Journal of Engineering Science and Technology
Vol. XX, No. Y (Year) PPP - QQQ

COMPARATIVE ANALYSIS OF AODV AND DSDV USING MACHINE LEARNING APPROACH IN MANET

AYUSHREE[1], SANDEEP KUMAR ARORA[2,*]

[1]School of Electronics and Communication Engineering, K L University, Guntur, Andhra Pradesh, India
[2]School of Electronics and Communication Engineering, Lovely Professional University, Punjab, India
*Corresponding Author: sandeep.16930@lpu.co.in

Abstract

Mobile Ad-Hoc networks possess a dynamic structure which is characterized by the absence of central administrator. Due to such dynamic network, the possibilities of acquisition of optimal path diminish to a great extent and hence the durability of the optimal transmission of data packet becomes severe. Each and every node in MANET is battery powered up and mobile in nature, hence mobility becomes the prime reason of energy exhaustion in such network. The main objective of presented paper is to attain the most reliable path with least mobility for successful transmission of data packets. The algorithm used for attainment of optimal path is knowledge based learning algorithm which is implied over two routing protocols; AODV (Ad-Hoc On Demand Distance Vector Routing) and DSDV (Destination Sequence Distance Vector Routing). The performance evaluation is done by means of Relay Number which is inversely proportional to the mobility of node. AODV and DSDV are further employed over network systems with varying number of nodes, i.e., 12 and 24 nodes network system. The performance comparison is made on the basis of two performance parameters such as throughput and PDR (Packet Delivery Ratio). A proposition is made that analysis of PDR and throughput in knowledge based learning algorithm is better in comparison with other traditional techniques like Destination Sequence Distance Vector (DSDV). The simulation is performed over NS-2 network simulator, which enables the implementation of wired and wireless simulation.

Keywords: PDR (Packet Delivery Ratio), Relay number, Throughput, DSDV, AODV, Black Hole attack, Malicious attack, Link failure.

Nomenclatures

B	Black hole node
d	Destination node
F	Input output mapping function
G	Required output function
$\underline{G_{i,j}}$	Path gain between n_i and n_j
I	Iteration of mobility samples
$\underline{(l,m)}$	Arbitrary point
M_1	Mobility at node 1
M_2	Mobility at node 2
M	Malicious node
N	Integer
n_i	Origin node
n_j	End node
P	Path
P_i	Transmitted power of n_i
pl	Link failure
R	Relay Number
r	Relay node
s	Source node
W	Network system
$(X1, Y1)$	Position of node
$(xi1....)$	Mobility at x coordinate
$(xi1\text{-}1.)$	Mobility at delayed x coordinate
$(yi1....)$	Mobility at y coordinate
$(yi1\text{-}1.)$	Mobility at delayed y coordinate

Greek Symbols

$\forall$	Parameter
Ψ	Threshold Value

Abbreviations

MANET	Mobile Adhoc Network
PDR	Packet Delivery Ratio
AODV	Adhoc On Demand Distance Vector
DSDV	Destination Sequence Distance Vector
RREQ	Route Request
RREP	Route Reply
NS2	Network Simulator 2
SNR	Signal to Noise Ratio

1. Introduction

A Mobile Adhoc Network (MANET) is a network system where every node works collectively without any hindrance from the centralized authority. An increase interest is observed in mobile wireless communication due to their pervasive feature. MANET is such a network which provides the flexibility to the network system by maintaining the fixed network and exchange of

information without any access point or base station requirement. Multi hop communication enables the network to achieve this and permits node to approach distant nodes by means of relay nodes or intermediate nodes. A fundamental problem observed in MANET is the maintenance and election of stable multiple hop path. There are numerous elements that cause asymmetry in the network topology like node mobility, excess power consumption and signal interference intervention, which leads to the loss of path and as consequence the information is lost.

An ample amount of work is performed on the attainment of link stability by using many traditional techniques as described in [1-4]. Moreover, performance analysis of network system is made on the basis of different routing protocols, such as, AODV, DSDV, and so forth [5-6]. There are certain factors which lead in the performance degradation of network inhibiting the successful transmission of data packets from source and destination. One of such factor is foreign attack discussed in [7-9] comprising effects of malicious, black hole, gray hole attack and many more over the network. These attacks tamper the entire network setup resulting into numerous adverse effects; energy exhaustion of nodes, link failure, loss of data packets, error in data packets transmission etc. [10]. In order to overcome these attacks certain methods are advocated in [11] which not only enables the path reconstruction but also provides the enhanced QoS of the network system. [12-14] portraits beneficial methods of mobility prediction and energy conservation topology implemented over Adhoc wireless network which leads in the establishment of stable and reliable path.

