since node movement can cause dynamic changes. Protecting MANET is high challenging than defending conventional networks for a lot of reasons. Uniqueness such as unpredictability, channel listening, energy loss, mobility, the security issue, diverse device communication scarcity of channels, collision, congestion, noise as well as interferences creates the network naturally least secure. Apart from that MANETs are much less secure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

infrastructure due to dynamic link connection depends on the movements of nodes, network size, changes in the applications depends on the climate, and some other factors. As a final result, it is tough to perfectly characterize legitimate behavior. Therefore, it is frequently tough to differentiate malicious character from normal character because of the unpredicted events.

In the network, a node can be the source to generate the packets, or it can be the final destination, or else it can be a forwarding intermediate of data packet transmission. When a node acts the role of a forwarder, it serves up as a routing device that can collect and retransmit data to its routing neighbor towards the destination. Time to time network nature can vary due to the environmental changes. These wireless networks have a lot of rewards:

- Dynamic Network Configuration: it is so easy to vary the network topology like nodes count, terrain size, coverage, traffic counts, and packet size, packet rate and so on.
- Minimum deployment Cost: MANETs can be placed on the convenient area; So that no infrastructure expensive such as cables, connectors or towers. Consume very less time to mane wireless connection
- Battery Powered: Without power supply also, nodes can function with the support of battery power
- Connection: Anyone can join and leave any time from wireless connection
- Relocation: Nodes can relocate from its location to another place whenever it wants.

II. CHALLENGES IN MANET

In a MANET, all the placed nodes assist with each new node to transmit the packets, so each node is efficiently act as a router. This is the major problem in wireless routing. This creates routing threaten in networks. In this segment, some of the other complications in MANETs are described:

- No centralized or fixed server is needed to maintain the state of the clients. This makes clients loyalty as a question.
- The dynamic network allows network keeps on changing from situational circumstances. Therefore, the protocols developed for such environments must also be adjustable to the network changes.
- The nodes deployed in challenging terrains operate on battery power and have demanding electricity consumption needs owing to constant engagement. The primary concern in this network pertains to energy conservation.
- Node identification (ID) maintenance is also the critical issue in MANET; Node ID duplication can be the issue due to open contact is quite significant. A MANET topology needs an ubiquitous ID allocation technique
- Network delay, node delay can occur because of long route communication. The routing loop is also being a cause for long delay. Packet waiting time due to buffer overloads also the reason. Unknown nodes can use the channel with intentionally to block the other's usage can happen
- Bypass route can be established by attackers to eliminate genuine communication. This causes the data loss heavily. So, the outcome of throughput, packet delivery ratio, and overhead can affect a lot, thus minimizes total network performances. Because every node participates in the route establishment, it may be legitimate or non-legitimate.
- Due to network dense high collapse can occur to the network, this implies in communication ranges of each node. High bandwidth utilization, energy loss, updating neighbors and routing path, due to network load high congestion can occur,
- Simultaneous several node communications lead high interference and noise inside the network. Bogus resource information can be exchanged with the nodes; this can be shared by the non-legitimate nodes. This affects the network lot. Due to this total network can be jammed in some emergency situation.

Mobile Ad hoc Networks (MANETs) has distinctive characteristics that render them vulnerable to various types of assaults. Due to the fact that communication takes place in a shared public environment, wherein multiple nodes collaborate to transmit data and control packets within the network, the identification of certain attackers can provide a challenge. Therefore, designing a secure system for wireless communication poses certain challenges compared to static cable networks. This paper presents an analysis of the security objectives for a Mobile Ad hoc Network (MANET). This paper examines various models of security threats and discusses their potential for assault.

The rest of the following paper is designed as follow: Section II discussed about the related works. Section III describes the multiple promising attacks on MANETs. Section IV express the conclusion of the analyzed paper.

