International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

Performance Evaluation of MANET Routing Protocols under Pulse Jammer Attack

T. T. Manikandan, Rajeev Sukumaran, M. R. Christhuraj, M. Saravanan

Abstract*: Mobile Ad Hoc network is comprised of large number of multi-hop movable sensor nodes. Nodes in the MANET usually communicates with the other nodes that co exists with them without any central administration. Since the Mobile Ad Hoc network has the natural ability to change the existing topologies in a rapid fashion, routing protocol plays a pivotal role in communication among nodes in the network. But in reality, nodes in the network are often vulnerable to various security attacks. Pulse Jammer Attacks is one such attack which restricts the nodes from communicating with its neighborhood nodes in a reliable fashion, so that it becomes responsibility of the routing protocol to deal with these types of attacks. This paper deals with the Pulse Jammer Attacks (PJA) and its consequences on proactive and reactive routing protocols such as Ad Hoc On Demand Distance Vector (AODV), Geographical Routing Protocol (GRP) and Optimized Link State Routing Protocol (OLSR).The simulation of the above mentioned protocols is done by taking into consideration various node characteristics under different scenarios using OPNET simulator. Then the detailed performance analysis is done by comparing the outcome of different scenarios and with the help of this analysis results network designers can be able to decide on the better performing routing protocols for MANET under PJA which may result in designing the network which withstand PJA.

***Index Terms*: AODV, GPR, MANET, OLSR, OPNET, PJA.**

I. INTRODUCTION

The Wireless network has emerged a lot according to the increasing demand of the end users. The attention of most of the researchers has been shifted from other network technologies to wireless network. Even though wireless network has its own constraints in the form of bandwidth restriction, limitation of power [1] and high error rate these constraints don't restrict the growth of wireless network. MANET is one such most wanted field among the researchers in the area of wireless networks. MANET encompasses mobile devices which might be usually known as nodes, and each one of them is equipped along with a radio transmitter and a receiver. MANET is a transient network of wireless mobile nodes where the network infrastructure is dynamic in nature. Each mobile node communicates with the mobile node which comes under its transmission and resumption range. In case if two nodes are not within the communication range, another node which is intermediate between these two nodes receives the message
from the source node and forwards it to the destination node. One of the challenging areas of research in wireless technology is routing techniques, and MANET routing also is not an exception and it has its own challenges and constraints. Hence MANET routing technology is focused in this paper.As said earlier, MANET does not have any fixed infrastructure [2], and it is usually termed as infrastructure less network. Nodes in the MANET have the flexibility to play the role of transmitter, receiver and router. Since MANET has the dynamic topology monitoring, the way in which the mobile nodes work in the network seems to be very difficult, and an authority to control the way nodes and to react during sending, receiving and forwarding of packets in the network is required. The function is done by routing protocols and those protocols are often vulnerable to various security attacks.Jammer attack is one of the popular attacks where the main motive of the attack is to restrict the transmissions completely on the wireless network. Jammer attack is done on the physical layer of the wireless medium where the packet is generated at high rate which makes the medium busy which in turn restricts the other nodes in the network from the usage of medium for transmission. In this paper, three different MANET routing protocols namely,OLSR, GPR and AODV have been implemented under different usage applications(FTP,EMAIL and DATABASE) different level of loads(High, Medium and Low) and the results have been collected. Then the same scenarios are tested under PJA and the results are correlated.The implementation and analysis have been done using OPNET Modeler 14.5.It supports various MANET routing protocol models, and also provides integration support for IP and wireless LAN.Apart from this OPNET is possible to be used for the rapid development of new MANET protocol models.The rest of the paper is organized as, Section 2 provides the detailed literature review of existing routing protocols. In Section 3, some of the security services which are necessary for MANET are discussed. In Section 4, Jammer attack and its impact on routing has been discussed. In Section 5, simulation environment, scenarios for analysis and the details on the configuration of nodes for simulation are presented. Section 6, provides the results and analysis of the experiments. Section 7, concludes the results.

Manuscript published on 30 March 2019.
***Correspondence Author(s)
T.T.Manikandan, Centre for Applied Research in Education, SRM Institute of Science and Technology, Kattankulathur (Chennai), India.
M.R.Christhuraj, Centre for Applied Research in Education, SRM Institute of Science and Technology, Kattankulathur (Chennai), India.
M.Saravanan, Centre for Applied Research in Education, SRM Institute of Science and Technology, Kattankulathur (Chennai), India.

