Hybrid Method for MANET Security against Jelly Fish, Blackhole and DoS

Prachi Sharma
Dept. of Computer Science & Engineering
JNCT
Bhopal,India

Kalpana Rai
(Guide)Dept. of Computer Science & Engineering
JNCT
Bhopal, India

Deepak Jain
(HOD)Dept. of Computer Science & Engineering
JNCT
Bhopal, India

B.L. Rai
(Dean)Dept. of Computer Science & Engineering
JNCT
Bhopal, India

ABSTRACT
The word mobile indicates the meaning of moving and the word ad hoc indicates the meaning of temporary or do not have any type of constant infrastructure, therefore mobile-adhoc-networks implies the networks that are temporary and allows the nodes to move within the network without any centralized administration. In this paper, the concern is on security issues found in the MANET. Then certain criteria for the security of mobile-adhoc-network and some major types of attacks are discussed which are present in it. Mainly this paper is targeted on the attacks of jellyfish and their some types. Due to some special features of MANET such as hop-by-hop communications, dynamic topology and simple and fast setup, this network has suffered lots of issues like issues in security, routing and some clustering issues. Hence, this paper tries to work by focusing on mainly for maintaining the security in MANET and some TCP-based attacks it is facing. .

Keywords
Jelly Fish, Black Hole, MANET, Attacks..

1. INTRODUCTION
In Mobile Ad-hoc Networks the nodes are autonomous and have the ability to work without having any type of constant infrastructure by the use of multi-hop radio-relaying. So the nodes in this network get communicate with each other by having mutual trust since there is no any centralized mechanism is present for the routing purpose of packets. MANET [1] provides the communication for nodes in a wireless medium for transport and routing of packets. In this there is a direct communication in between the nodes that are within the radio-frequency whereas the intermediate nodes provide help in communication for the nodes that are not within this range. Hence some security mechanism is required because it is having the mobile nodes such as they are having limited physical security, scalability, lack of centralized administration and dynamic topology. Due to all these weakness the MANET is more likely to the malignant attacks.

There are various types of attacks are also possible in the MANET due to its vulnerable nature like impersonation, passive eavesdropping, active interfering and denial-of-service attacks.

Therefore, various security mechanisms have introduced such as intrusion detection system, encryption algorithms etc, for reducing the most critical issue of security in the MANET that detect and prevent the malicious attacks

There are various attacks that do not obey the rules of protocol only the attackers of Jellyfish attack may obey the rules. The main strength of this Jellyfish attack is the acceptance of data-plane and the control-plan therefore it is very complicated to detect this attack. Since having the wireless architecture for communication in MANET, it works on the TCP/IP framework to provide the connectivity in between the nodes. To provide the efficient functionality, the basic TCP/IP model is get modified to satisfy the needs of MANET.

Some major issues and sub-issues of MANET are [2] security,multicasting/broadcasting, routing, TCP/UDP, location service, IP addressing, mobility management, clustering, fault tolerance, power management, standards/products and QoS/multimedia. As the to set an upper limit to the security, routing protocol is used of any packet in network, so any mistake in doing this can destroy the whole network. The main problem of routing protocol is it depends only on the reliability of the nodes used in the process of routing. So it is difficult to differentiate in between the nodes that are compromised or the nodes suffered the bad-links.

To find the solutions for security in MANET are the main issues particularly for those that are selecting the private applications must fulfill all the aspects at the time of referring the issues mentioned previously. Vulnerability of MANET is more as compare to the wired networks because it is having the mobile nodes such as they are having limited physical security, scalability, lack of centralized administration and dynamic topology. Due to all these weakness the MANET is more likely to the malignant attacks. Therefore, the main objective of this work is to analyze major attacks of MANET and the JF-attack in MANET based on TCP architecture.

2. VARIOUS ATTACKS
Based on the types of the attackers the attacks in MANET are divided in to two major types that are external attacks and the internal attacks in MANET in the form of protocol including all the rules that are necessary.

- **External attacks**

In this type, the attacker creates traffic within the network by transmitting fake routing detail within the network or by disturbing the nodes such that they cannot provide the services properly [3]. In this the attackers are aimed at disrupting the nodes to from providing better services.