III. RELATED WORK

A Mobile Ad hoc Network (MANET) refers to a network architecture consisting of mobile routers that are interconnected by wireless networks and has the ability to configure themselves autonomously. The routers have the freedom to travel in a random manner and arrange themselves in any desired configuration [4]. The DDoS "master program" initiates an attack directive to numerous mobile agents, resulting in the execution of flooding attacks on the targeted entity [1]. The susceptibility of wireless networks to radio signal interference is heightened due to their broadcast nature, resulting in disruptions to regular network communications. Jamming can cause disruption to wireless transmission and reception, and this disruption can occur due to interference or collision at the receiver side [6]. The act of denial of service refers to an intentional assault on the availability of a service, with the objective of preventing authorized customers from accessing the service provider [2]. In order to ensure secure communication, it is imperative to apply authentication mechanisms and implement end-to-end authentication. Without these measures, attackers have the ability to manipulate routes within intercepted packets. It is important to note that only communications generated by attackers are considered to potentially include maliciously-composed routes [9]. The concern lies not with the Internet itself, but rather with its tendency to alter mandatory or required information in response to minor changes in protocols. The phenomenon of Distributed Denial-of-Service (DDoS) is rooted in the foundational structure of the Internet [5]. The utilization of the alpha-beta filtering technique enables the algorithm to effectively adapt to the dynamic nature of the network, hence facilitating the detection of colluding assaults perpetrated by hostile nodes [8]. This methodology supports the expansion of the working region, but at the cost of increased complexity at the physical layer. Malicious nodes have the capability to conduct scans for destination nodes that are beyond their range by inundating the network with broadcasts, which are subsequently relayed by each node. In the context of an ad-hoc

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

network, it has been shown that power consumption tends to be elevated due to the transmission of packets by the nodes [10]. Passive attacks primarily pose a threat to secrecy, whereas active assaults pose a risk to integrity. The most severe sort of active attack compromises the availability of broadband wireless networks [3]. The act of cloning a node or engaging in adversarial behavior involves the propagation of the original node's key or identifier, resulting in the creation of other replicas of the specific node inside the existing network, all possessing the same identifier. Furthermore, this cloned node has the potential to disrupt the entire network [7].

A. Multiple Promising Attacks in MANETs

Table 1. Categorization of Attackers

Attackers	Types of Attacks	Characterization
Active Attacks	Data Modifier	This attack changed the legitimate data format Tried to do unauthorized data modification
	Denial of service	Block the regular use of channel by delivering the continues bogus packets
	Playback Attack	A playback attack involves to reproduce the same data again and again or tried to delay the data delivery
		Tried to waste the network resources
	Duplication	Node ID duplication is a massive corruption method by duplication
		Duplicate data's can be store inside the memory to occupy memory space
Passive Attacks	Man in the Middle Attack	Attacks sit between two nodes and silently listens the message communication
	Packet analyzer Attack	Observes the node location from the packet transmissions between nodes
		Extract packet from encrypted format
		Knows the packet frequency and length
Adaptation	Misrouting Packet attackers	Reroute the data packet from its original path to the incorrect directions
	spoofing attacks	Spoofing attack act like another node by capturing IP, AR or Server Activities
		It can steal data, bypass network control, spread malware across network
Grabbing	Wormhole attacks	In the wormhole attack, a worm node captures the packets at one place and tunnels them to another side, and then partially or completely can drop the packets.
	Black hole attacks	Packets are habitually dropped from a lossy network; the black hole attack is tough to monitor and prevent. It increases its destination sequence number and act like destination some times. Selectively it can drop the packets at every random packet at every random period.
Untruth Attack	Deficiency attacks	The main aim is to consume lots of resources like the energy, bandwidth by continually makes them active unnecessarily
	Path rescue attacks	Data packets might not arrive at the final destination because of the wireless nature, due to link loss or because of the attacker's presence.
Breaking attacks	Packet droppers	Direct breaking to the control packets could be done by the packet droppers.
	Flooding attacks	Challenger also might break off the usual process in the transmissions by flooding the massive unnecessary packets to the destination
	Non-Cooperative attacks	Non-cooperation from the neighbors and routing nodes to complete in the network executions launched by the attackers

B. Attackers and Their Behaviors in Wireless Communications

In common, the non-legitimate attacks of routing can usually be classified as routing interruption attacks and resource spending attacks. In routing interruption model, the attacks try to disturb the routing techniques by diverting packets of incorrect paths; during resource spending attacks, some destructive nodes may try to insert false information in order to utilize the network resources.

