Performance Comparison of DSR and DSSR Protocols With and Without False Data Injection Attack Based on Two Fish Algorithm using Manet

Rajat, Naveen Hemrajani

Abstract: ***The arrangement of remote applications or conventions with regards to Mobile Ad-hoc Networks (MANETs) frequently requires a venture through a recreation stage. For the consequences of the re-enactment to be significant, it is very much essential to have a model which is based on test system that coordinates as intently as conceivable the truth. However, the distributed service provisioning over MANETs need sufficient assistance for the discovery of service and also invocation. Numerous existing protocols for service discovery have been proposed to be efficient for the wireless environment, and are found to be focused mainly on infrastructure-based 1-hop ad hoc wireless networks. This proposed method demonstrates the performance comparison of DSR and DSSR protocol that has been dissected and identified and their simulation results are obtained based on the two fish algorithm using MANET. It is a decentralised network with most encouraging and quickly developing innovation which is the self-sorted out and also it is quickly conveyed system.***

Index Terms: DSR, DSSR, MANET, Attack

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has been projected as one amongst the most pervasive areas of research in the on-going years due to certain difficulties it postures to various related protocols. MANET is the new developing innovation which empowers users to convey with no physical framework regardless of their geographical area that is the reason which in some cases it is suggest as infrastructure less network [11]. The multiplication of less expensive, little furthermore, increasingly ground-breaking gadgets make MANET quickest developing network. A significant problem in MANET is the availability of resources. Giving secure communication in such evolving condition just as assurance against explicit dangers and assaults prompts to advancement of different security plans and structures. Resource availability is one of MANET's major challenges. Rendering a secure communication in such a variable environment, and providing protection against particular threats and attacks, results to the development of different types of security schemes and architectures.

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this is communicating with rest of the world while being mobile. The disadvantage is their limited bandwidth is memory processing capabilities and open medium are the issues that are faced in accordance with various parametric metrics [12].

The idea of a MANET such as open medium, dynamic network topology, absence of centralized monitoring, and absence of clear defence mechanisms makes it very difficult issue to several routing attacks. In MANET routing, there exists a high possibility for intermediate nodes to be dangerous that it might be a serious risk in losing the security. Black hole is the very common attack in ad hoc routing in which the malevolent node that are used in the process of routing to state itself of being the shortest path all the way to the sink node [13]. After receiving the data packet from the node it will drop the data packet instead of forwarding them to the neighbouring node the black hole attacker does not obey the communication model. Transmission of data is introduced in between the nodes utilizing UDP agent and CBR traffic. Transmitter sends the data through an attacker. Source node passes the data to the attacker that will not have a shorter path to sink [14]. Attacker does not forward data to its neighbours. These protocols are parameterized ones and were developed to meet the demands of the Advanced Encryption Standard (AES) competition and were chosen among the top five finalists. This protocol has in their structure, a variable block size and a variable key size and is capable of encrypting four w-bits simultaneously. Symmetric key encryption is regular to guarantee information classification, it utilizes same key for both encryption and decryption then unscrambles the figure content. A mixture of aspects namely, performance, security, ease of implementation, efficiency and flexibility contributed to the algorithm selection as the AES. Two fish were intended to meet the necessities of the Advanced Encryption Standard (AES) two fish used as a 16-round Feistel-like structure with extra brightening of input and the output. The important non-Feistel constituents are the 1-bit pivots. The revolutions can be moved into the F functions to develop the Feistel structure, yet the rotation takes place in the F function to create a very pure Fiestel structure.. The plaintext is part into four 32-bit words, these are XORed with four catchphrases in info brightening step. This is pursued by sixteen rounds. In each round, the two words on the left are utilized as contribution to the capacities. (One of them is turned by 8 bits first.) This work contains four byte-wide key dependent S-boxes, trailed by a direct blending venture dependent on a MDS network. The consequences of both the g capacities are combined using a Pseudo-Hadamard Transform (PHT) and by incorporating two catchphrases. Then these two outcomes are XORed to form words on the right (among the two, one is pivoted to the left by 1 bit first and the second one is pivoted right after a short interval).

Revised Manuscript Received on June 05, 2019
Rajat, CSE, JECRC University, Jaipur, India.
Dr. Naveen Hemrajani, CSE, JECRC University, Jaipur, India.

Then the parts of right and left are exchanged for the following round with the exclusion of the final round and all the four words are XORed with four key words to deliver the figure content.

II. RELATED WORKS

Kavitha et al. (2019) [1] proposed during the time period of DS construction that had been used in accordance with a selection of nodes having more energy, minimum residual energy with less degree than its coefficient for a maximum effective degree. The results had shown that this CDS-SDS QoS had a higher jitter for having a high count of nodes and good efficiency when compared to QoSAOMDV and AOMDV. In this point of view, the QoS could have been established by including the energy constraint combined with timestamp as well as the link of a life time.