II. LITERATURE REVIEW

The detailed research on literature has been carried out to identify the gap between the current needs in the field of routing technology in MANET and the existing proposals. Most of the researches have been concentrated only on the performance analysis of different routing protocols of MANET under different application loads. But in this research paper evaluation of performance of routing protocols with respect to security attacks is analyzed which makes this paper unique.The Ad-hoc On Demand Distance Vector Routing (AODV) the most popular adhoc routing algorithm are delt by [3][4]. AODV provides flexibility with respect to network configuration due to which it becomes one suitable choice for the networks like Ad Hoc networks which is dynamic and self-administrative in nature. It is shown that AODV has the capability to scale to very vast range of network nodes to create an ad hoc network. Apart from that, the proposed algorithms have been evaluated by the author using the simulated resultsThe routing framework which is adaptive in nature is analyzed. With the help of the analyzed framework the new adaptive routing protocols [5] have been implemented which gives the flexibility to nodes in the network to change their modes of operation with ease. During the process of mode changeover, the routing states are maintained. The whole scenario is simulated to demonstrate the correctness of the proposed algorithms at the time of mode changeover. It has been evaluated that the new algorithm shows that the protocol with the capacity to match the performance of either proactive or reactive routing algorithms.The energy usage and its impact in ad hoc networks routing protocols [6] has been taken in to the consideration. The detailed comparison of Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) have been presented. The average energy consumption of the network and routing energy consumption are the two factors considered for comparing of DSR and AODV.The in depth performance analysis of various adhoc routing protocols [7] such as AODV,ZRP,DSR.OLSR and TORA are performed and the results have been evaluated using the performance metrics packet delivery ratio and end-to-end delay. Based on the analysis the experiment suggests that TORA and AODV have great reliability in high dense network when compared with the OLSR.The packet delivery ratio in AODV and TORA are superior when compared with OLSR.

III. SECURITY SERVICES IN MANET

MANET has dynamic portable nodes which poses unique security threats when compared with the other kind of networks. Wireless networks are more vulnerable to eavesdropping attack. In the case of MANET, the main motive is to provide the security features such as authentication, confidentiality, integrity, and non-repudiation which enable reliable communication among the nodes.

A. Authentication

Authentication is must in wireless networks to avoid malicious nodes entering the network and initiating the security attack in the network. Authentication will evaluate the authenticity of the information transferred before sending it to another node in the network. This will avoid the data duplication which in turn ensures the information transferred to the source is received by the node in the destination in the same way as it is being sent.

B. Confidentiality

In MANET, the information which has been sent by the node to another node in the network to be accessible only by the designated node. In case if the confidentiality is not there is a huge possibility of adversary node acting as the authenticated node and spoofing the information sent to some other node in the wireless network, which subsequently leads to the unauthenticated node getting the access to the network and doing malicious activities. In order to avoid this data transmitted over the wireless medium it is to be encrypted before transmission.

C. Integrity

Integrity plays a vital role in ensuring that the message transmitted in the wireless network is never corrupted by some malicious attacks. The main motive of these attacks is to duplicate the message sent and can even redirect the network traffic route to some other node in the network instead of the actual designated node.

D. Availability

Availability is the most important security service that is needed for MANET.Avalilability is the way of ensuring guaranteed service irrespective of the presence of malicious nodes in the network. Denial of service attack can be made on any layer of the MANET.The malicious nodes has the capability to block the transmission on physical layer and can even disturb the routing mechanism and reduces the resources in the network. Hence to cop up with the above challenges it is to ensure the availability.

E. Non Repudiation

It is the process which ensures no message has been sent or received over the wireless medium which does not deny by the receiver.Non Repudiation is ensured by using the technique of digital signatures. Digital signature is the cryptographic technique which provides unique identity to each and every message that is passed over the network from one node to another and ensures non repudiation.

IV. PULSE JAMMER ATTACK

Many attacks with different intentions are made at various layers of the MANET.One of the most impactful attack among all those attacks is jammer attack [8]. Jammer attack [9] [10] [11] is launched on the physical layer of the network, when the attack is made, it results in physical layer generating packets at very high rate on the wireless medium constantly, which in turn keeps the medium busy.

Subsequently this restricts the nodes in the network from accessing the network medium because of the unwanted high traffic generated by the jammer attack.

In Jammer attack, one of the malicious node in the network uses the device named jammer. This device continuously monitors the radio frequencies in the network.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The process of monitoring is done until the intruder or attacker find the matching frequency to the frequency which is received from one of the nodes present in the network which intern is the point of interest for launching the jammer attack.