- **Internal attacks**

In this type of attack, for accessing the activities of networks the attacker are required to obtain the access. In this the attacker are act as a new node with few malignant impersonation to obtain the access from the network

2.1. Jelly Fish Attack

This is one of the types of various attacks faced by MANET which is very hard to find out and also it is a type of denial-of-service attack. It is also the type of passive attacks. Within the network this attack generated delay before sending and receiving the packets of data by disturbing the performance of the protocols includes in both the process. This attack is aimed at the closed-loop-flow for attacking. As the TCP is more susceptible towards the drop, delay and mis-order of the packets, so there may be possibility to drop few of the packets and also the sequence get changes because of this. This is the only attack that follows all the rules of TCP, where the Jellyfish node decreases the good-put by reordering of packets, delaying or dropping of few packets. Based on this there are some variants of Jellyfish attacks which are mentioned as:

2.1.1 Jellyfish Reorder Attack

This is the first type of JF-attack in which the packet reordering is done to attack the MANET. As the TCP has more vulnerability towards the reordered packets because of some reasons like it uses the multi-path routing, routes get changed and various modifications done in TCP have been suggested to enhance the protection against the mis-ordering consists of the TCP Stack and the re-order powerful TCP.

2.1.2 JF Periodic Dropping Attack

Due to the overflow of buffer there are losses of some packets in network as a result of traffic in the network which implies that if these types of losses are found regularly at the RTO that is re-transmission-time-out then it will results in the zero end-to-end throughput.

2.1.3 JF Delay Variance Attack

In this type of attack, the attacker required to obtain the access first of the routing path and then it enters the malicious node in the network which randomly delays the packet without modifying packet's order.

2.2. Black-hole attack

In this type of attack, the fake routing information gets entered into the network by the malicious node and these nodes then directs the packets toward them or discards them [4-5]. In this paper suggested that the mechanism for black-hole detection and its elimination techniques.. The mechanism includes that if any of the intermediate nodes in the new route provide the response to RREQ message, then it is prepared to decrease the routing-delay, and it is also utilized by the malicious-node to affect the whole system.

2.3 DoS attack

In this type of attack, the malignant node not allows the other verified nodes to access the services or data of the network [6-8]. By the use of this attack, one particular node or the service may not get accessed and the resources of network such as bandwidth will get wasted. Additionally, the packet-delay and the traffic get increased in the network. This attack is targeted at the disturbing the routing information completely and the overall working of the ad-hoc network.

3. LITERATURE REVIEW

In this paper [9] present that the time used for sending through AODV is less as compare to the DSR protocol. And the generated throughput is also better by AODV as compare to the DSR Routing. The DSA routing uses the similar value two times and uses one value which is predictable or there may be leaking even some bits of P in individual signatures which is sufficient to destroy the DSA. In this the initialization process of RSA needs to select randomly the two very large primes. The high security level at the smaller size of key is the main benefit of this approach.

In this paper [10] few available solutions have been investigated for Black-hole or Gray-hole attacks that are found in MANET and suggested a novel technique to overcome these types of attacks which effectively identified both the Black-hole and Gray-hole nodes within the MANET and remove them from all the further communications that will be done to provide the network security efficiently. Instead of removing the entire path containing the malicious node, this work targeted on eliminating of only the attacker node.

Theoretical analysis represented that this technique would heavily raise the PDR and also works along with the issues of false positive [11]. With the dual verification approach the false positives are eliminated effectively. Also this approach is deal with single node failure issues by regularly monitor the energy levels of Back-bone node.

In this work [12] the simulation have been done to observe that if the percentage of the JF attackers is ten percent the throughput get reduces only up to the 0.03 percent. Whereas if there is raise in the percentage of the attackers up to twenty percentage then the throughput is reduced up to 7.58 percent that is higher than previous. The end-to-end delay also rises up to 3.38 percent for the ten percent of the attackers and the 10.76 percent for the twenty percent of the attackers. Therefore according to this suggested that the performance of the network is less affected up to the ten percent of the JF-attackers whereas the performance is worse for the twenty percent of the JF-attacker.

[13] This paper described an advance version of AODV routing-protocol for defense method against the Jellyfish-Delay-Variance attack which is found within the MANET. In this JF-delay-variance attack suggested the delay in transmitting the packets at the network-layer. Also it utilizes the MAC addresses to estimate the route for sending the packets towards the destination nodes. While forwarding the packets the attacker may produce delay, because of this end-to-end delay is increased and the network throughput gets reduced. Therefore this drastically decreases the overall network's performance. Also in this suggested an improved in AODV protocol to find out the malignant nodes within the network and to eliminate them from routing path without informing them.