Verma et al. (2012) [11] experimented in resource perspective according to the proposed algorithm concluded that will gain extra memory while comparing with other state-of-the-art algorithms While considering CPU utilisation was same for all the other algorithms. So the proposed algorithm was simpler and faster when were compared to other experimental algorithms.

Muchtar et al. (2018) [3] demonstrated in this new suggestion four strategies were proposed to overcome the energy efficiency problems in the previous research content. It greatly reduces the routing and flooding traffic activities that were used in bio-inspired approach to create content more adaptive and efficient routing that had a better use of data structure.

Canning et al. (2012) [10] proposed the verification that were taking place in DSR components structure was required through assurance in other samples for enabling its generalisation to wider populations. Moreover, the recruited PMS sufferers for this research were diagnosed by using 30% increase in criterion. Energy efficiency, PDR, and also other parameters were analysed and were then compared with other State of art algorithms and their methods were reported.

Goulden et al. (2018) [6] proposed the detailed sequence concerning the limitations of the user visions, and the capability of industry to approach beyond the limit towards a more distinguished view. They concluded it by broadening the landscape carried out by delivering DSR, in order to foster an extensive diversity of roles of the end user, and finally getting higher demand response from a broader user base.

Kang et al. (2018) [5] proposed to allow ORGMA to attain high PDR in dynamically changing MANET environments. Reliable multi-hop packet delivery in MANETs becomes efficient. ORGMA performs better than the state-of-the-art routing protocol to a great extent, and also its performance reaches close to the performance of an ideal routing method with global data.

Kumari et al. (2018) [4] proposed algorithm further enhanced the system and made the system work smartly and in an energy efficient manner. There were antennas involved in terms of performance and evaluation**.**

Muchtar et al. (2018) [3] experimented the process to have a good energy efficient one must totally avoid retransmission in order to have a better energy efficient. There was a critical view assumption in an energy consumption study with MANET.

Omran et al. (2017) [7] demonstrated the control power flow to alleviate and gets overloaded due to high power transfer compared and used to demonstrate the effectiveness of DSR control in load growth handling. Only the impedances which were unbalanced were addressed, but the impacts of impedance unbalance were presented to be important on the resulting DSR design.

Saraswat et al. (2015) [9] proposed presented the results of the simulation for the purpose of choosing the efficient routing algorithm to provide an effective performance when implemented over the target mobile grid application.

Shabut et al. (2018) [2] proposed model, the performance of the network was evaluated using average throughput in the network, packet loss and energy consumption in the presence of nodes that are dishonest/malicious. It also increases the network's overall performance.

Upadhyay et al. (2016) [8] experimented provisions for security mechanism in routing were essential in WSN. Proposed solutions had a long network life because of the malicious nodes and also the shutdown takes place for further research in battery chargers and also in case of other networks.

III. COMPARATIVE STUDY

The comparative study of both the existing and proposed methodology has been analysed in both the DSR and DSSR protocol based on two fish algorithm using MANET. Generally, MANET neither have any fixed centralized administration control nor fixed infrastructure, and it contains mobile nodes that are dynamically connected. Because of its varying topologies in MANET, the routing process of selecting the optimum path in a network and administering the network traffic is critical Sensor nodes are developed from Wireless sensor organize and are operating under the control of central authority Base station are fit for showing fascinating applications because of their capacity to be conveyed universally in antagonistic and inescapable conditions. In any case, because of same reason security is turning into a noteworthy worry for these systems. Predominantly disturbing attack is the Wormhole attack- it is actually a Denial of Service attack, in which were hackers will establish a low-latency link in the network between two points. On account of the survey of existing techniques of identifying Wormhole attacks, researchers are focusing to detect and determine the significant challenges of research in the detection of Wormhole attacks in network layer. In our proposed methodology the attacks like wormhole attack, Session attack and false detection attack are some of the malicious attacks that are involved in wireless sensor networks. Now, in this proposed methodology two main protocols are involved the DSR and DSSR protocol using two fish algorithm in MANET. In this article, we uncover an obscure weakness of existing awful estimation location calculations by exhibiting and dissecting another class of assaults, called false information infusion assaults. False detection attacks are also the one of the malicious attack that are taking place in wireless sensor network. Application layer may mean diminished application proficiency with higher improvement costs.

Besides, changing algorithms that the matrix administrators are utilized to and have picked up huge involvement with isn't daintily done. All the more regularly than not, new calculations are first presented as research and advancement models and are not appointed for generation use until the administrators increase some involvement and get alright with utilizing the new algorithm. Comparison of both the DSR and DSSR is carried out in this proposed article using NS2.