1.B.1. Data Modifier Attacks (DMA)

In this type of DMA attacks, few of the control packet fields of the data's sent among the nodes are change, thereby resulting

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

in packet transmission may be diverted, dropped or information may change. The coming sections talk about a few of these kinds of malicious attacks.

 One issue that can arise in network communication is the presence of false packet sequence numbers. The adversaries possess the capability to modify the Sqn (sequence number) in the path request messages or path reply messages with the intention of presenting a recently updated path. Occasionally, misbehaving attackers, denoted as M, obtain a path request (PREQ) either from the source node S or an intermediate node I, which is intended for the destination node D. The attackers get the path reply PREP and unicast it to the subsequent node that possesses a maximum destination sequence number (Sqn) greater than the latest publicly announced Sqn by D. Node S first acknowledges the PREP (Packet Reception Event Protocol) and thereafter facilitates the transmission of data packets to node D via node A. If the destination sequence number (DSN) received by the destination (S) is lower than the one transmitted by the source (M), the packet will be rejected by the destination as an outdated entry. The state will remain unchanged until an appropriate precondition with a higher squadron maximum than that of A is received from source S.

 False hops count: This kind of attacker can maximize the option that they are joined in a recently constructed path by arranging differently the hop count (HC) field of a PREQ to the minimum hop count. Similarly, as like path changing attack of Sqn, the HC field in the routing messages is changed to get to attract the data packet.

 The Figure 2 illustrates the occurrence of a false path, wherein the attack behavior of path collapse is evident. This behavior is characterized by the establishment of a shortest distance path from source node S to destination node D. It is also expected that there is an inability for nodes B and D to communicate with each other, as well as an inability for nodes C and X to communicate with each other. Node M is a node exhibiting disruptive behavior by actively engaging in a denial of service (DOS) attack. Let us consider a scenario in which a sender, denoted as S, transmits a dataset to a recipient, denoted as D, using the path S-A-B-C-D. In the event that M intercepts the aforementioned data packet, it proceeds to eliminate C from the routing list and thereafter transmits the packet to B. B will make an attempt to transmit this message to D, however the likelihood of success is low due to B's inability to receive auditory signals from D. The individual denoted as M has initiated a Denial of Service (DoS) characterization on network D with the intention of causing its collapse.

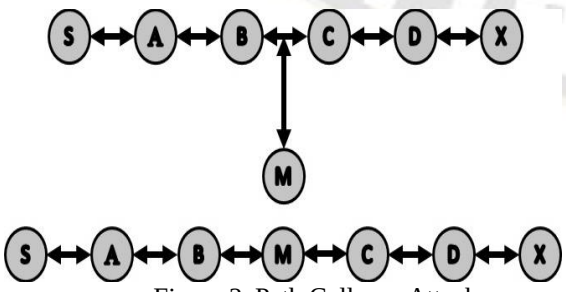

Figure 2. Path Collapse Attack

1.B.2. Denial of service Attacks DoS

In this particular form of attack, as seen in Figure 3, the assailant endeavors to obstruct the access of bona fide and duly authorized users to the network's provided services. A Denial of Service (DoS) assault resulted in the prevention of nodes from establishing contact with a certain system for a specific period of time. The prevalence of Distributed Denial of Service (DDoS) assaults has rendered numerous websites inaccessible to users, leading to significant reputational, financial, and other consequential damages. The subsequent section presents an analysis of the characteristics and patterns exhibited by Denial of Service (DOS) assaults.

 Utilization of limited resources, such as bandwidth and network connectivity.

 Devastation or modification of high sequence number configuration information.

 Physical damages or adjustment of network mechanism.