Many traditional techniques are used prior, in the attainment of most reliable path by means of learning algorithm. In [15] an extreme learning approach is proposed in order to compute the path with least stability. Likewise, in the proposed method stable route is attained by means of Knowledge based learning algorithm. Knowledge Based Learning algorithm is applied to unsupervised learning problems which does not require any training data. Absence of training data leads in the minimization of burden over the network system. This algorithm does not have any target or outcome variable to predict or estimate. On the other hand, other machine learning approach is applied to a supervised learning algorithm which would require training data. This algorithm consists of an outcome variable which is to be predicted from a given set of independent variables.

If a comparison of knowledge based learning algorithm is made with other machine learning algorithm as given in [15] than the proposed work would be preferable as it is an unsupervised learning algorithm and does not require any training data. If a supervised data would be taken under consideration than the complexity of network maintenance would increase as training data is required for supervised learning algorithm.

In the proposed work, prime focus is to achieve the most stable path which has already experienced link loss due to mobility of node. This is achieved through knowledge based learning algorithm. It is a type of machine learning algorithm which recruits former learned network and make decisions on the basis of acquired information. Furthermore, by application of different routing algorithm, such as, AODV and DSDV, a performance comparison is made amongst the cases of varying number of nodes. AODV and DSDV are reactive protocols which are acknowledged as per the demand in the network system. Moreover, the above discussed cases are

analyzed by introduction of black hole and malicious attack; in general, there are three cases which are analyzed in the proposed work. One is the ideal case where no foreign attack is imposed over the network and the other is non-ideal case, where network is imposed over black hole and malicious attack. After the establishment of all the autonomous environment as discussed above, a comparison is made by performance parameters throughput and PDR (Packet Delivery Ratio).

The following paper is organised as follows: Section II presents the proposed work; Section III presents research methodology; Section IV presents result, simulation and analysis; finally, Section V concludes the paper and identifies conclusion and future scope.

2. Knowledge Based Learning Algorithm

As discussed prior, the foremost condition of data packets for routing from origin to end node is to persist effectiveness in network. If the consumption of energy is less, than it would result in increased lifetime of node which would help in data transmission. In particular, the main aim of our paper is to reduce the possibility of link failure. The parameter used for the assumption of efficient path in knowledge based learning algorithm is relay number.

Knowledge based learning algorithm recruits the previous learned algorithm and make the decisions based on the knowledge attained. This would allow us to make conclusions of when and where efficient knowledge is available. By means of previous knowledge and pattern recognition, relay numbers are allocated to each respective node in the network system. An unknown function given as $F: A \rightarrow B$ where F is the actual truth on which input and output are mapped as a $\in A$ and $b \in B$. Training data accompanies these instances which would denote the accurate sample of required output producing a function of $G: A \rightarrow B$. The function G would provide us an approximate estimation of required output. Probability estimation of each possible outcome is made for every input instance whenever pattern is supposed to be analyzed on the basis of stability. The yielded function is shown in Eq. (1):

$$f(label|a, \forall) = x(a, \forall) \tag{1}$$

Here characterisation of *'x'* is performed by parameter $\forall$. The inverse probability of $f(a|label)$ is approximated with the previous probability by usage of Bayes' rule as shown in Eq. (2) :

$$f(label|a, \forall) = \frac{f(a|label, \forall) f(label|\forall)}{\sum_{L \in alllabels} f(a|L) f(L|\forall)} \tag{2}$$

To attain continuous distribution of labels integration is preferred rather summation which is given as Eq. (3): -

$$f(label|a, \forall) = \frac{f(a|label, \forall) f(label|\forall)}{\int_{l \in label}^{L \in alllabels} f(a|L) f(L|\forall) dL} \tag{3}$$

