JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

Hybrid model for Protocol Independent Secure Video Transmission using improvised OSLR with optimized MPR and DYDOG

Ravi Shanker Sharma [1]
Research Scholar, Suresh Gyan Vihar University. India
er.ravishankarsharma@gmail.com

Bright Keswani[2]
Professor, Department of CSE, Suresh Gyan Vihar University, India
bright.keswani@mygyanvihar.com

Dinesh Goyal[3]
Professor, Department of CSE, Poornima Institute of Engineering & Technology, India
dinesh8dg@gmail.com

ABSTRACT

Mobile Ad-hoc Network (MANET) is a group of mobile nodes with changing topological network structures. The mobility of nodes affects the energy level of these nodes which further affects the different QoS parameters of MANET like average delay, Packet delivery ratio, Average throughput etc. At the same time, malicious nods might execute an attack by flooding the network with wrong data or by forestalling different nodes from getting a complete network topology map which further affects QoS parameters. The proactive protocols like OLSR, TORA, AODV etc. are not designed to address these network and security issues at the same time. In this paper, a new hybrid approach is proposed to ensure secure video streaming over MANET that can optimize delay and energy utilization in OLSR, by considering the mobility of nodes as well as to improve the security by dealing with different malicious node attacks like wormhole, black hole and packet replication, that can be achieved with encryption techniques like AES, digital signature etc.

Subject Classification: *Network security*, *Cryptography*

Keywords- MANET, Proactive and Reactive routing protocols, OLSR, Digital Signature, Wormhole Attack.

1. INTRODUCTION

MANET is an infrastructure-free network in which the forwarding of data packets is done through mobile nodes, which can be any device, such as cell phones, laptops, and PDAs. Network topology is inherently dynamic because intermediate nodes are mobile. This topology behavior causes the link state between each node and its neighbors to change, which in turn leads to frequent routing changes and thus traffic overhead. The efficiency of the MANET is closely related to the capabilities of the routing protocol [1].

The whole communication in MANET is done in two stages, namely, route discovery and data transmission. Both the stages are unsafe for various attacks in an adverse environment. Early research focused on protective schemes to protect routing protocols in MANET. Different cryptographic and key management techniques which are used to protect unauthorized nodes from joining the network are the basic solutions. Although, these methods cannot prevent attacks from infected nodes with valid keys. Therefore, intrusion detection and response systems are needed to deal with attacks as the second layer of protection.

2. Related Work

N. Harrag et al., 2017 presented a neighbor discovery by using differential evolution optimization that adjusts the value of the hello interval to find the optimal hello message to improve controlled message overhead. [14]

J. romanik et al., 2016 presented the concept of resource aware OLSR –based routing mechanism for MANET algorithm which was based on node-local resources of node. Simulation experiments were done with the OMNET++ simulation tool and compared with OLSRv2. The WILLINGNESS factor was determined by battery level and traffic node. [15]

Abdelkabirsahnoun et al., 2016 presented an existing algorithm including multi-metric routing metrics that consist of multiple crossed layer parameters. In this proposed work, author put the available residual energy of the neighbor node in WILLINGNESS variable. Simulation experiments were done with NS3 network simulator. [16]

Sefali Prajapati et al., 2015 presented consideration of energy parameter for improving network lifetime. In the proposed technique, MPR selection in OLSR protocol using energy parameter with the degree of 2-hop neighbor node.[17]

Prathviraj n. et al., 2014 presented a technique for MPR selection considering out-degree of node and lifetime of nodes selected as MPR i. e. node which had the highest out-degree and lifetime was greater than the threshold energy. Lifetime of node below threshold energy was not selected as MPR. [18]

K. Prabu et al., 2014 presented a routing algorithm which selects the optimum path between sender and receiver. By using some assumptions like Global positioning system receiver, author firstly select source with 1-hop and store them. It was compared with OLSR algorithm and evaluated through NS-2 simulator. [19]

N. ENNEYA et al., 2009 presented a method to enhance Delay in MANET Using OLSR Protocol which describes that links must be more stable and less mobile to avoid fragile connections which involves data loss and frequent route changes. The main concept was determining the stability (done by calculating node mobile function for mobility and node energy function for residual energy) and fidelity of nodes was determine by the degree of reached ability.[20]

3. Research Gap

As the MANET topology is dynamic in nature, the mobility of nodes is very high. In OLSR protocol, the MPR nodes are used to forward the packets in the routing path. High mobility of MPR nodes causes the re-transmission and re-routing which further lead to high energy consumption and delay. Some experiments in OLSR shows that link mobility should be very low in order to avoid weak connection which involves data loss and frequent rout changes. Uniform utilization of nodes is also a big challenge in order to extended lifetime of nodes and improved network availability.

An effective quantitative method should be proposed to calculate the link stability/mobility for one and two hop MPR selection in enhanced OLSR protocol which may improve different QoS parameter in MANET network transmission.