Once the intruder finds the radio frequency of the target network using jammer, then it sends continuous radio frequencies of high range to the target frequency, which is within the transmission range of the target network. Since the range of frequencies sent is huge, it generates lot of unwanted noise in the network which leads to loss of packets which are actually transmitted by the authenticated nodes present in the network. Jammer attack is a king of brute force attack to wipe out transmission among nodes in the network.

There are different kinds of jammers available but some of the most popular jammers are constant jammer, random jammer, reactive jammer and deceptive jammer. In this paper, pulse jammer attack has been implemented. The jammer is called as pulse jammer because, pulse ON and pulse OFF are the two most important parameters that defines the behavior of the jammer Apart from this the transmission power of the jammer node is much lower than that of the normal nodes present in the network. This subsequently reduces the throughput of the network.

In this study the pulse jammer attack is created using the OPNET simulation tool, and it is applied on Ad Hoc on Demand Distance Vector, Geographical Routing Protocol and Optimized Link State Routing. All the above mentioned protocols have been implemented in two steps. In the first step, each algorithm is implemented under normal traffic generated by the set of applications such as FTP, Email and Databases. Similarly in the second step the same algorithm is implemented by imposing pulse jammer attack into it. Here the application and profile are configured by setting certain parameters to generate application traffic. In the following session, the detailed information on simulation environment and different network scenarios used for implementation are presented.

V. SIMULATION ENVIRONMENT

The simulation tool required to be used to carry out the experiments is OPNET Modeler 14.5. OPNET provides the rich environment for simulation and modeling of network. It provides flexibility for the user in order to modify the network components using its programming library. Since the OPNET supports all the phases of the research such as model design, data collection, simulation and analysis the OPNET stands out among all the other network simulators.

A. Architecture of OPNET

The architecture of the OPNET is simple. Support for modeling and evaluation of communication and distribution of systems is one of the most exciting features provided by OPNET.The OPNET tool has number of suits where each suit concentrates on one of the features needed for modeling. There are three phases in general, which has inter relation as shown in the simulation flow, in the Figure 1.

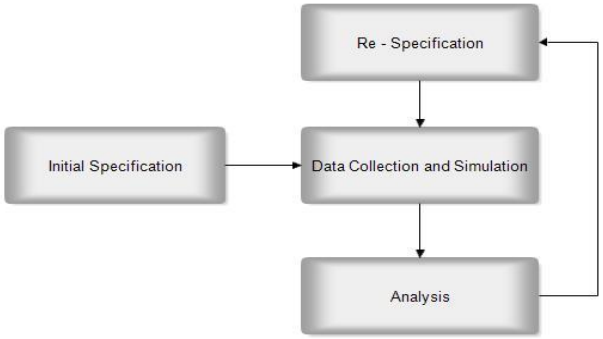

Fig 1. Architecture of OPNET

B. Configuration of Simulation Environment

A campus network scenario 1000x1000 is created for the purpose of simulation. 24 MANET nodes are deployed on OPNET Modeler simulator. The IEEE 802.11 network standard has been followed for MANET nodes. The simulation run time for each scenario is set as 10 minutes with the seed value of 128 and simulation kernel is set as optimized mode. The number of network scenario are three, each network scenario is implemented with different routing protocol. Scenario 1 implements pulse jammer attack on Optimized Link State Routing protocol (OLSR), Scenario 2 implements pulse jammer attack on Geographical Routing Protocol (GRP), scenario 3 implements intelligent jammer attack on Ad-Hoc On Demand Distance Vector (AODV).These scenarios are compared with the network scenario where the jammer is not involved and only the respective algorithms are being run under the traffic generated by three different applications namely FTP, Email and Database.

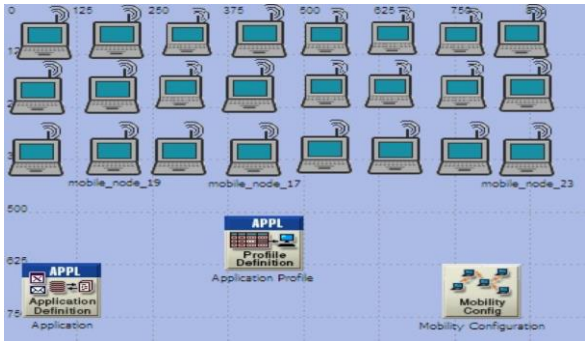

Fig 2. MANET Network Scenario without Jammer

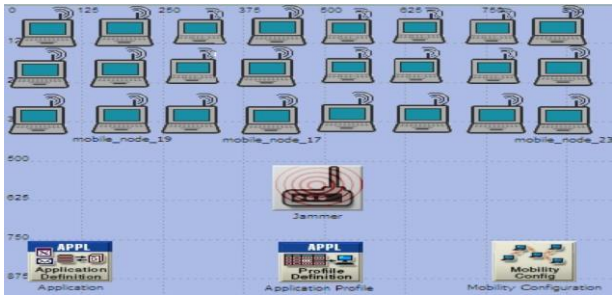

Fig 3. MANET Network Scenario with Jammer

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The scenarios created for the simulation in OPNET Modeler is shown in Figures 2 and Figure 3.