The algorithm of Knowledge Based Learning Algorithm is given as follows: -

Algorithm 1: Knowledge Base

$Manet(\ )$

$£ \rightarrow networksystem$
$n \rightarrow 0, 1, 2, 3 \ldots\ldots\ldots\ldots . N$
$£(t) = \{(X1, Y1) \ldots\ldots\ldots\ldots\ldots (Xn, Yn)\}$
$where$
$X1 = \{xi1, xi2, xi3 \ldots\ldots\ldots\ldots\ldots xin\}$
$Y1 = \{yi1, yi2, yi3 \ldots\ldots\ldots\ldots\ldots yin\}$
$£(t-1) = \{(X1, Y1) \ldots\ldots\ldots\ldots\ldots (Xn, Yn)\}$
$where$
$X1 = \{x(i1-1), x(i2-1), x(i3-1) \ldots\ldots\ldots\ldots\ldots x(in-1)\}$
$Y1 = \{y(i1-1), y(i2-1), y(i3-1) \ldots\ldots\ldots\ldots\ldots y(in-1)\}$
$for\ i = 1 \rightarrow n$
$Computationofnodeposition$
$R \rightarrow RelayNumber$
$if((£(t) == £(t-1))$
$9 \leq R \leq 10$
$elseif(£(t)! = £(t-1))$
$5 \leq R \leq 8$
$else$
$1 \leq R \leq 4$
end
end

The given algorithm provides the working of knowledge based learning algorithm where the network setup is taken as $Manet(\ )$.

Initially the mobility of node is monitored which is present at a certain arbitrary point (*X, Y*). £(*t*) collectively gives information of mobility of node at present instant of time. It is followed by delayed *£(t-1)* which provides us the information of the very same node with x and y coordinate *(X, Y)* at the previous instant of time. When the data is transmitted from 1 to n (integer number), relay number (*R*) is allocated by recruiting £(*t*-1) along with £(*t*). If £(*t*) is nearly equal to £(*t*-1) '*R*' will range between 9 to 10. Whereas if £(*t*) is not equal to £(*t*-1) than the '*R*' will range between 5 to 8 and if none of the condition is true than it can be conclude that the network is highly degraded in terms of performance and efficiency ranging '*R*' from 1 to 4.

3. Research Methodology

The pattern recognition allows gathering of the knowledge about mobility of node and by means of these patterns relay numbers are allotted accordingly. Whenever the information is transmitted from one to another node than the power required is inversely proportional to the n^{th} power of the distance *(d)* between these nodes by $1/d^n$. Here n ranges between 2 and 4 on the basis of the distance between the observed nodes. For successful routing SNR (signal to noise ratio) of second node must be in excess with threshold value. If

n_i: Origin node
n_j: End node
Ψ: Threshold value

The SNR_jmust satisfy the following conditiongiven in Eq. (4): -

$$SNR_j = \frac{P_i G_{i,j}}{\sum_{k \neq i} P_k G_{k,j} + \eta_j} \Psi_j(BER) \quad (4)$$

where P_i: Transmitted power of n_i, $G_{i,j}$: Path gain between n_i and n_j and Ψ_j: Threshold value

$$G_{i,j} = \frac{1}{d_{i,j}^n} \quad (5)$$

The methodology is initiated by setting up 4 network setups; 2 setups consisting 12 nodes where is processed over AODV and DSDV routing algorithm. Likewise, 2 more setups are considered that consist of 24 nodes where each is routed through AODV and DSDV routing algorithm. If this network setup suffers from any link failure than knowledge based learning algorithm is applied. The selection of the optimal path is done by means of relay number which is inversely proportional to the node mobility. As per the network setup the network configuration for AODV and DSDV routing algorithm is given in Eq. (6) to Eq. (9) follows:

$$W_{AODV} = \{s, d, r, pl\} \quad (6)$$

$$P_{s \to r} = \left\{(l,m) \middle| power_{s \to r \to (l,m)} < power_{s \to (l,m)}\right\} \quad (7)$$

$$W_{DSDV} = \{s, d, r, pl\} \quad (8)$$

$$P_{s \to r} = \left\{(l,m) \middle| power_{s \to r \to (l,m)} < power_{s \to (l,m)}\right\} \quad (9)$$

W_{AODV}: Network system of AODV, W_{DSDV}: Network system of DSDV, s: Source node, *d*: destination node, *r*: relay node, *pl*: path loss, *P*: Path