At the same time security of MPR nodes is another concern to be addressed. Malicious nodes usually interrupt the routing protocol process. The forwarding nodes can be affected by wormhole attack, Black-Hole Attack or Packet Replication attack. Therefore it is require detecting these malicious nodes in order to provide secure forwarding of the packets.

Previously via many research efforts, numbers of enhancements have been proposed in OLSR to improve delay and energy by considering mobility of nodes as well as to improve the security by dealing different malicious nod attacks like wormhole, black hole and packet replication.

However, these routing and security issues have not been taken into concern simultaneously which may lack in overall performance of Video Transmission in OLSR over various QoS parameter.

4. Proposed Protocol Independent Secure Video Transmission (PISVT)

As discussed in research gap in above chapter, we need a synchronized approach to ensure secure video transmission in OLSR so that routing issues of optimization of route identification of MPR nodes and security issues of data packets can be resolved in tandem. To achieve the same we propose a new hybrid framework, namely, PISVT, that combines two existing models in an improvised manner so that fast and secure video transmission can be ensured. The proposed framework is a hybrid model that is an extension of existing OLSR protocol, we have proposed the concept of node stability and link stability for MPR selection and concept of digital signature with DYDOG detection technique for malicious nodes in a single framework.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

The mobility of nodes affects the energy level of nodes which further affects the different QoS parameter of MANET like average delay, Packet delivery ratio, Average throughput etc. However, the MPR nodes with high mobility need to be eliminated from the route as they can affect the performance of routing. In our proposed framework the nodes which have high stability factor will have higher priority for MPR list.

At the same time malicious nods might execute an attack by flooding the network with wrong data or by forestalling different nodes from getting a complete network topology map which further affects QoS parameters. In our proposed framework, we have used the concept of previously existing digital signature with DYDOG detection technique to ensure that malicious nodes are not the part of MPR list as well as to ensure secure and uninterrupted video transmission.

4.1 Node Stability Degree

In the earlier research by Nourddine Enneya et al.,[20], proposed a concept of node mobility factor which was used in MPR selection procedure for optimization of delay in OLSR. This method of MPR Selection has its own limitation while secure video transmission over OLSR as this method does not provide the way to identify the malicious nodes affected by various attacks like wormhole, Sybil etc. In our proposed PISVT method we have enhanced the above technique by implementing 2 major changes, method to discard malicious nodes during MPR selection only, while keeping the concept of node mobility rate based selection/discard process for having more stable links in the network.

As per [20], the link status of network changes frequently in time as the nodes move in the mobile ad-hoc network. However, we define a Stability measure representing the degree of node Stability in the network.

Stability degree of a mobile node i at a time T is defined by the following formula:

$$MB_i^{\mu}(T) = \mu \frac{nodesout(t)}{nodes(T-\Delta T)} + (1-\mu) \frac{nodesin(t)}{nodes(T)} \quad \textbf{(1)}$$

Where:

NodesIn(T): The total nodes that moving in the transmission domain of during the interval $(T - \Delta T)$

NodesOut(T): The total nodes that moving out the transmission domain of during the interval $(T - \Delta T)$

Nodes(T): The total nodes in the transmission domain of i at time T.

μ: The Stability coefficient between 0 and 1

The degree of stability of a node at a given time T for a node in MANET is defined as the change in its neighbors compared to the previous (state) at time. Thus, mobile nodes that enter and/or leave a node's neighbors will certainly affect the evaluation of its degree of stability. In addition, we have chosen a stability factor μ between 0 and 1 in order to have a node stability degree in the interval [0, 1].

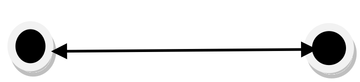
4.2 Link Stability Estimation

Links should be more stable and less mobile to avoid weak links associated with data loss and frequent route changes.

We define the Stability of a link Li between two nodes P and Q as the average Stability of the involved nodes, as showed in following equation:

$$MB_{Li(P,Q)}^{\mu} = \frac{MB_P^{\mu}(T) + MB_Q^{\mu}(T)}{2} \quad \textbf{(2)}$$

20% 50%



The dependence between the Stability of nodes composing a link (in the network core) at the time t can be seen as Stability dependence of link L(A,B) as follows:

$$D^{\mu}_{Li(P,Q)}(T) = |MB^{\mu}_{P}(T) - MB^{\mu}_{Q}(T)| \quad \textbf{(3)}$$

A reliable symmetric link in terms of Stability can be seen as a link satisfying the two following conditions:

The average Stability of the link L(i,j) is higher than a threshold THD_Link which depends on the characteristics of the wireless network (network density, network Stability, network scalability, network dimension):

$$\mathbf{MB^{\mu}_{Li(P,Q)}(T)} > THD\_Link \quad \textbf{(4)}$$

The Stability dependence of link L (i,j) is near to one :

$$\mathbf{D^{\mu}_{Li(P,Q)}(T) \rightarrow 1} \quad \textbf{(5)}$$

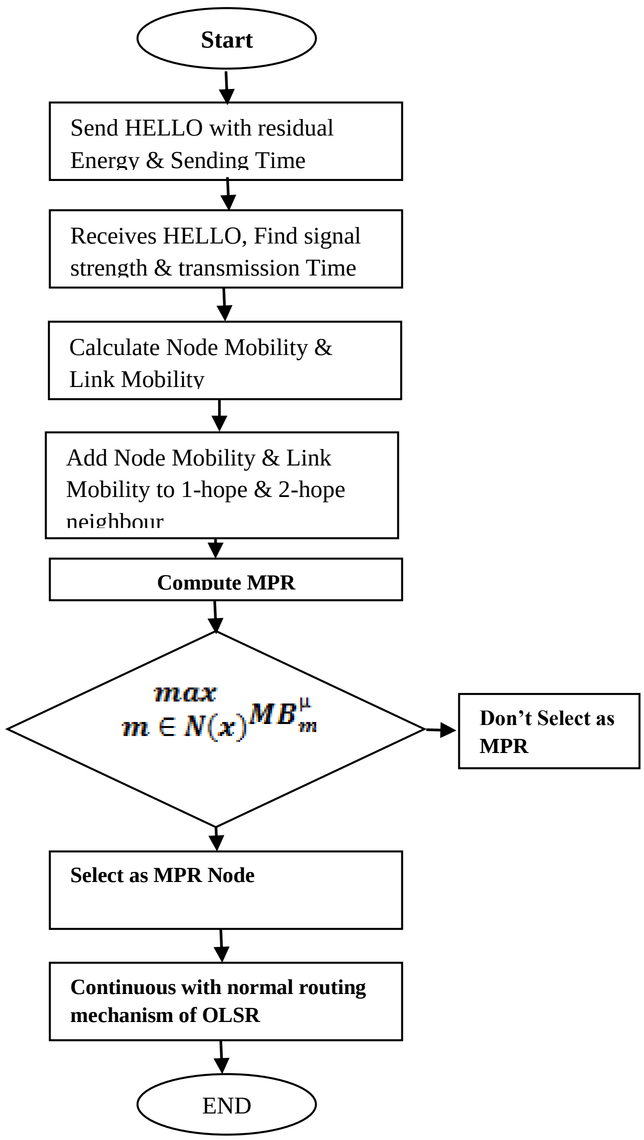


Figure 1: Flow chart to select MPR through stability concept

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

4.3 Digital Signature with DYDOG-

When a node involved in the transmission sends a request to the DYDOG node, at the sender side the hashed data are created by adding a hash function and two fish algorithm for encryption. Cipher Block Chain (CBC) cipher is used for generating a certificate.

The cryptographic technique is processed by encrypting the hashed data using a private key and also by generating the digital signature for the data to be signed. On the receiver side, digitally signed data is decrypted and is verified using the same hash function using the public key. Signed data are compared with the evaluated digital signature. If there is a match, the receiver can accept the message as an authenticated data; otherwise, the node is identified as a Sybil.