C. Application Configuration Setting

For running any nodes in the OPNET there is to be an application which acts as a source for the generation of traffic. Application configuration in OPNET is the way of defining the nature of traffic that the particular application should generate in order to carry out the simulation.

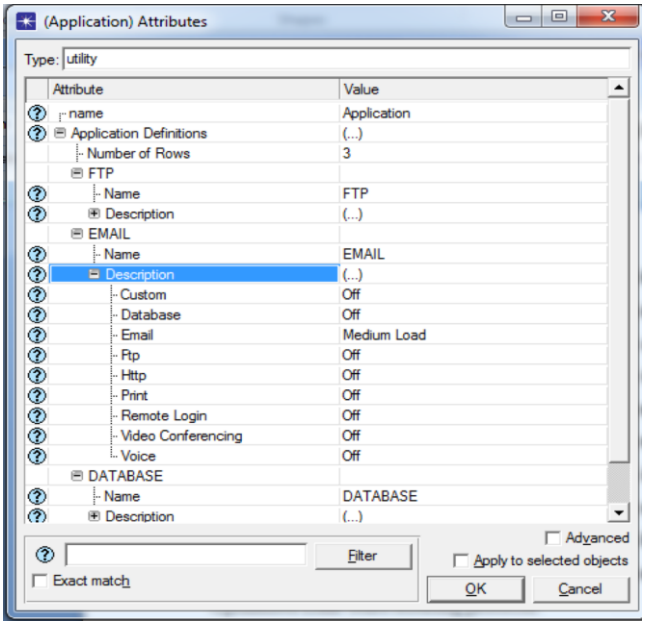

Fig 4. Application Configuration Setting

In this scenario FTP, Email and Database have been chosen as the application to generate the network traffic that is needed to carry out the simulation.The Figures 4 and 5 shows the application configuration and profile configuration setting required for the simulation.

D. Mobility Configuration Setting

The Mobility setting enables the MANET nodes in the network to move in the random direction which results in the break of link between the nodes, and the new link is established after finding the new routing table. The default values of speed, start time, stop time and pause time are changed as follows for the purpose of simulation. Figure 6 shows the Mobility configuration setting.