The equation mentioned above states that whenever the data packets are routed in a particular network starting from the source node to any arbitrary point *(l,m)* than the required power for direct transmission of data packets from source to relay node is greater than the power required for indirect transfer of data packets. If the path experiences any link failure than the above equation can be modified as Eq. (10) and Eq. (11):

$$P_{s \to in \to pl} = \left\{(l,m) \middle| power_{s \to r \to pl \to (l,m)} < power_{s \to (l,m)}\right\} \quad (10)$$

$$Data\_Packets_s > Data\_packets_d \quad (11)$$

$Data\_Packets_s$: Data Packets at source node,$Data\_Packets_d$: Data packets at destination node

As the obstruction occurs in the data packet transmission knowledge based learning algorithm is acknowledged providing the equations as follows:

$$W' = \{s, d, r_n\} \quad (12)$$

$$s = \{s_{t1}, s_{t2}, \ldots\ldots\ldots\ldots s_{tn}\} \quad (13)$$

$$d = \{d_{t1}, d_{t2}, \ldots\ldots\ldots\ldots d_{tn}\} \quad (14)$$

$$r_1 = \{r_{t11}, r_{t12}, \ldots\ldots\ldots\ldots r_{t1n}\} \quad (15)$$

$$r_2 = \{r_{t21}, r_{t22}, \ldots\ldots\ldots\ldots r_{t2n}\} \quad (16)$$

$$r_N = \{r_{tN1}, r_{tN2}, \ldots\ldots\ldots\ldots r_{tNn}\} \quad (17)$$

The above stated equations, Eq. (12) to Eq. (17) provides the information about the mobility samples at distinct instant of time. Through these mobility samples the behaviour of every node is scrutinized, henceforth, allotment of relay number on respective node is accomplished. If range of relay number is between 1 to 10, 'R' represents Relay Number: $1 \leq R \leq 10$

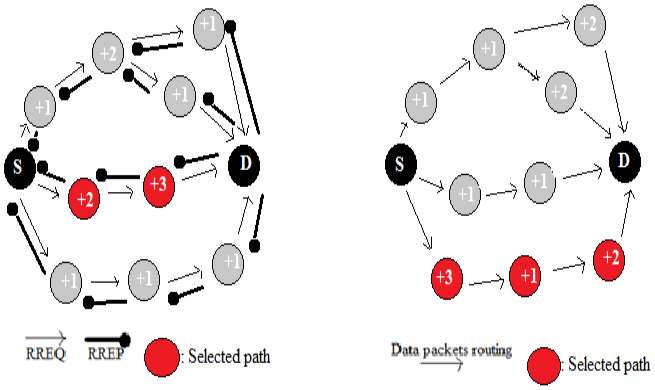
If Rs, Rd, Rr represent relay number at source node, destination node and relay node, then, the relay number of each relay node is given as follows:

$$R_1 = \sum(R_s + R_d + R_{r1}) \quad (18)$$
$$R_2 = \sum(R_s + R_d + R_{r2}) \quad (19)$$
$$R_N = \sum(R_s + R_d + R_{rN}) \quad (20)$$

Eq. (18) to Eq. (20) is the average sum of relay number which is linked in the path of relay node r_1, r_2 up to i_n. As discussed prior that mobility and relay number of respective node possess an inverse relation therefore one can conclude that increase in mobility would result in decrease of relay number. The mathematical formulation is given as follows:

If
$R_1 > R_2$
Then
$M_1 < M_2$
M_1: Mobility at node 1
M_2: Mobility at node 2

Below shows the schematic representation of the discussed scenario and the considered routing protocols are AODV, DSDV. In Fig 1 the red colored nodes are the selected path nodes because they possess highest average relay number hence least mobility.



(a) AODV **(b) DSDV**

Fig. 1. Relay number allocation.

The application of knowledge based learning algorithm is shown in Fig. 1(a) and 1b) where the most reliable path is selected as the path that consists of highest average relay number. More the relay number less would be the energy exhaustion of node, which enables the sustainable routing of data packets leading in reduction of link failure possibilities. The work is further extended by intrusion of certain foreign attacks over the network system; malicious and black hole attack.