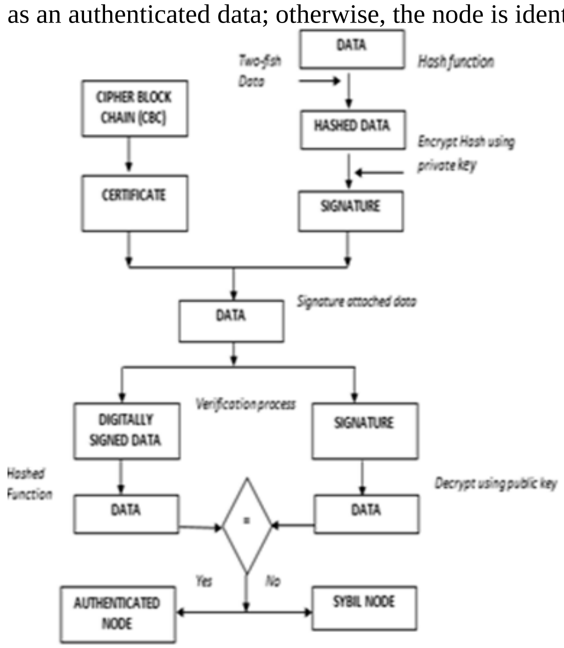


Figure 2: Flowchart of DS with DYDOG

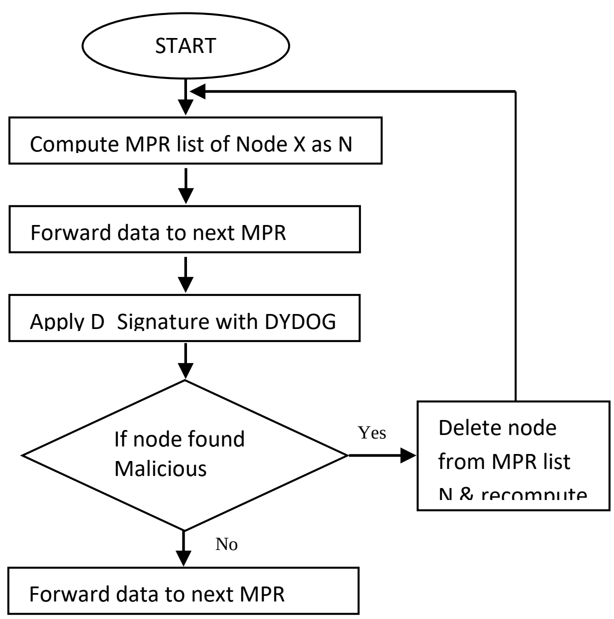


Figure 3: Flow chart for secure transmission using PISVT

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

Fig.2, illustrates a secured data communication processed by embedding the cryptographic technique. In the encryption phase, each data traversing the network is applied with the two-fish algorithm and hash function. The data is encrypted using a private key, and the signature is appended to it. Meanwhile, from the (CBC), a certificate is generated. Both the data with the signature and the certificate is integrated to produce a secured data. In the decryption phase, the output of the encryption phase undergoes a verification process. From the digitally signed data and signature, the data is extracted using the hash function.

Whereas, the signature is decrypted by accessing the public key and the data is retrieved. Both the obtained data are verified. If both the data is equal, it is an authenticated node; otherwise, the node is identified as a Sybil attacked node.

5. SIMULATION PARAMETERS

The parameters considered for simulation are presented in Table 4.1. Then the performance measures, namely, Average Delay, Packet Delivery Ratio (PDR), throughput and energy spent are estimated in NS-2 environment. The number of nodes considered for the implementation is 50, and size of the packet is 500 bytes. The routing protocols considered for the implementation are AODV, AOMDV, DSDV, TORA and our Proposed PISVT. The time taken for the process of simulation is 10 seconds. And the protocol used at application layer is the User Datagram Protocol (UDP).

Table 1: Simulation Parameters

PARAMETERS	**VALUES**
Number of nodes	50
Packet Size (Bytes)	500
Routing Protocol	AODV, DSR ,AOMDV, DSDV, TORA, PISVT
Simulation Time (s)	10
Simulation Area (m)	500*500
Application Protocol	UDP
Video Format	MP4/H.264/SVC

6. SIMULATION RESULTS

In this section, simulation results obtained for different protocol under normal condition and wormhole attack are presented

Table 2: Simulation Results under all situation

	Time	**UNDER NORMAL CONDITION**				**UNDER ATTACK CONDITION**			
		Average Delay	**Energy Spent**	**PDR**	**Throughput**	**Average Delay**	**Energy Spent**	**PDR**	**Throughput**
AODV	2	2040	16.3	0.1296	18.08	2570	17.7	0.012	18.5
	4	1360	16.4	0.1987	23.9	1560	18	0.0198	24.4

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

	6	975	16.6	0.2877	27.15	1270	18.3	0.0287	36.4
	8	837	16.8	0.337	27.2	1140	18.7	0.0337	33.2
	10	785	16.9	0.3681	25.65	1050	19	0.0368	29.9
AOMDV	2	181	16	0.3296	36.08	1285	17.5	0.11	36
	4	113	16.2	0.3987	46.9	780	17.8	0.18	48
	6	74	16.4	0.4877	54.15	635	18.1	0.37	72
	8	160	16.6	0.537	54.2	570	18.5	0.33	66
	10	55	16.7	0.5681	50.65	525	18.8	0.4	58
DSDV	2	1040	16.1	0.2296	18.08	3570	18.7	0.032	28.5
	4	360	16.2	0.2987	23.9	2560	19	0.0398	44.4
	6	875	16.3	0.3877	27.15	2270	19.3	0.0487	46.4
	8	737	16.4	0.437	27.2	2140	19.7	0.0537	43.2
	10	685	16.5	0.4681	25.65	2050	18	0.0568	49.9
TORA	2	840	15.2	0.2296	28.08	970	18.7	0.0562	180.5
	4	660	15.4	0.4987	43.9	760	18.8	0.0698	240.4
	6	775	15.6	0.5877	47.15	770	19.3	0.0687	360.4
	8	537	15.8	0.537	47.2	540	19.7	0.0637	330.2
	10	585	15.9	0.5681	45.65	750	20	0.0668	290.9
PISVT	2	0.9	12.6	0.5	40.7	4.5	11.6	0.6	140
	4	18.5	12.7	0.8	130.1	90	11.7	0.9	130
	6	28.3	12.9	0.7	120.15	140	12.1	0.8	200
	8	28.3	13.1	0.8	121.1	140	12.2	0.9	210
	10	28.6	13.2	0.84	120.95	140	12.2	0.9	200
PISVT with DYDOG	2	Is applicable in attack condition only				0.45	10.6	0.9	240
	4					9	10.7	0.9	230
	6					14	11.1	0.9	300
	8					14	11.2	0.9	310
	10					14	11.2	0.9	300

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

6.1 COMPARISON OF AODV, AOMDV, DSR, TORA AND PISVT

Following Figure 4 represents the plot for Average Delay obtained for all protocol under all situations.