[14] This paper is targeted on various effects of the jellyfish attack found over the routing protocols of MANET. In this some protocols are used like DSR, AODV, GRP and TORA. Some measures are calculated for the performance of network such as Data dropped due to buffer overflow or retry threshold gets exceeded, Media access delay, Load, or attempts for Retransmission.. DSR is having the poor performance than the other three types of protocols. To raise the density of node, apply the forwarding rate of the packets and use separate protocol, also introduced the JF-periodic-dropping attack to improve the performance.

[15] In this paper, suggested a new approach for protecting the network against the jellyfish-reordering-attack This suggested model utilizes the time-space-cryptography technique and the enhanced SHA-1 (mSHA-1) hash-function approach for authenticating that the packets got reorder or not while transmission. And the solution generated by this simulation

results is proved effective in raising the network's performance.

[16] This paper represents the performance analysis among the three types of reactive-routing protocols such as DSR, AODV and TORA that are used within the MANET under the JF-delay-variance attack having the increased density of node. This paper suggested that the use of DSR protocol is proved effective in MANET where the possibility of JF-attack is high and if the time efficient service of network is required for exchange of information along with the various nodes. And TORA is selected if high throughput is required along with the consistent service within network with high node density.

In this paper [17] the most recently found attack within the MANET have been suggested that is hard to detect which is called as Jellyfish periodic attack, since this type of attack follows all the TCP (Transmission Control Protocol) rules. To overcome this attack, a strong and effective approach needs to be developed. In this paper, by the use of a technique called as Genetic Algorithm, JF-periodic attack have been overcome and thus provides the security to the MANET.

In this paper [18], suggested an efficient solution for the making secure data-packets through adding the digital-signature which is dependent on the symmetric-cryptography approach developed by using the AES algorithm and the SHA2 hash function. According to this, a node without having the digital signature cannot perform any communication within the network. By this approach successfully obtained the non-repudiation, access control, prevents spoofing and unauthorized participation in routing.

4. PROPOSED METHOD

This section deals with the proposed work and it's functionality. This is as follows:

a. Start the network

b. Initialize all nodes

c. Send "Hello' Packets to all other nodes of the network.

d. Established Path between Source-Destination.

e. Establish Jelly-Fish, Blackhole and DoS Attackers in Network

```
for {set i 0} {$i < 4} {incr i} {
   set a($i) [new Agent/MessagePassing]
   $node($i) attach $a($i) $probing_port
   set w($i) [new Application/Jellyfish/Blackhole/DoS/ Dnh]
   $w($i) attach-agent $a($i)
   $w($i) addr-range 0 [expr $val(nn)- 2]
}
for {set i 5} {$i < $val(nn) - 1} {incr i} {
   set a($i) [new Agent/MessagePassing]
   $node($i) attach $a($i) $probing_port
   set w($i) [new Application/Jellyfish/ Blackhole/DoSDnh]
   $w($i) attach-agent $a($i)
   $w($i) addr-range 0 [expr $val(nn)- 2]
}
```

f. Jelly-Fish, Blackhole and DoS Attacker Node send data Packet in network for rushing

g. now starts infection

h. Place some Watcher Node to sense these special data packets.

i. Watcher nodes are fixed.

j. Identification: Watcher nodes identify the data Packet which are sent by Jelly-Fish Attacker, Blackhole and DoS Node By

If

- Some node is rushing data into network
- Rushing in regular interval then
- Sinking various packets
- Disobeying normal behavior of nodes

Then

Identify those nodes as Attacker nodes.

k. Prevention: Watcher Node sinks these rushing packets and make network clean. If detect these attacks then-

Control the data flow of those nodes by applying various parameters to control the behaviors of attacker nodes.

l. Keep working like these by watcher nodes till end of network.

m. Exit.

1. SIMULATION SETUP AND NETWORK SCENARIO

There are two part of this section. First is all about simulation while another part is all about various results. There are various tools available for simulation of the adhoc network.