The following practical events can be used to give a protection for DoS attacks:

 Detection and elimination
 Timely protocol update
 Node & network separation
 Flow Monitoring

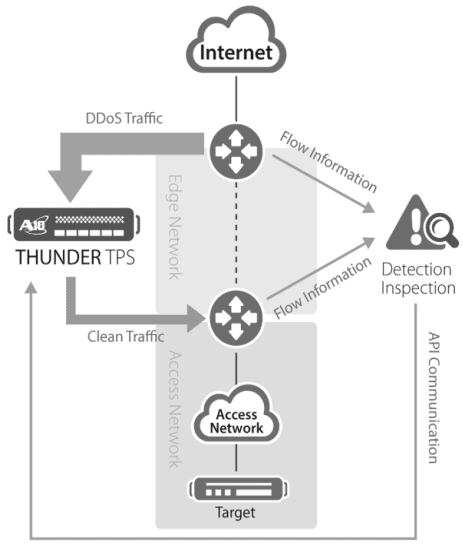

Figure 3. DOS Attack Model

1.B.3. Communication Session Hijacking

Initially the attacker's take-off the IP address of destination or forwarding node and conclude the exact sequence number. Then the attacker performs like DOS on the sufferer. As a result, the destination becomes busy for certain period. So those, the hijacker now carries on the session with the other node as a legitimate object.

1.B.4. Resource Utilization Attack

Security is a major issue in the wireless network due to its dynamic nature and restricted coverage area of each node. The impact of resource utilization attack is one of the DOS attacks in which the malicious node keeps broadcasting control packets in order to reduce the resources of network like bandwidth, energy, node queue to minimize the performance.

Detection of Resource Utilization Attack

 Resource information sharing among nodes
 Monitor high resource utilized node using protocol

1.B.5. Duplication Attacks

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Duplication attacks to disobey genuineness and privacy in a network. An attacker can replicate the node address of some other node in order to change the idea of the network as supposed by someone. Such an attacker can be mentioned as follows in Figure.4

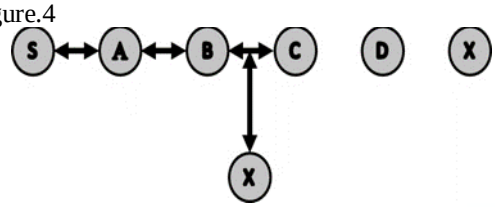

Figure 4. Duplication Attack

Node S plans to deliver data to X and starts a PREQ process. The misbehave attacker M, nearer to S than X, duplicates the destination ID X as misbehaving node ID X'. Misbehave node delivers PREP to S. Without validating the genuineness of the PREP, Source S believes the path to the PREP and initiates to deliver data to the misbehaving node. This kind of malicious behavior can cause a path loop between some nodes in the network.

1.B.6. Grabbing Attacks

In the context of cybersecurity, grabbing attacks refer to malicious activities aimed at injecting fake messages or control packets with the intention of disrupting the normal functioning of a system or process. Monitoring these types of attacks in a network poses challenges due to the deceptive nature of the incoming information, which appears as authentic messages being distributed to the nodes. Figure 5 exemplifies instances of falsification assaults.

Source S initiates the transmission of data to destination X by sending a Path Request (PREQ) message in order to get the routing path to X. The misbehaving node M falsely claims to possess a cached path to destination X, and subsequently transmits erroneous information (PREP) to node S. The S node, in the absence of confirming the PREP, accepts the PREP and initiates the transmission of data to M. Furthermore, the presence of misbehaving nodes inside a network might result in the generation of path errors, leading to the intentional disruption of connectivity to a particular node.

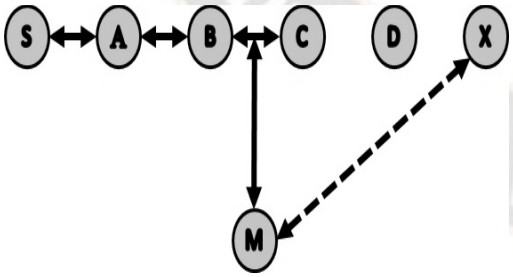

Figure 5. Grabbing attack

1.B.7. Tunneling Wormhole Attack

The wormhole assault is a severe form of attack when two worm nodes are able to exchange packets over a secure "tunnel" within the network, as depicted in Figure 6. During the presence of a worm's node, specifically a worm1 node, it functions by receiving control and data packets at a particular location within the network. Subsequently, it tunnels these packets to the subsequent location in the network, from where they are retransmitted into the network environment. The phenomenon of tunneling between two interconnected attackers is commonly referred to as wormholes.