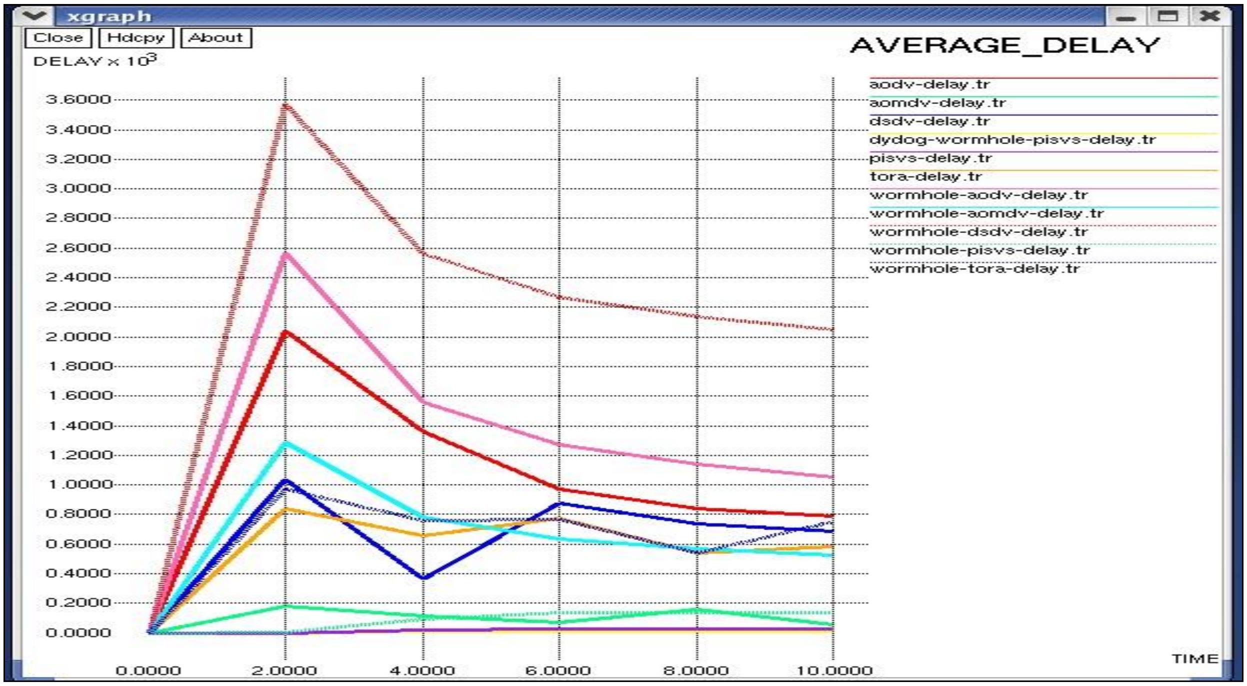


Figure 4: Average Delay Comparison of all protocol under all situations

Following Figure 5 represents the plot for Energy Spent obtained for all protocol under all situations.