We have implemented and tested the adhoc environment clock synchronization in NS-2.31. Different NS-2.31 initial parameters are as follows, which were taken in consideration while performing the experiments:

Table 1: Simulation Parameters

Property	**Values**
set val(chan)	Channel/WirelessChannel
set val(prop)	Propagation/TwoRayGround
set val(netif)	Phy/WirelessPhy
set val(mac)	Mac/802_11
set val(ifq)	Queue/DropTail/PriQueue
set val(ll)	LL
set val(ant)	Antenna/OmniAntenna
set val(ifqlen)	50
set val(nn)	50
set val(rp)	AODV
set val(x)	800
set val(y)	800
set val(stop)	50

There are three parameters on which we have proved our work. Those parameters are as follows:

1. Packet Delivery Ratio: This is the ratio of the number of data packets successfully delivered tothe destinations to those generated by sources.
2. *Throughput:* It is the rate of *successful* message delivery over a communication channel.
3. *Drop of Packets:*It is the number of packets droped during transmission.

6. RESULT ANALYSIS

Figure 1 shows a clear cut picture of the effectiveness of the proposed work on Packet Delivery Ratio.

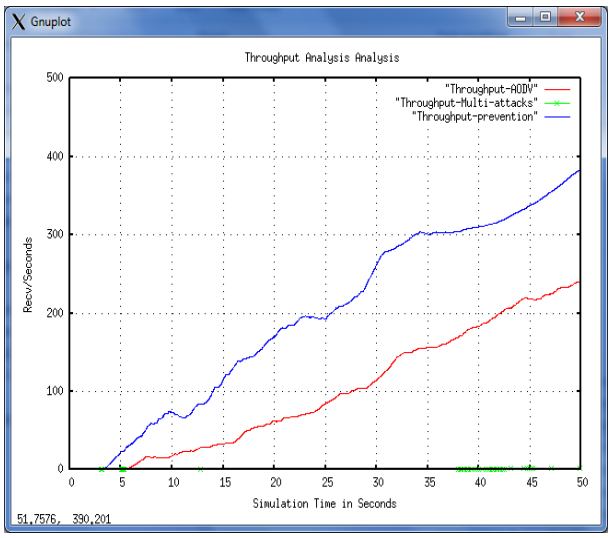

Figure 1: PDR Comparison

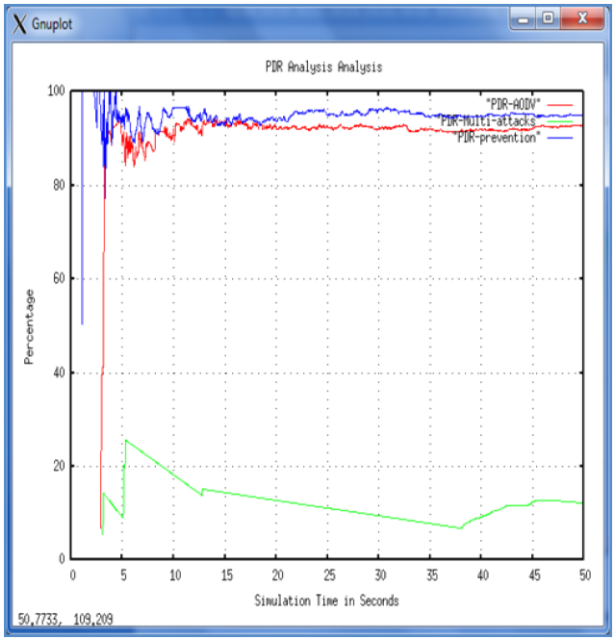

Figure 2: Throughput Comparison

Figure 3 shows a clear cut picture of the effectiveness of the proposed work on Packet Drop.