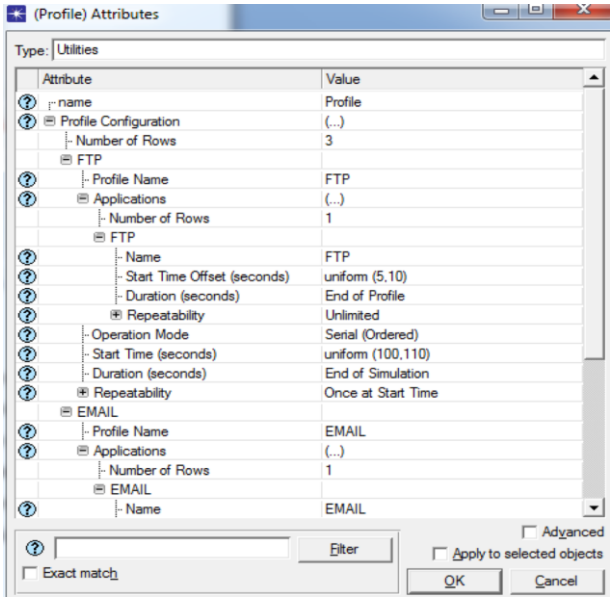

Fig 5. Profile Configuration Setting

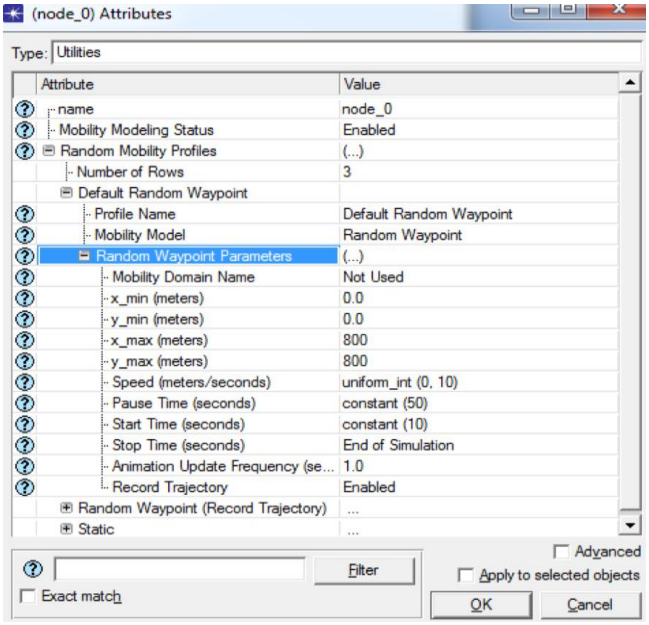

Fig 6. Mobility Configuration Setting

E. Node Configuration Setting

Every node in the MANET plays the role of router as well as the host to do the forwarding of packets among the nodes in the network.The way of forwarding is called as trajectory and it is defined as vector in this case. Apart from this, the traffic related parameters such as Start time, packet inter arrival time, RTS threshold and buffer size are changed from the default values for the purpose of simulation as shown in Figure 7

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

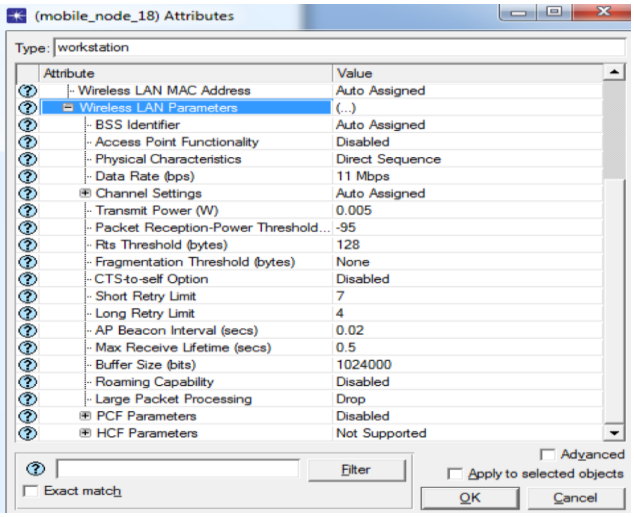

Fig 7. Node Configuration Setting

F. Creating Pulse Jammer Node

Pulse Jammer is different from MANET node. The structure of the pulse jammer node itself is completely different from the structure of the normal MANET node structure. Jammer node has the radio transmitter which is responsible for the generation of noise in the network medium which in turn halts the transmission in the network. There are three types of jammer nodes such as fixed jammer, mobile jammer and satellite jammer. For the purpose of simulating the pulse jammer attack on the network scenario the default values of band frequency of the jammer node, transmitter power of jammer, pulse off time and pulse on time of the jammer node are created and modified.

VI. RESULTS AND DISCUSSION

A. Performance of OLSR under Jammer Attack

The network scenario has been created in the size of 1000x1000.Initially OLSR protocol has been implemented on the 24 nodes, with the default protocol setting on OPNET tool. In order to generate the traffic for OLSR protocol, the application configuration, profile configuration and mobility configuration have been defined appropriately as discussed in section 5. The simulation run is executed to record the performance result of the OLSR protocol.

The previous scenario is then modified by including the pulse jammer in to the existing scenario, now the jammer generates the traffic as per the pulse setting. Now the performance of the OLSR routing is once again recorded. The performance of the two different scenarios of OLSR with and without jammer attacks are evaluated based on throughput, delay and network load.

From the results obtained through the simulation, it is evident that the jammer decreases the throughput of the whole network by the generation of unwanted noise traffic in the network transmission medium. Throughput observed without any jammer in the network is 1.4 Megabits whenever the jammer is taken into the consideration and the throughput significantly reduced to 1.2 Megabites.From this, it is clear that the jammer attack degrades the overall network performance.