The parameters on which we will analyse are end to end delay, throughput, energy spent, PDR and routing overhead Topology of mobile adhoc networks with more no. of nodes and transmission of packets between them is routed using Dynamic Source Routing Technique [DSR protocol], parameters such as end to end delay, throughput, energy spent, PDR and routing overhead will be calculated and output are shown. Topology of mobile adhoc networks with more no. of nodes and transmission of packets between them is routed using Dynamic Source Routing Technique [DSR Protocol] and Wormhole Attack is introduced in the network, to check the performance parameters such as end to end delay, throughput, energy spent, PDR and routing overhead will be calculated and their output is shown in graphs. So for every DSR and DSSR protocol each attack will be introduced and for each attack the parameters will be analysed and results will be shown. Dynamic Source Secure Routing with Digital Signature and Dydog Mechanism integrated with Two fish algorithm [DSSR protocol] and this will also have all three attacks that are to be will be introduced to the protocol and the parameters are analysed and the results will be shown in graph.

IV. RESULTS AND DISCUSSION

A. Simulation Results

A simulation environment is created using NS-2 simulator, and the parameters are defined in Table 1. In order to obtain the performance of a proposed scheme, various QoS parameters such as Delay, PDR, Energy spent, throughput and routing overhead are considered in the evaluation. The DSSR is implemented with attacks in the NS-2 simulator. The following figures in this section describe the various attacks with the proposed protocol.

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS-2
Simulation time (s)	10 sec
Simulation Area (m)	500*500
Total Nodes	50
Protocol used	DSR
Application Protocol	UDP
Packet Size (Byte)	500

B. DSR and DSSR protocols under false data injection attack

The data packets in the MANET are prone to various attacks. In this research work false data injection attack is considered in DSR and DSSR protocols. And different performance parameters are monitored for comparing the performance of DSR and DSSR protocols under false data injection attack.

Fig 1 and 2 represent the comparative plots for the average delay of DSR and DSSR protocols under attack.

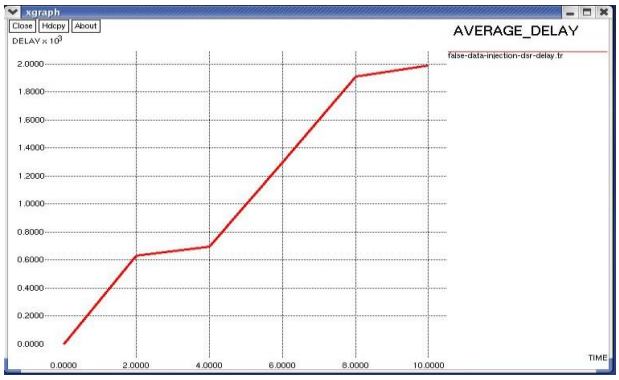

Fig 1: Average delay for DSR Protocol under attack

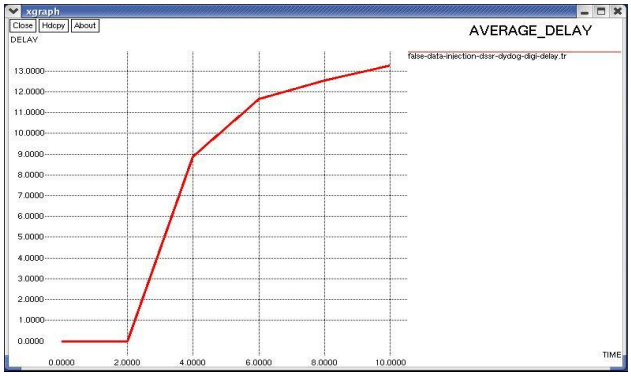

Fig 2: Average delay for DSSR Protocol under attack

Fig 3 and 4 represent the comparative plots for the average throughput obtained for DSR and DSSR protocols under attack.