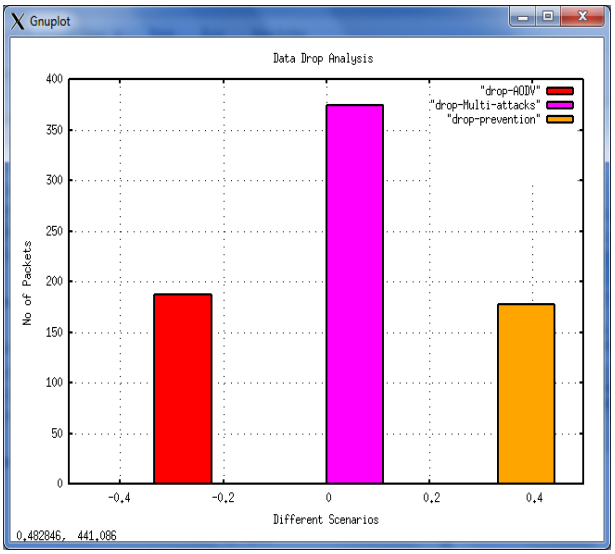

Figure 3: Packet Drop Comparison

7. CONCLUSION

In this paper, analysis has been done on the various security threats that MANET have suffered and also the suggested objective regarding the security have been obtained. On Since the MANET are more vulnerable for the various attacks so in this paper presented the some novel approaches from preventing the Jellyfish attacks that are found mostly in TCP based environment. In this paper various variants of the Jellyfish attacks have also been described along with the way how they are affecting the performance of the MANET. Some existing approaches in this regards have been suggested that provides the security objective to be achieved by applying those novel approaches against the Jellyfish-attack. In the future work for this paper includes the enhancing the performance of the MANET by introducing some efficient approaches that completely eliminates the arrival of these types of attacks.

We have shown through the experiment that the performance of the proposed work in respect to three of the parameters,

1.Packet Delivery Ratio

2.Throughput

3. Drop of Packets , is better than the performance of the base paper.

8. REFERENCES

[1] Robinpreet Kaur & Mritunjay Kumar Rai, Department of Electronics and Engineering, Lovely Professional University, Phagwara,Punjab, India "A Novel Review on Routing Protocols in MANETs" under Undergraduate Academic Research Journal (UARJ), ISSN : 2278 -1129, Volume-1, Issue-1, 2012

[2] Dhamande C.S and Deshmukh H.R, "A Competent to diminish the brunt of gay hole attack in MANET", Vol.2, Issue 2 Mar 2012.

[3] Q. Guan, F. Richard Yu, Shennimg Jing and Victor C.M Leung, "Joint Topology on Vehicular technology", Vol.61, No.6, Jul 2012.

[4] S.a.A.k.G, H.o.d.R.m, and S. sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69, 2013.

[5] A.MISHRA, R. Jaiswal, and S. Sharma, " A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network," presented at the 3rd International Conference on Advance Computing Conference (IACC), 2013

[6] Supriya and M. Khari, "Mobile Ad Hoc Netwoks Security Attacks and Secured Routing Protocols: A Survey," Advances in Computer Science and Information Technology, Networks and Communications Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84, pp. 119-124, 2012.

[7] J.Soryal and T. Saadawi, "IEEE 802.11 Denial of Service attack detection in MANET," Wireless Telecommunications Symposium (WTS), 2012.

[8] R.H.Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012

[9] K.Sangeetha, "Secure Data Transmission in MANETS Using Eliptic Curve Cryptography", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014, pp:2557-2562.

[10] Swati Pokhariyal, Pradeep Kumar, "A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets", IJCSMC, Vol. 3, Issue. 12, December 2014, pg.217 – 223

[11] Harsh et al, "Cooperative Blackhole/ Grayhole Attack Prevention in Mobile Ad hoc Network: A Review", International Journal of Computer Applications, Vol 64, Feb, 2013, pp. 16-22

[12] Mohammad Wazid, Roshan Singh Sachan, R H Goudar, "Measuring the Impact of JellyFish Attack on the Performance of Mobile Ad Hoc Networks using AODV Protocol", Proc. Int. Conf. on Computational Intelligence and Information Technology, CIIT, 2012.

[13] Garg, S., & Chand, S. (2014, September), "Enhanced AODV protocol for defense against JellyFish Attack on MANETs", In Advances in Computing, Communications and Informatics ICACCI, 2014 International Conference on (pp. 2279-2284). IEEE.

[14] Kaur, A., & Wadhwa, D. S. (2013). Effects of jelly fish attack on mobile ad-hoc network's routing protocols. IJERA, 2248 (9622), 1694-1700.

[15] Patel, H. P., & Chaudhari, M. B. (2013, July), "A time space cryptography hashing solution for prevention Jellyfish Reordering attack in wireless ad hoc networks", In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[16] Mohammad Wazid, Vipin Kumar, RH Goudar, "Comparative performance analysis of routing protocols in mobile ad-hoc network under Jelly fish attack", 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.

[17] Manjot Kaur, Malti Sarangal, Anand Nayyar , "Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks", International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014

[18] S.S.Zalte, Prof.(Dr.)Vijay R.Ghorpade, "Secure Token for Secure Routing of Packet in MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 6916-6919