A black hole attack is one of the foreign attacks on the network setup where disorientation happens due to the false reply from the tampered node. In such attack the affected route acknowledges a false reply (RREP) to the source node after achieving route request (RREQ) from the adjacent node. This reply mistakenly assumes to be genuine, henceforth, leading in the construction of false network maintenance. If W_B is considered as the network system that is affected by the black hole attack than the equations are modified as follows given in Eq. (21) to Eq. (28):

$$W_{B(AODV)} = \{s, d, r, B\} \quad (21)$$

$$W_{B(DSDV)} = \{s, d, r, B\} \quad (22)$$

Here *B*: Black hole node

$$s = \{s_{t1}, s_{t2}, \dots\dots\dots\dots s_{tn}\} \quad (23)$$

$$d = \{d_{t1}, d_{t2}, \dots\dots\dots\dots d_{tn}\} \quad (24)$$

$$r_1 = \{r_{t11}, r_{t12}, \dots\dots\dots\dots r_{t1n}\} \quad (25)$$

$$P_{s\to r} = \{(l,m) | power_{s\to r\to(l,m)} < power_{s\to(l,m)}\} \quad (26)$$

If $r \in B$

Then

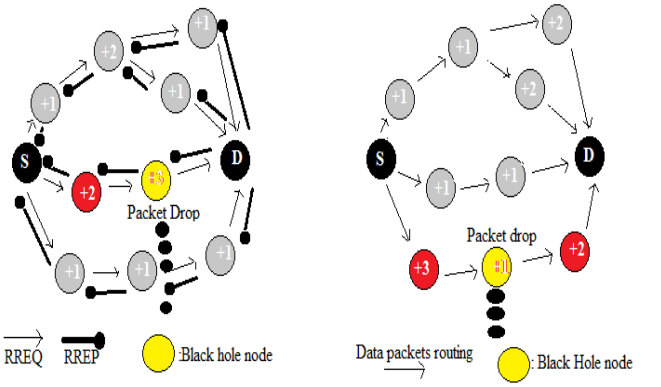
$$W_{B(AODV)} \notin \{d\} \quad (27)$$

$$W_{B(DSDV)} \notin \{d\} \quad (28)$$

Therefore, the final selected path W_B is:

$$W_{B(AODV)} \in \{s, d, r\} \quad (29)$$

$$W_{B(DSDV)} \in \{s, d, r\} \quad (30)$$



(a) AODV protocol **(b) DSDV protocol**

Fig. 2. Introduction of black hole node.

The above shown Fig. 2 (a) and 2(b) shows the loss of data packets as node of the selected path is affected by black hole attack. It would not only lead in the destruction of data packets routing but also in the performance degradation.

Performance parameters are adversely affected due to the loss of data packets, such as, throughput, overhead, packet delivery ratio and further more.

Another network setup is considered where instead of black hole attack the network is affected by malicious attack. Malicious attack is slightly different from black hole attack as it would impede the communication between nodes and inhibits the transmission of data packets. If W_M represents the network setup suffering from malicious attack than the equation would be modified as given in Eqs. (31) and (32)

$$W_{M(AODV)} = \{s, d, r, M\} \quad (31)$$

$$W_{M(DSDV)} = \{s, d, r, M\} \quad (32)$$

M: Malicious node

$$s = \{s_{t1}, s_{t2}, \ldots\ldots\ldots\ldots s_{tn}\} \quad (33)$$

$$d = \{d_{t1}, d_{t2}, \ldots\ldots\ldots\ldots d_{tn}\} \quad (34)$$

$$r_1 = \{r_{t11}, r_{t12}, \ldots\ldots\ldots\ldots r_{t1n}\} \quad (35)$$

$$P_{s\to r} = \{(l,m) | power_{s\to r\to(l,m)} < power_{s\to(l,m)}\} \quad (36)$$

If $r \in M$

Then

$$W_{M(AODV)} \notin \{d\} \quad (37)$$

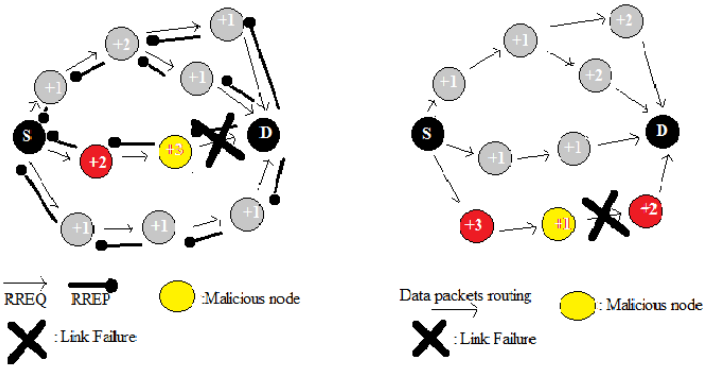
$$W_{M(DSDV)} \notin \{d\} \quad (38)$$

Therefore, the final selected path Q_M is given by Eq. (33):to Eq. (38)

$$W_{M(AODV)} \in \{s, d, r\} \quad (39)$$

$$W_{M(DSDV)} \in \{s, d, r\} \quad (40)$$

Figures 3(a) and (b) show the intrusion of malicious node in the network system. It not only degrades the performance of the system but also leads in the loss of the most reliable path. This loss would deduce the throughout, PDR, overhead and several other performance factors.