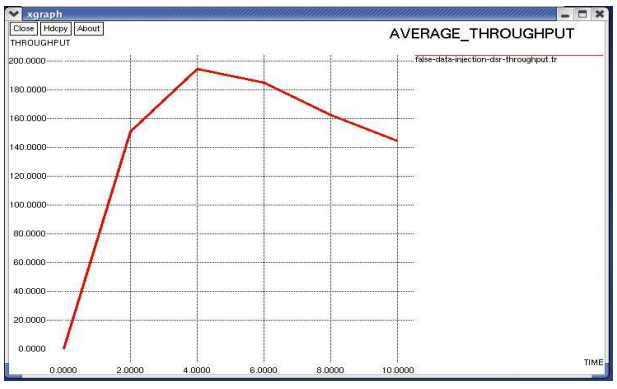

Fig 3: Average Throughput for DSR Protocol under attack

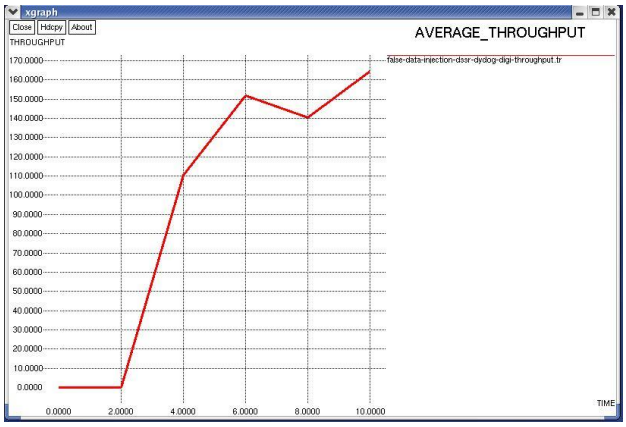

Fig 4: Average Throughput for DSSR Protocol under attack

Fig 5 and 6 represent the comparative plots for the energy spent on DSR and DSSR protocols under attack

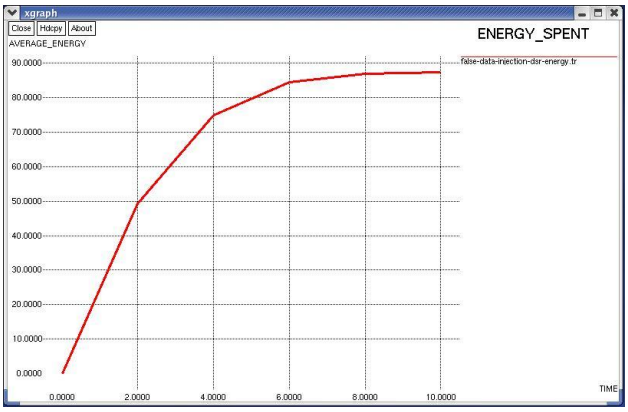

Fig 5: Energy spent for DSR Protocol under attack

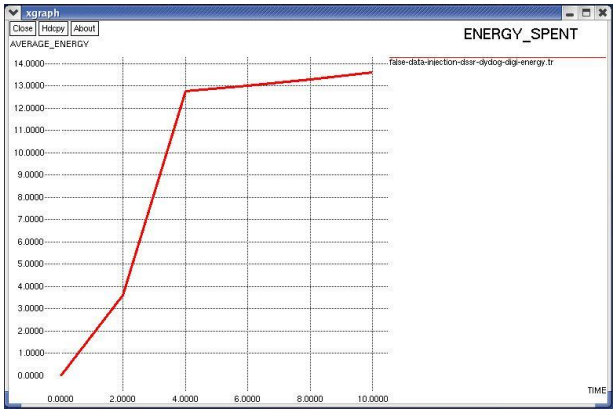

Fig 6: Energy spent for DSSR Protocol under attack

Fig 7 and 8 represent the comparative plots for PDR obtained for DSR and DSSR protocols under attack.

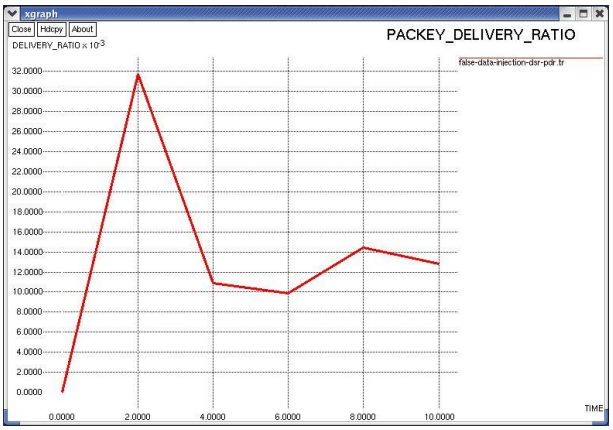

Fig 7: PDR for DSR Protocol under attack

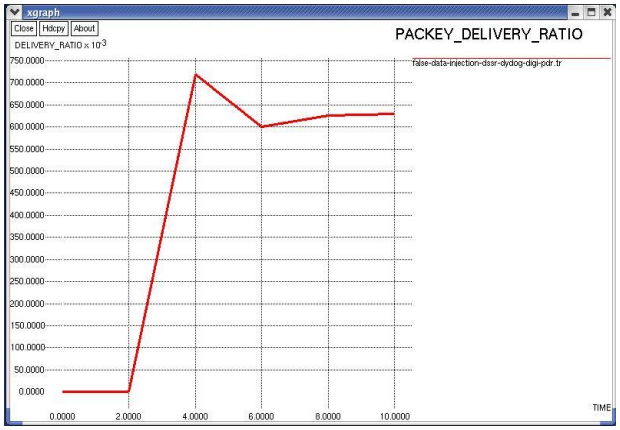

Fig 8: PDR for DSSR Protocol under attack

Fig 9 and 10 represent the comparative plots for the routing overhead obtained for DSR and DSSR protocols under attack.