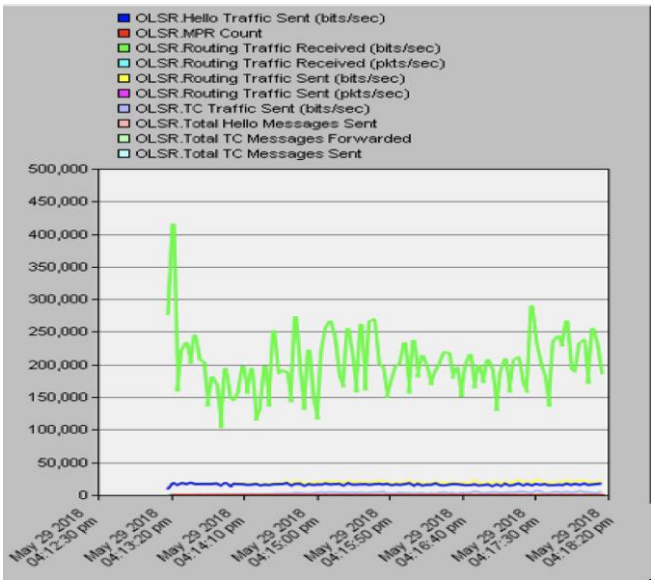

Fig 8. Normal Behavior of OLSR protocol

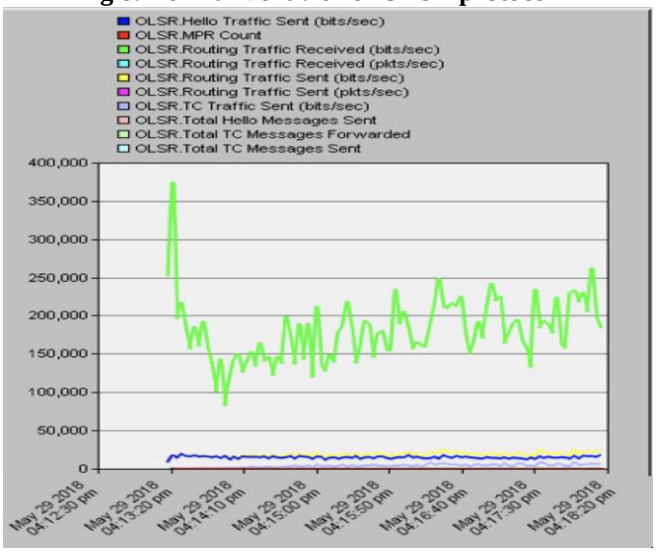

Fig 9. Behavior of OLSR under Jammer Attack

Apart from the throughput, network load is also having an impact because of jammer attack. Without the involvement of jammer, the network load is 1.3 Megabites whereas with jammer it is reduced to 1.0 Megabites.The performance comparison of OLSR with and without jammer attack is shown in the Figure 8 and 9 respectively.

B. Performance of GRP under Jammer Attack

This scenario is implemented in two stages. During first stage the nodes in the network scenario created is configured with the Graphical Routing Protocol where the default parameters of the protocol is kept as it is for the simulation. To generate the traffic for the analysis FTP, Email and Database applications are considered with application configuration and profile configurations which are defined to decide the way of behavior of the application in the scenario created for simulation. The simulation run is carried out in order to record the results.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

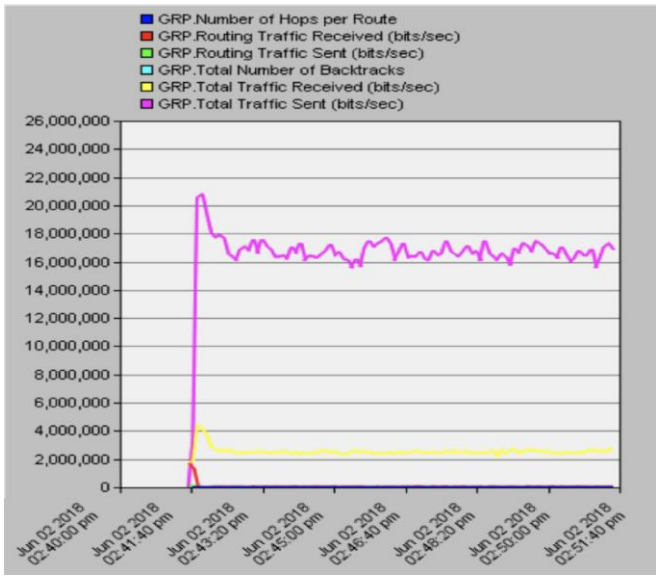

Fig 10. Normal Behavior of GRP protocol

Similarly in second stage the same scenario is modified by including the Pulse jammer and the simulation run is carried out once again. When compared with the characteristics such as throughput, network load and delay. Throughput of the network under GRP protocol is significantly affected by the Jammer attack. When the throughput is compared, it is 3.5 megabits without the presence of jammer and it reduces to 1 megabit with the presence of jammer.

Similarly, Network load and the Delay of the network is increased after introducing the pulse jammer which indirectly means that the reliability of the network is affected by the noise generated by the jammer node. The Performance evaluation of GRP is presented using the throughput, network load and delay graphs.

The performance analysis of GRP with and without jammer attack is shown in Figure 10 and 11 respectively.