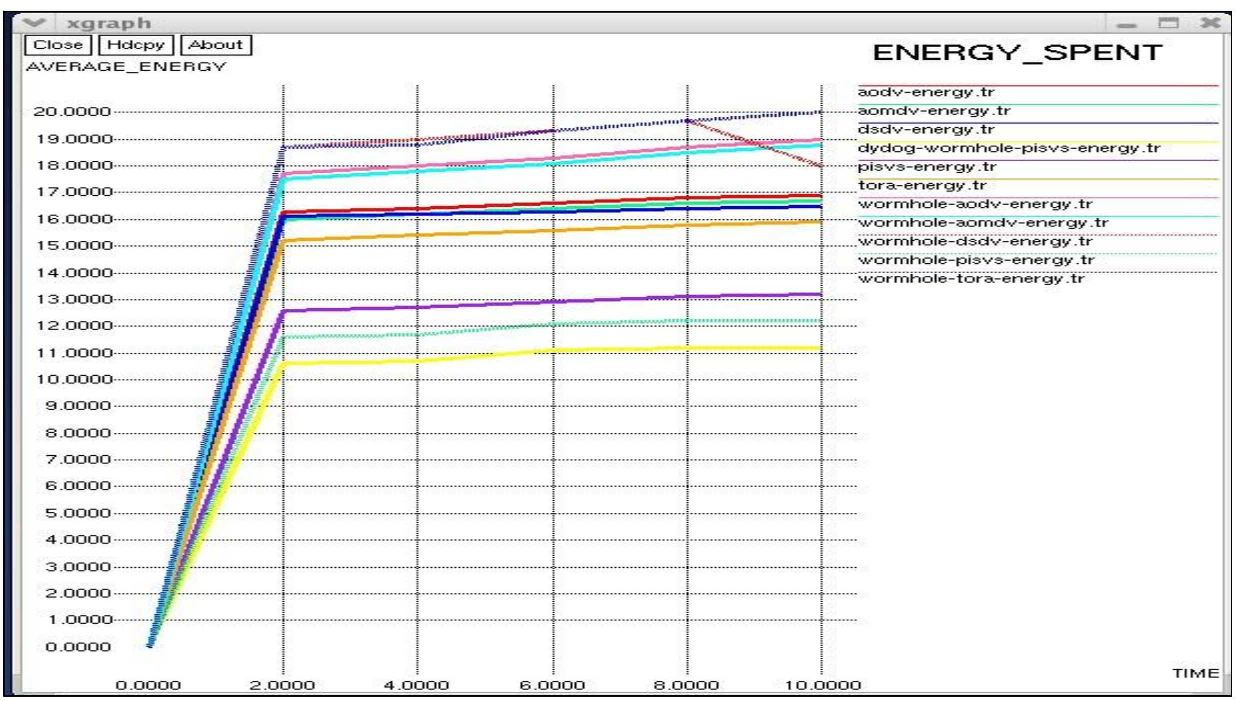


Figure 5: Energy Spent Comparison of all protocol under all situations

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

Following Figure 6 represents the plot for Packet Delivery Ratio obtained for all protocol under all situations.

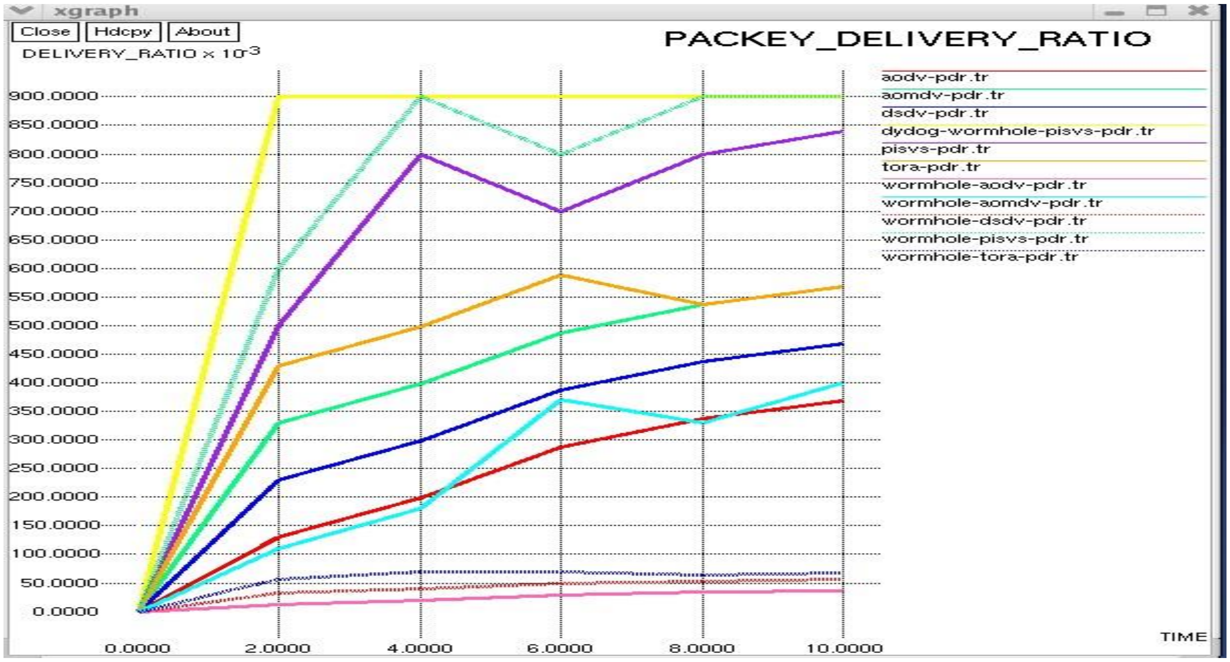


Figure 6: PDR Comparison of all protocol under all situations

Following Figure 7 represents the plot for Throughput obtained for all protocol under all situations.