Fig 9: Routing overhead for DSR Protocol under attack

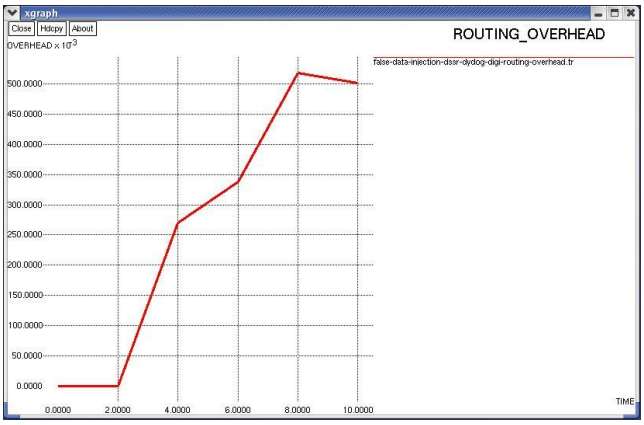

Fig 10: Routing Overhead for DSSR Protocol under attack

C. DSR and DSSR protocols without attacks

The average delay, average throughput, energy spent, PDR, and routing overhead are calculated for DSR and DSSR protocol without any attacks and the results of simulation are provided in this section.

Fig 11 and 12 represent the comparative plots for the average delay obtained for DSR and DSSR protocols without attacks.

Fig 11: Average delay for DSR Protocol without attacks

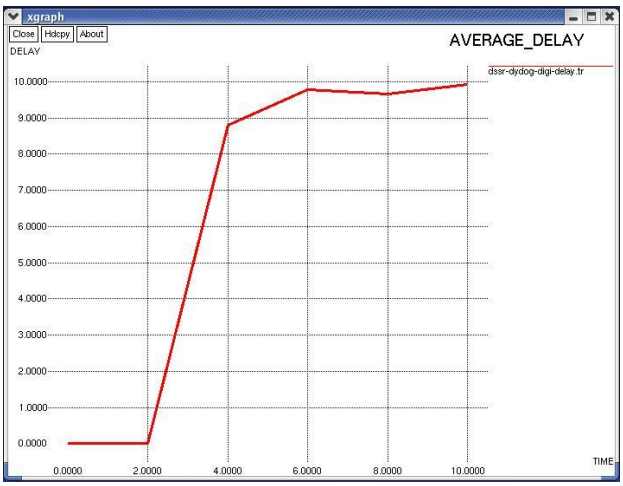

Fig 12: Average delay for DSSR Protocol without attacks

Fig 13 and 14 represent the comparative plots for the energy spent on DSR and DSSR protocols without attacks.

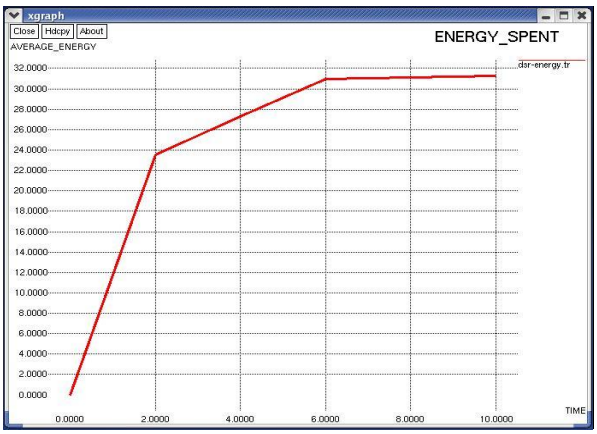

Fig 13: Energy for DSR Protocol without attack.

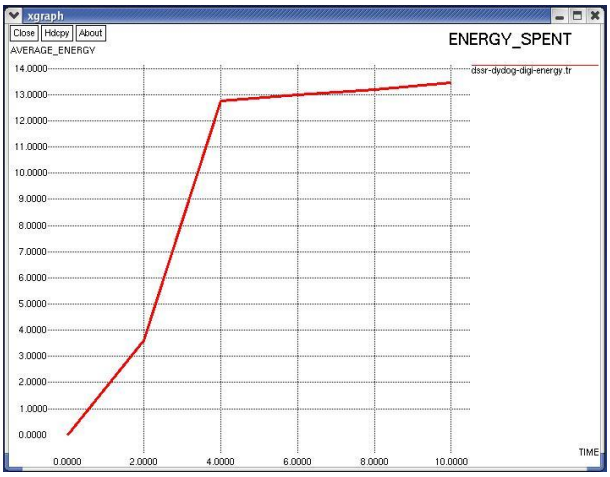

Fig 14: Energy for DSSR Protocol without attacks

Fig 15 and 16 represent the comparative plots for the PDR obtained for DSR and DSSR protocols without attacks.