(a) AODV protocol **(b) DSDV protocol**

Fig. 3. Introduction of malicious node.

4. Results and analysis

4.1. Simulation tool and scenario

The proposed is carried out on NS2 (Network Simulator) on Linux (Ubuntu 12.04) operating system. The performance parameter values are achieved from awk scripts.

4.2. Performance parameters

Throughput: It measures the rapid transmission of data through network. It seems that bandwidth and throughput are similar, but in real, they are different. If *X* bps is the transmitted data but in actual only *Y* bps is transmitted than *Y* bps is said to be the throughput where, *Y*<*X*. Throughput is given in as: -

$$Transmission\ Time = \frac{File\ Size}{Bandwidth} \tag{41}$$

$$Throughput = \frac{File\ Size}{Transmission\ Time} \tag{42}$$

Packet Delivery Ratio: It is defined as the ratio of summation of total received packets to the summation of sent data packets. It is the measure of the loss of data packets when transmitted from origin to destination. PDR is given as

$$PDR = \frac{\sum Totalnumberofreceivedpackets}{\sum Totalnumberofsentpackets} \tag{43}$$

In our proposed work the simulation is performed by using NS2 tool (Network Simulator) in Ubuntu 12.04. Simulation parameters and specifications are as follows:

Table 1. Simulation parameters.

Simulation Parameters	Specification (12 nodes)	Specification(24 nodes)
Simulation time for ideal case	1 m 10 s	1m 34s
Simulation for malicious case	1 m 24 s	.1m 30s
Simulation time for black hole case	1 m 5 s	1m
Channel type	Wireless channel	Wireless channel
Antenna model	Omni directional	Omni directional
Radio propagation model	Two ray ground	Two ray ground
Number of nodes	12	24
Number of malicious node	1	1
Number of black hole node	1	1
Number of packets	50	50
Traffic type	CBR	CBR
Routing Protocol	AODV	DSDV

Simulation results: The results are given as follows which are attained by using compatible awk scripts. Table 2 and 4 represents the scenario of varying number of nodes under AODV routing protocol whereas Table 3 and 5 represents for DSDV routing protocol. The approach for each case is different as AODV is reactive routing whereas DSDV is proactive routing.

Table 2. Throughput and PDR for 12 nodes network system (AODV).

Parameters	Ideal case	Malicious case	Black Hole attack
Average Throughput (kbps)	274.50	176.45	145.86
PDR (Packet Delivery Ratio)	0.919235	0.69567	0.27454

Table 3. Throughput and PDR for 12 nodes network system (DSDV).

Parameters	Ideal case	Malicious case	Black Hole attack
Average Throughput (kbps)	121.55	97.23	65.57
PDR (Packet Delivery Ratio)	0.74345	0.40677	0.16357

Table 4. Throughput and PDR for 24 nodes network system(AODV).

Parameters	Ideal case	Malicious case	Black Hole attack
Average Throughput (kbps)	449.3	278.02	175.31
PDR (Packet Delivery Ratio)	0.954368	0.732756	0.35691

Table 5. Throughput and PDR for 24 nodes network system(DSDV).

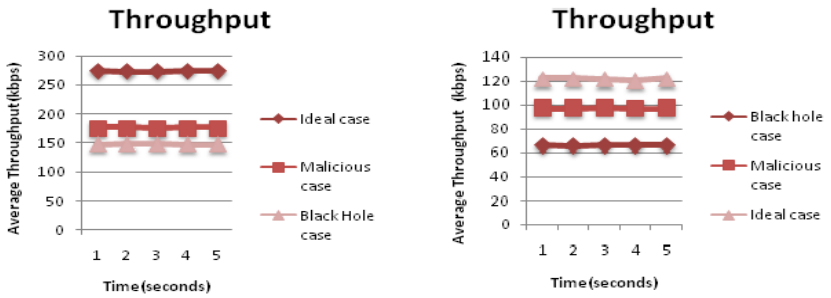
Parameters	Ideal case	Malicious case	Black Hole attack
Average Throughput (kbps)	275.39	146.41	87.48
PDR (Packet Delivery Ratio)	0.786739	0.563268	0.21027