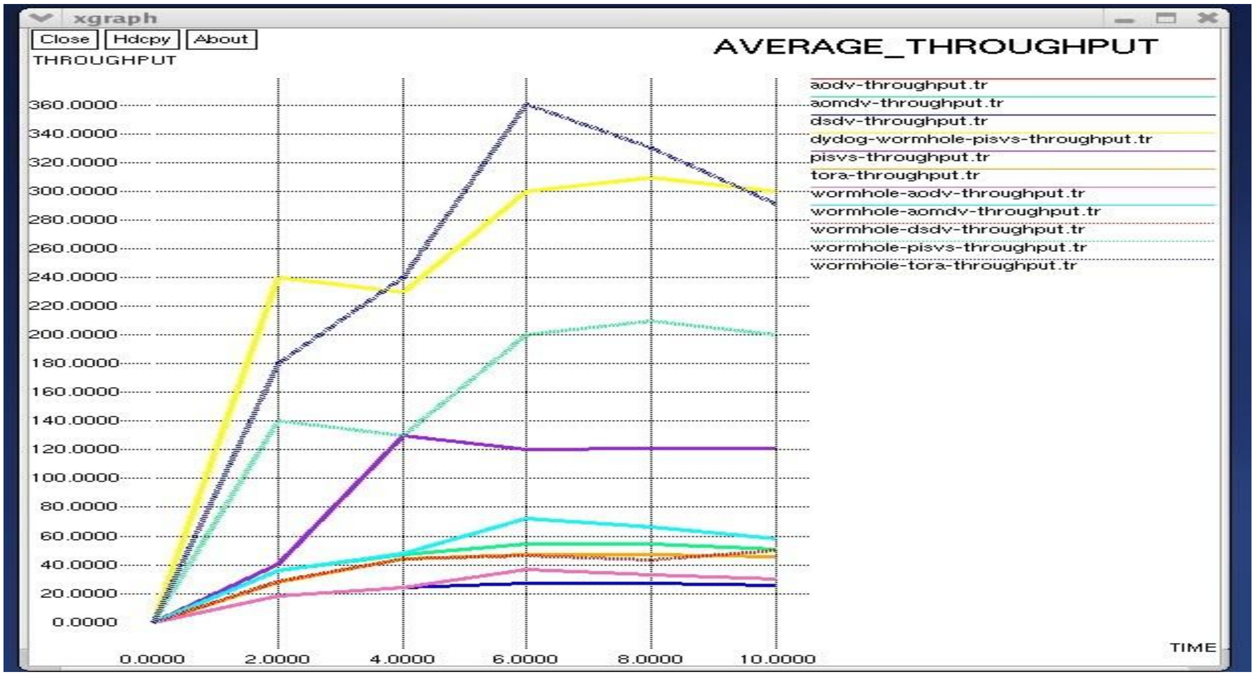


Figure 7: Throughput Comparison of all protocol under all situations

Following Figure 8 represents the plot for PSNR obtained for all protocol under all situations.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1669 - 1679
https://publishoa.com
ISSN: 1309-3452