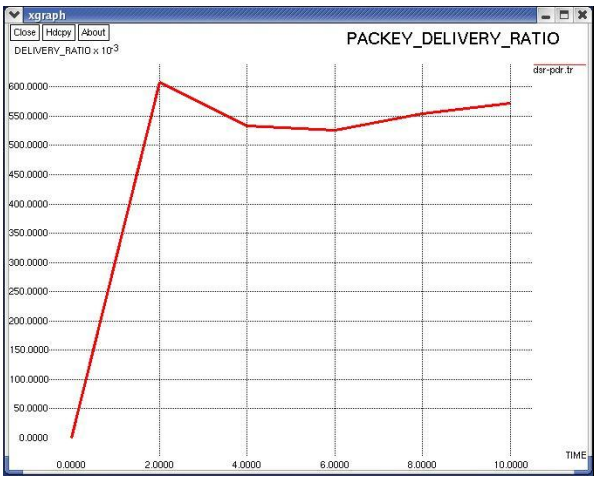

Fig 15: PDR for DSR Protocol without attacks

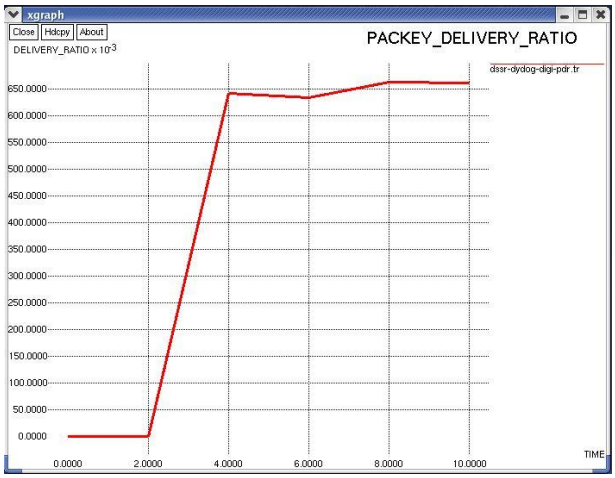

Fig 16: PDR for DSSR Protocol without attacks

Fig 17 and 18 represent the comparative plots for the routing overhead obtained for DSR and DSSR protocols without attacks

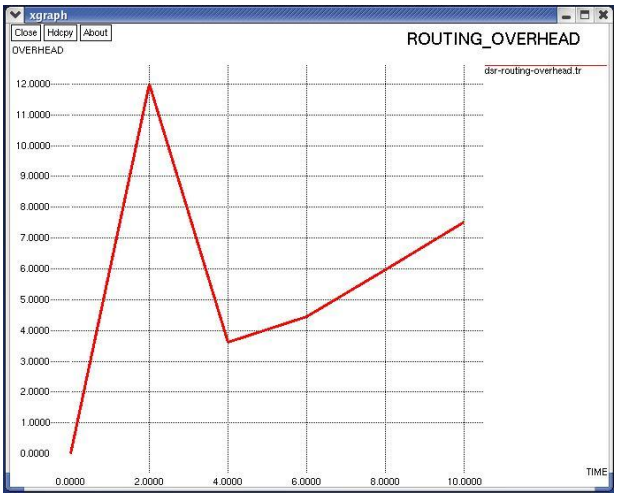

Fig 17: Routing Overhead for DSR Protocol without attacks

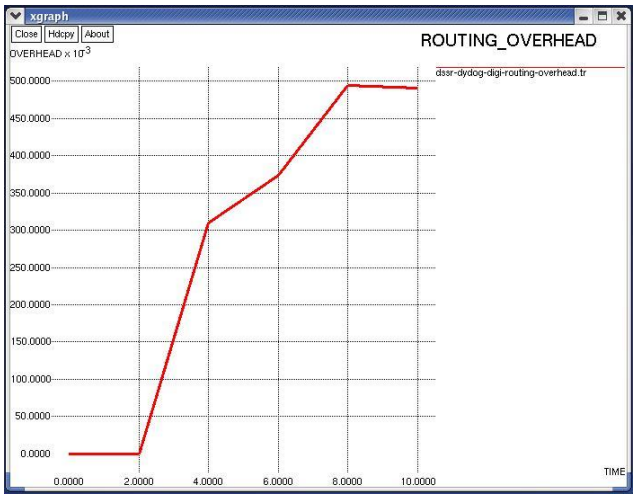

Fig 18: Routing Overhead for DSSR Protocol without attacks

Fig 19 and 20 represent the comparative plots for the average throughput obtained for DSR and DSSR protocols without attacks.