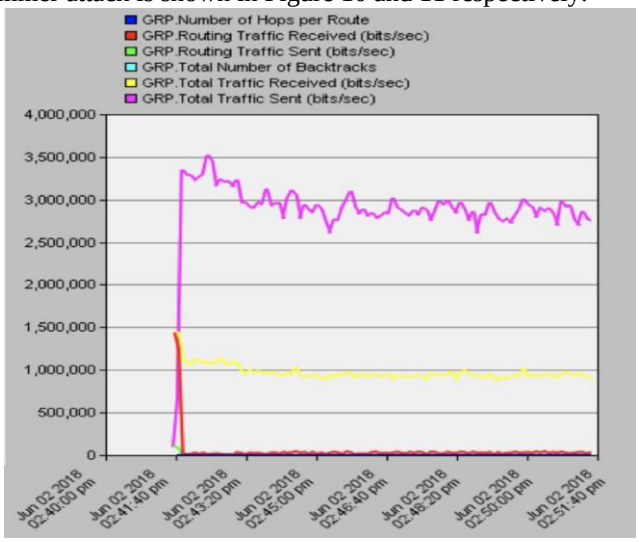

Fig 11. Behavior of GRP under Jammer Attack

C. Performance of AODV under Jammer Attack

In the first stage of simulation the nodes in this scenario are configured with the AODV protocol and the traffic is generated by appropriately setting the parameters of the application configuration, profile configuration and mobility configuration. The Simulation run is carried out and the results are recorder.

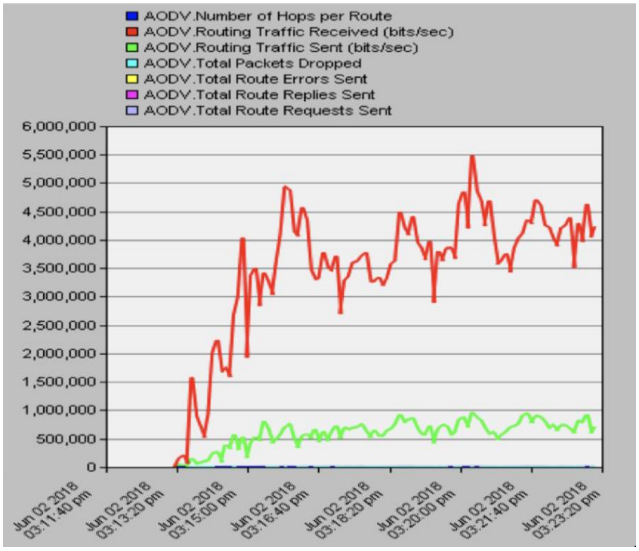

Fig 12. Normal Behavior of AODV protocol

In the second stage of simulation, the jammer attack is introduced into the network simulation environment and the simulation run is carried out once again. Then the results of both the stages of simulation are compared by using the characters such as throughput, network load and delay of the network. Here the network throughput without the involvement of the pulse jammer is compared with the throughput of the network once the jammer is introduced into the network simulation environment. When the throughput is compared, it is clearly differentiable that when jammer is introduced, the congestion occurs in the network which subsequently degrades the overall performance of the network.

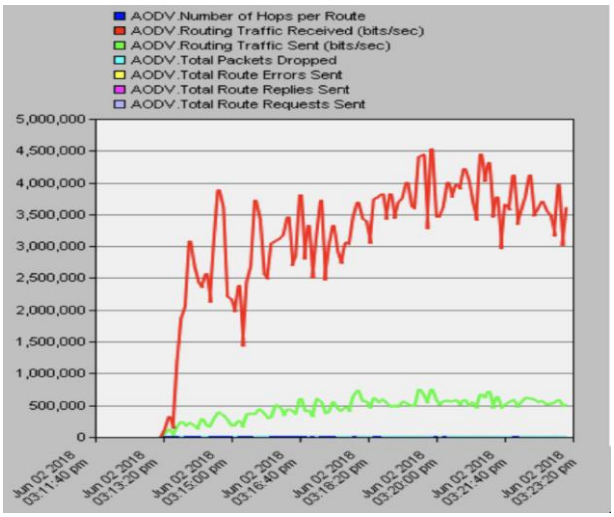

Fig 13. Behavior of AODV under Jammer Attack

The overall performance of the network with and without the presence of the pulse jammer is compared and it is shown in Figure 12 and 13 respectively. In the presence of Jammer attack it leads to significant reduction in the available bandwidth of the network. Reduction in bandwidth has an impact on the reliability and availability factor of the network and subsequently makes the network vulnerable to the network. From the analysis of performance it is clearly seen that the delay of the network starts increasing after the introduction of pulse jammer into account. This is because of the fact that when the jammer is involved in the network, it starts generating the unwanted noise through the wireless medium of the network. This in turn restricts the transmission on the network.