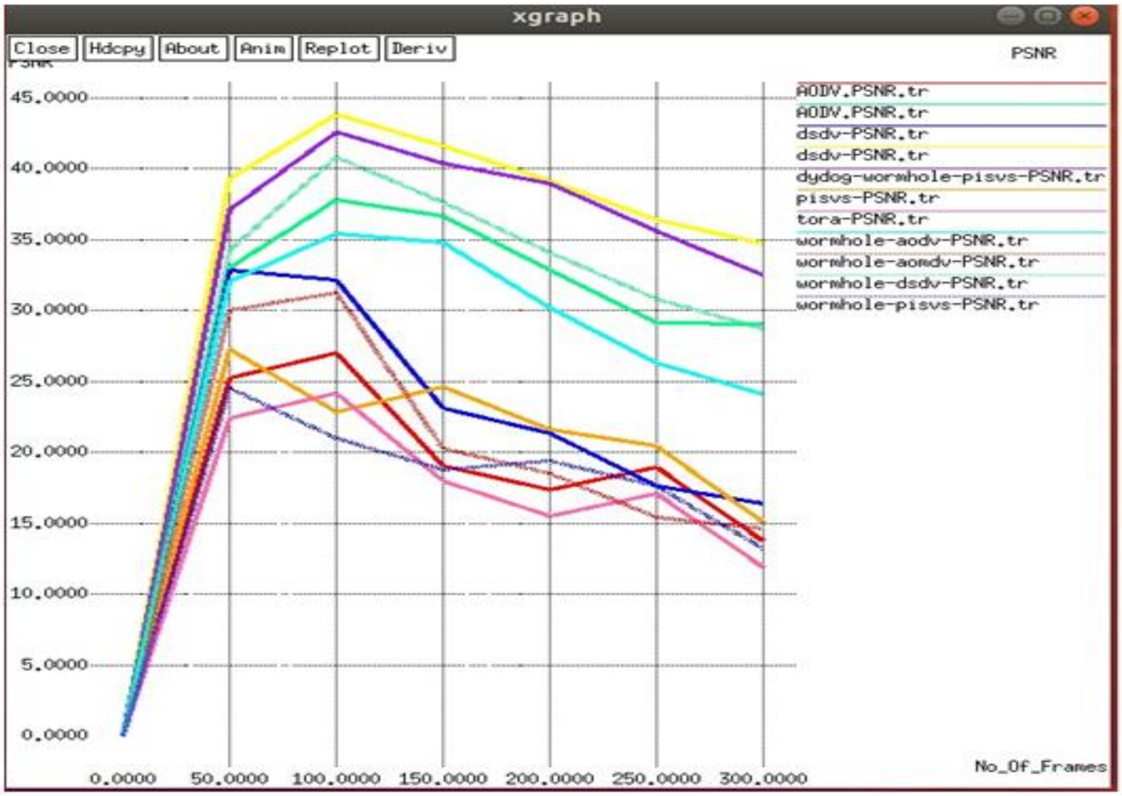


Figure 8: PSNR Comparison of all protocol under all situations

7. Conclusion

This paper proposes a hybrid framework namely PISVT and compares its simulation results of five protocols, namely, AODV, AOMDV, DSDV, TORA and our proposed PISVT. These protocols were simulated and analyzed over NS2 for their performance in normal condition (no attacks), and when subjected to attacks like false data injection, session hijacking, and wormhole. The performance of proposed PISVT protocol for routing in MANETs show better performance compared to the other protocols over various QoS parameters.

REFERENCES

[1.] Jian Liu, Xin Ji, Ci Huang and Xinxin Tan "A NOVEL OLSR PROTOCOL WITH MOBILITY PREDICTION" Third International Conference on Cyberspace Technology (CCT 2015), IEEE Xplore: 07 April 2016

[2.] J. Coriil, S. Ochoa, J. Pino. High level MANET protocol: Enhancing the communication support for mobile collaborative work. Elseiver journal of Network and Computer Applications. 2012; 35 (1), 145-155.

[3.] P. Papadimitratos, Z.J. Haas, Secure message transmission in mobile ad hoc networks, in journal Ad Hoc networks. 2003; 1(1),193-209.

[4.] Perkins C, Belding-Royer E, Das S. Ad hoc on-demand distance vector (AODV) routing. IETF RFC 3561, 2003.

[5.] Johnson DB, Maltz DA, Hu Y-C. The dynamic source routing protocol for mobile ad hoc networks (DSR). IETF Internet Draft, draft-ietf-manet-dsr-09, 2003.

[6.] T.Clausen, P. Jaquet, IETF Request for Comments: 3626 Optimized Link State Routing Protocol OLSR, october 2003.

[7.] Ogier R, Lewis M, Templin F. Topology dissemination based on reverse-path forwarding (TBRPF). IETF Internet Draft, draft-ietf-manet-tbrpf-07.txt, 2003.

[8.] J-H. Zygmunt : A new routing protocol for the recon_gurable wireless networks. In Proceedings of 6th IEEE International Conference on Universal Personal Communications, IEEE ICUPC'97, October 12-16, 1997, San Diego, California, USA.

[9.] Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer E. A secure routing protocol for ad hoc networks. Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[10.] Zapata MG, Asokan N. Securing ad-hoc routing protocols. Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), Atlanta, GA, U.S.A., September 2002; 1–10.

[11.] Hu Y-C, Johnson DB, Perrig A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002). IEEE: Calicoon, NY, June 2002; 3–13.

[12.] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, 27–31 January, 2002.

[13.] Zhou L, Haas ZJ. Securing ad hoc networks. IEEE Networks Special Issue on Network Security, November/ December 1999; 24–30.

[14.] Harrag, N., A. Refoufi, and A. Harrag. "Neighbour discovery using novel DE-based adaptive hello messaging scheme improving OLSR routing protocol performances." Systems and Control (ICSC), 2017 6th International Conference on. IEEE, 2017.

[15.] Romanik, Janusz, Adam Kraśniewski, and Edward Golan. "RESA-OLSR: RESources-aware OLSR-based routing mechanism for mobile ad-hoc networks." Military Communications and Information Systems (ICMCIS), 2016 International Conference on. IEEE, 2016.

[16.] Sahnoun, Abdelkabir, Jamal El Abbadi, and Ahmed Habbani. "Increasing network lifetime by energy-efficient routing scheme for OLSR protocol." Industrial Informatics and Computer Systems (CIICS), 2016 International Conference on. IEEE, 2016

[17.] Prajapati, Sefali, Nimisha Patel, and Rajan Patel. "Optimizing Performance of OLSR Protocol Using Energy Based MPR Selection in MANET."Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on. IEEE, 2015.

[18.] Prathviraj N., Prashanth Kumar A,"Lifetime aware MPR selection in OLSR for MANET",International Conference on Electronics, Communication and Computational Engineering (ICECCE),2014

[19.] Prabu, K., and A. Subramani. "Performance analysis of modified OLSR protocol for MANET using ESPR algorithm." Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014.

[20.] N. ENNEYA, K. OUDIDI, M. ELKOUTBI Enhancing Delay in MANET Using OLSR Protocol, Int. J. Communications, Network and System Sciences, 2009, 5, 392-399