Fig 19: Throughput for DSR Protocol without attacks

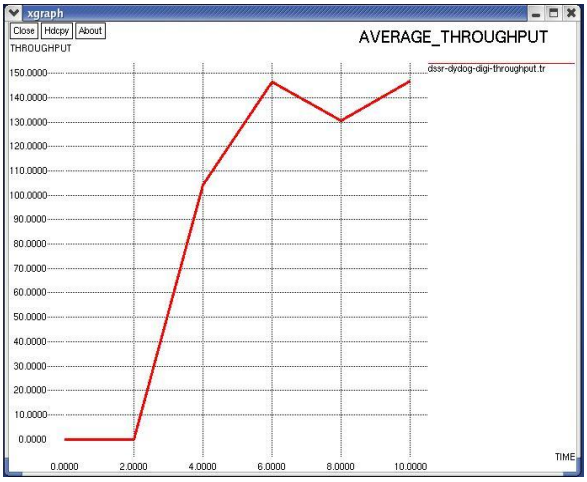

Fig 20: Throughput for DSR Protocol without attacks

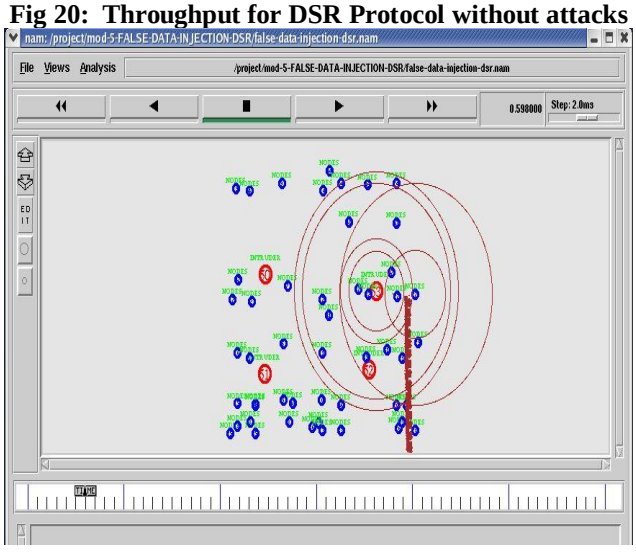

Fig 21: False data injection with DSR protocol

In the above diagram the simulation results of false detection attack are detected and are monitored with the correspondent DSR protocol and are then analysed with various parametric metrics.

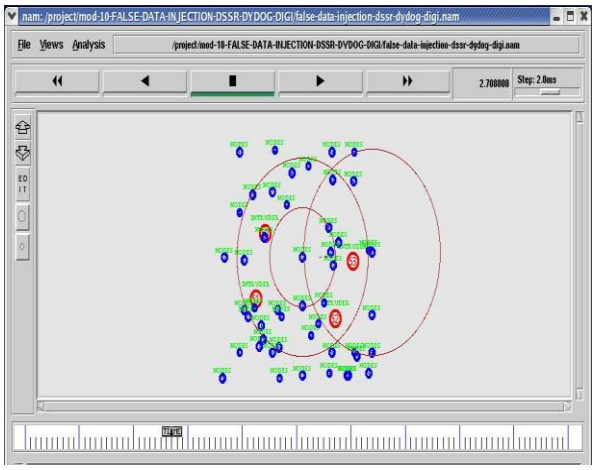

Fig 22: False data injection with DSSR protocol

In the above diagram the simulation results of false detection attack are detected and are monitored with the correspondent DSSR protocol and are then analysed with various parametric metrics. These simulation results clearly show about the malicious attacks that are taking place in both the protocols and the results are analysed. The values of the performance metrics for DSR and DSSR protocols with and without attacks are tabulated in the Table 2.

Table 2: Performance comparison of DSR and DSSR protocols with and without attacks

Performance Metrics	Time (sec)	Without attack		With attack (False data injection attack)	
		DSR Protocol	DSSR Protocol	DSR Protocol	DSSR Protocol
Delay	0	0	0	0	0
	2	1054.99	0	628.85	0
	4	1069.04	8.80	693.32	8.87
	6	1073.08	9.79	1297.16	11.66
	8	1042.71	9.67	1912.04	12.53
	10	1021	9.93	1988.42	13.25
Energy	0	0	0	0	0
	2	23.52	3.62	49.12	3.62
	4	27.26	12.77	74.88	12.76
	6	30.99	13.01	84.44	13.03
	8	31.12	13.19	86.79	13.29
	10	31.24	13.45	87.34	13.60
PDR	0	0	0	0	0
	2	0.6076	0	0.0317	0
	4	0.5341	0.6429	0.0109	0.7193
	6	0.5267	0.6343	0.0099	0.6
	8	0.5539	0.6641	0.0144	0.6263
	10	0.5725	0.6622	0.0128	0.6290
Routing	0	0	0	0	0
	2	12	0	1.895	0
	4	3.61	0.310	4.526	0.270
	6	4.452	0.374	4.614	0.338
	8	5.96	0.494	2.315	0.518
	10	7.516	0.491	2.137	0.501
Through put	0	0	0	0	0
	2	27.74	0	151.02	0
	4	29.35	104.13	194.14	110.48
	6	28.22	146.56	184.96	151.99
	8	24.77	130.66	162.48	140.2
	10	22.59	146.69	144.43	164.48