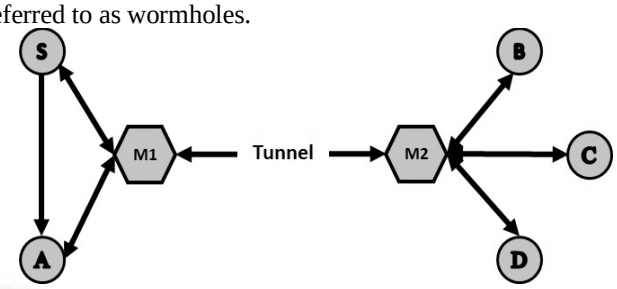

Figure 6. wormhole Connection

Here, M1 and M2 are two worm nodes which joint through a confidential link. Each packet that M1 collects from the source then forwarded through a connected "worm node" M2. A worm node interrupts routing by tunneling and giving shortest path. Such types of malicious activities are tough to monitor in a network, and may harshly spoils the communication between the nodes.

Detection of Wormhole

- Neighbor list analysis-based detection
- Hop count-based detection
- Routing time-based detection
- Worm node location-based detection

1.B.8. Black hole Attack

In this instance of attack, the node endeavors to redirect the packets towards itself by masquerading as the intended destination. In the context of a black hole region, when a node indicates a zero value for each destination, it necessitates that all nodes inside the region must direct their data towards this particular node. Every wireless protocol is vulnerable to a black hole attack. In a flooding-based environment, a black hole exhibits attentiveness towards the path requests for the networks. When a black hole receives a request for a path to a destination, it formulates a response that includes an exceptionally concise route and proceeds to engage with the pathway to manipulate the packets that go between them. The following steps outline the process of black hole detection.

- Validation of destination sequence number
- Valid certificates distribution among legitimate nodes to secure the packet metrics
- Monitoring malicious intention nodes by legitimate nodes
- Both the source and destination validate the confirmation of paths and documents by evaluating them with certificates enclosed in their directory and all path lengths.

1.B.9. Jamming Attacker

In jamming attack, the attacker starts observing the communication channel in order to conclude the regularity at which the final destination is receiving packets from the source. Attacker then starts to transmit the packets on that regularity so that error less reception at the destination is stalled as shown in Figure.7.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

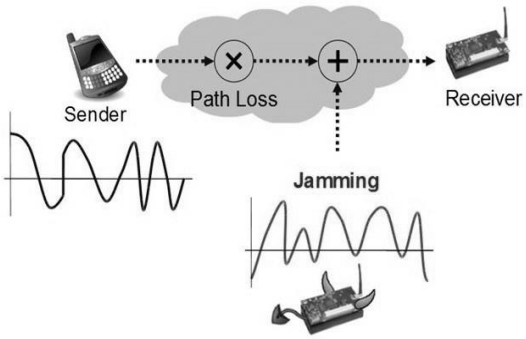

Figure 7. Jamming Attack

1.B.10. Vampire Attack

In our vampire attack, a challenger composes messages with intentionally launch routing loops. We call it the vampire attack, since it shares packets in a circle loop manner as shown in Figure.2. It aims to spoil routing by developing the restricted confirmation of packet headers at forwarding nodes, allowing some packets to continually pass through the same nodes. Also, it increases the path length to drain the nodes life time quickly as shown in Figure.8.

Many papers explore different mitigation solutions to avoid the harm in vampires, and find that while the attack is easy to prevent from negligible control overhead, the vampire widens attack is still far challenging. The first safety technique we discussed is about routing, where any intermediate node can resend the data packet if it knows a short distance path to the final destination. In second validation, we change the detection to assurance that a packet goes through the network. Each node makes sure that the packet goes through each next hop closer to its destination.

Security is a major issue in the wireless network due to its dynamic nature and restricted coverage area of each node. The impact of resource utilization attack is one of the DOS attacks in which the malicious node keeps broadcasting control packets in order to reduce the resources of network like bandwidth, energy, node queue to minimize the performance.