VII. CONCLUSION

In this analysis the performance of three routing algorithms namely OLSR, GRP and AODV which is being set over the MANET using different kind of application traffic are investigated. For evaluating the performance of the routing algorithms with the presence of pulse jammer attack, initially simulation is done without jammer. Subsequently jammer is introduced for conducting simulation once again. For evaluating the effectiveness of the routing protocol in the presence of jammer attack throughput, network delay load and delay are considered as evaluation metric.

From the simulated results, it is found that no routing algorithm among OLSR, GRP and AODV stands as the best protocol in all aspects. OLSR has the worst performance result when compared to the other two routing techniques with respect to the throughput, network delay and network load. From the analyses done using the OPNET simulator it is concluded that protocols OLSR and GRP are more vulnerable to jammer attack and AODV is the best performer under pulse jammer attack. So it is suggested that if the network designers use AODV routing protocol for MANET the overall performance of the network against pulse jammer attack will be better when compared to other routing protocols.In future there is a possibility of extending this research to other security attacks such as black hole attack and wormhole attack.

REFERENCES

1. Sarkar SK, Basavaraju TG, Puttamadappa C., “Ad hoc mobile wireless networks: Principles, protocols and applications”, 2nd ed.,FL, USA: CRC Press, Inc. Boca Raton, 2013.
2. Ramanathan R, Redi J., “A brief overview of ad hoc networks: Challenges and direction”, IEEE Communications Magazine 2002, pp.20-22.
3. Pirzada AA, McDonald C., “Secure routing with the AODV protocol”,In Communications, Asia- Pacific Conference;5 October 2005; Perth, WA, Australia:IEEE. pp. 57-61.
4. Royer EM,Perkins CE.,“An implementation study of the AODV RoutingProtocol”,Proc.WCNC,2000,IEEE,vol.3,pp.1003-1008.
5. Larry L, Davie Davie, “Computer networks - A system approach”,5th ed. Burlington, Massachusetts, United States: Morgan Kaufmann Publishers, 2003.
6. Barati M,Atefi K,Khosravi F, “Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET”, International Conference on Computer and Information Science (ICCIS), June 2012; Kuala Lumpur, Malaysia, pp. 636-642.
7. Wu B., Chen J., Wu J., Cardei M.A, “Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless Network Security, Signals and Communication Technology Springer 2006, 2:103-135.
8. Jagat Singh, Sachin Gupta, “Impact of Jamming Attack in Performance of Mobile Ad hoc Networks” , International Journal of Computer Science Trends and Technology (IJCST) – Volume 5, Issue 3, May – Jun 2017, pp.184-190.
9. Sari A.,“Security Approaches in IEEE 802.11 MANET - Performance Evaluation of USM and RAS”,International Journal of Communications, Network and System Sciences, September 2014,7(09),pp.365-372.
10. Grover K, Lim A, Yang Q., “Jamming and anti-jamming techniques in wireless networks: A survey”, International Journal of Ad Hoc and Ubiquitous Computing,2014,17(4),pp:197-215.
11. Baljinder Singh, Dinesh Kumar, “Jamming attack in MANET: A Selected Review”, International Journal of Advanced Research in Computer Science and Software Engineering, April 2015,5(4), pp. 1264-1267.

AUTHORS PROFILE

Manikandan received a B.Tech in Computer Science and Engineering from SASTRA University, Thanjavur, Tamilnadu, India and ME in Computer Science and Engineering from College of Engineering, Anna University, Chennai, Tamilnadu, India. Currently he is working in Centre for Applied Research in Education, SRMIST, Chennai.

Rajeev Sukumaran is an Engineering Epistemologist and a Learning Researcher. He received his Ph.D in Computer Engineering and is an active researcher in Modeling Wireless Communication Networks and is with the Teaching Learning Centre, Indian Institute of Technology Madras, Chennai, India.

Christhu Raj is an active researcher in constructing Stochastic Network Calculus Models for Underwater Wireless Communication Networks. He received his Ph.D in Computer Science and Engineering and is an active researcher. Currently he is working in SRM Centre for Applied Research in Education, SRMIST,Chennai.

Saravanan received a BE in Computer Science and Engineering from Maharaja Engineering College (Anna University), Avinashi, Tamilnadu, India and M.E in Computer Science and Engineering from National Engineering College (Anna University), Kovilpatti, Tamilnadu, India. Currently he is working in Centre for Applied Research in Education, SRMIST, Chennai.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)