V. CONCLUSION

In this paper discussion and comparison the encryption algorithm, Data security and also the protocols are monitored with and without attacks of false data injection attack there are some more malicious attack that are very hazardous to the wireless sensor network. In this paper we have discussed about the novel two fish encryption algorithm in both the DSR and DSSR attacks and are then monitored for a certain node with and without false data injection attack using MANET domain. Even though the two-fish algorithm is selected as the top five cryptographic algorithms chosen by NIST to become the AES standard, it can only support up to 256-bit block. The future work will be enhancement of the block size with varying key length. The simulation results compare the values of both the protocols and proposes a better result when are compared with the other state of art algorithms.

REFERENCES

1. Kavitha, V. R., & Moorthi, M. (2019). A Quality Of Service Load Balanced Connected Dominating Set-Stochastic Diffusion Search (Cds-Sds) Network Backbone For Manet. Computer Networks.
2. Shabut, A. M., Kaiser, M. S., Dahal, K. P., & Chen, W. (2018). A multidimensional trust evaluation model for MANETs. Journal of Network and Computer Applications, 123, 32-41.
3. Muchtar, F., Abdullah, A. H., Hassan, S., & Masud, F. (2018). Energy conservation strategies in Host Centric Networking based MANET: A review. Journal of Network and Computer Applications.
4. Kumari, N., Kumar, R., & Bajaj, R. (2018). energy efficient communication using reconfigurable directional antenna in MANET. Procedia Computer Science, 125, 194-200.
5. Kang, D., Kim, H. S., Joo, C., & Bahk, S. (2018). ORGMA: Reliable opportunistic routing with gradient forwarding for MANETs. Computer Networks, 131, 52-64.
6. Goulden, M., Spence, A., Wardman, J., & Leygue, C. (2018). Differentiating 'the user'in DSR: Developing demand side response in advanced economies. Energy policy, 122, 176-185.
7. Omran, S., Broadwater, R., Hambrick, J., Dilek, M., Thomas, C., & Kreikebaum, F. (2017). Load growth and power flow control with DSRs: Balanced vs unbalanced transmission networks. Electric Power Systems Research, 145, 207-213.
8. Upadhyay, R., Bhatt, U. R., & Tripathi, H. (2016). DDOS attack aware DSR routing protocol in WSN. Procedia Computer Science, 78, 68-74.
9. Saraswat, B. K., Bhardwaj, M., & Pathak, A. (2015). Optimum Experimental Results of AODV, DSDV & DSR Routing Protocol in Grid Environment. Procedia Computer Science, 57, 1359-1366.

10. Canning, S. E., Waterman, M. G., Simpson, N., & Dye, L. (2012). Reliability and component structure of the modified Daily Symptom Report (DSR-20). Journal of Affective Disorders, 136(3), 612-619.
11. Verma, H. K., & Singh, R. K. (2012). Performance analysis of RC6, Twofish and Rijndael block cipher algorithms. International Journal of Computer Applications, 42(16), 1-7.
12. Ouni, S., Bokri, J., & Kamoun, F. (2009). DSR based Routing Algorithm with Delay Guarantee for Ad Hoc Networks. JNW, 4(5), 359-369.
13. Tamilselvan, L., & Sankaranarayanan, V. (2007, August). Prevention of blackhole attack in MANET. In The 2nd international conference on wireless broadband and ultra wideband communications (AusWireless 2007) (pp. 21-21). IEEE.
14. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N., Stay, M. (2000). The Twofish team's final comments on AES Selection. AES round, 2, 7.

AUTHORS PROFILE

Rajat pursuing PhD from JECRC University. He has completed B.Tech (H)-M.Tech in computer science and engineering from LPU and has academic experience of 6 years. The area of research is Mobile adhoc networks.

Prof.(Dr.) Naveen Hemrajani, HOD, Computer Science & Engg, JECRC University has more than 26 years of Teaching Experience. He was Principal (Engg.),SGVU and is former Chairman of CSI(Jaipur Chapter). He has received his B.E degree in Computer Science & Engineering from Shivaji University in the year 1992 and M.Tech(CSE) in 2004. His Research Topic for PhD was Admission Control for Video Transmission over IP Networks. He possesses 26 years of Teaching and research experience. He has published three books and many research papers in International and National Journals of repute. He has also presented several papers in International and National conferences. He is also Editorial Board member of many international Journals of repute. He has also organized various International conferences, workshops and seminars.