Still more several attacker behaviors reside in the network communication. Many of them discussed above. With the similar behavior with various way of presence attacker can do it activities and deviate the regularity of the network a discussion of the attacks and exploits in the routing protocols, the next section discusses two secure routing protocols for ad hoc wireless networks.

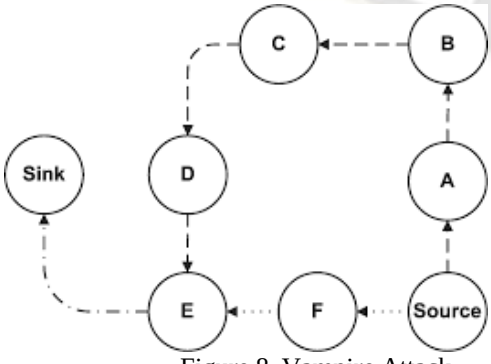

Figure 8. Vampire Attack

In general, wireless communication is very much insecure one if the built-in protocol does not have security awareness and each normal node need to built with that kind of security monitoring knowledge protocol towards each neighbor and path nodes. This avoids the network loss and degradation. The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

IV. METRICS FOR EVALUATION OF EACH ATTACKS TO KNOW THE HARSHNESS DURING ITS PRESENCE AND AFTER ELIMINATION

1. Packet Delivery Ratio: This is the output of total number of received packets at destination divided by total number of sent packets from source.

2. Control Overhead (CO): This is the total number of paths finding packets sent divided by the total number of data received at destination.

The higher CO count is, the maximum overhead of the network and as a result it reduces the competence of the communication.

V. CONCLUSION

The attackers are used to make misbehave nodes and build multiple cruel situations, with dissimilar attackers and with the number of misbehave nodes the network can interrupt much. The final aim of a protocol is to resourcefully transmit the data from source to destinations; in which there is no any malicious node, in order to receive packets from genuine nodes are so easy. Then, when attackers sits inside the network with diverse misbehave environments the received packets are evaluated with the earlier packets can reveal the packet loss based on the overhead values, this validates the impact of a network damages. This happens because of the data is forward to unknown or attackers' direction, some cases packets may discard due to the misbehave activity. This concludes that the routing protocols must design with the secure transmission knowledge with monitoring the changes in network. More investigations are needed in the wireless protocol design.

REFERENCES

[1] Qiang Huang, Hisashi Kobayashi, and Bede Liu,"Modeling of Distributed Denial of Service Attacks in Wireless Networks",IEEE 2003.

[2] Lawan A. Mohammed and Biju Issac,"Detailed DoS Attacks in Wireless Networks and Countermeasures",Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 1, 2006.

[3] Shafiullah Khan, Kok-Keong Loo1, Tahir Naeem, Mohammad Abrar Khan, "Denial of Service Attacks and Challenges in Broadband Wireless Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008.

[4] Sreedhar. C, Dr. S. Madhusudhana Verma and Dr. N. Kasiviswanath, "Potential Security Attacks on Wireless Networks

and Their Countermeasure", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010.

[5] Kuldeep Tomar, and S.S Tyagi, "Quantifying the Impact of Flood Attack on Transport Layer Protocol", International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.6, December 2014.

[6] Pratibha S. Gaikwad, Prof. S. P. Pingat, "Preventing Jamming and Replay Attack in Wireless Applications", International Journal of Innovative Research in Computer and Communication Engineering. 3, Issue 7, July 2015.

[7] Megha Sharma, Rajshree Purohit, "Node Replication Attack Detection Technique in Wireless Sensor Network – A Survey", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084 Volume-3, Issue-8, Aug.-2015.

[8] H. Khosravi, R. Azmi, and M. Sharghi, "Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks",International Journal of Future Computer and Communication, Vol. 5, No. 2, April 2016.

[9] Devikarani Roy, Shilpa Verma, "Vampire Attacks: Detection and Prevention", International Journal of Computer Techniques -– Volume 3 Issue 3, May-June 2016.

[10] Jasmeen Mangat, Er. Jaspreet Kaur, "Review on the Flooding Attacks in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, April 2017.