By the given mentioned values one can easily conclude that with the increase in number of nodes, the increase in throughput as well as PDR is seen irrespective of the type of routing protocol applied. More the number of nodes more will be the throughput and PDR. But if the comparison is made between AODV and DSDV routing than the values attained in AODV is greater in comparison with the values attained in DSDV. Therefore, we can conclude that AODV is an efficient routing algorithm in comparison with DSDV. The graphical representation of the above mentioned values are given as follows.

Tables 2 and 4 represents the scenario of varying number of nodes under AODV routing protocol whereas Table 3 and 5 represents for DSDV routing

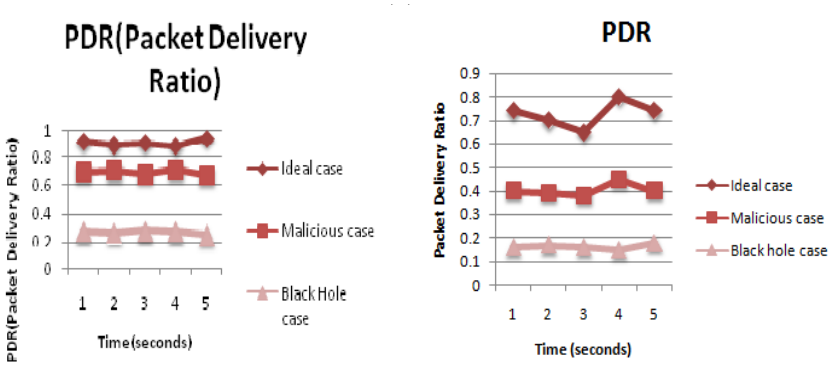
protocol. The approach for each case is different as AODV is reactive routing whereas DSDV is proactive routing.

Figures 4(a) and (b), Figs. 5(a) and (b), Figs. 6(a) and (b), Figs. 7(a) and (b) display the outcome achieved by varying number of nodes (12, 24) and the performance comparison is made on the basis of throughput and packet delivery ratio. Fig. 4(a) and 4(b), 5(a) and 5(b) provide the values of throughput and PDR in 12 nodes network system which is much less in comparison with 24 nodes network, as given in Fig. 6(a) and 6(b), 7(a) and 7(b). This is due to the inclusion of nodes which increase the throughput and PDR. Moreover, the value in AODV routing is much greater than DSDV because the AODV possess much more routing data packets by avoidance of looping. On the other side, DSDV is a table driven routing protocol which would not allow greater data packets to route in comparison with AODV. The comparison of AODV and DSDV performance is showcased in Figs. 4(a) and (b), Figs. 5(a) and (b), Figs. 6(a) and (b), Figs. 7(a) and (b) where (a) corresponds to AODV and (b) corresponds to DSDV.



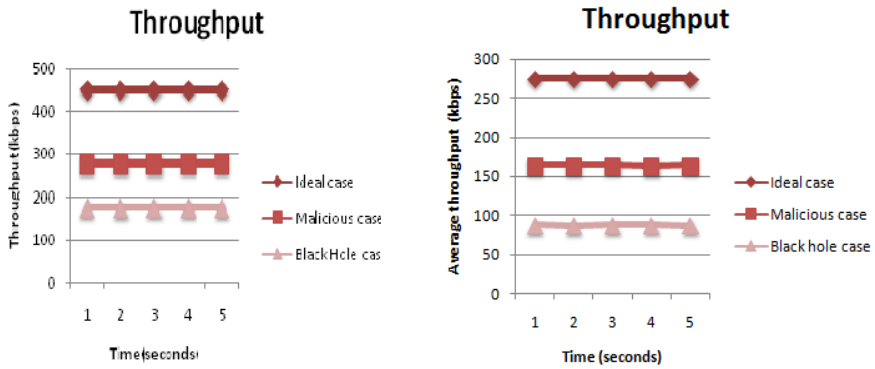
(a) AODV protocol **(b) DSDV protocol**

Fig. 4. Average throughput (12 nodes).



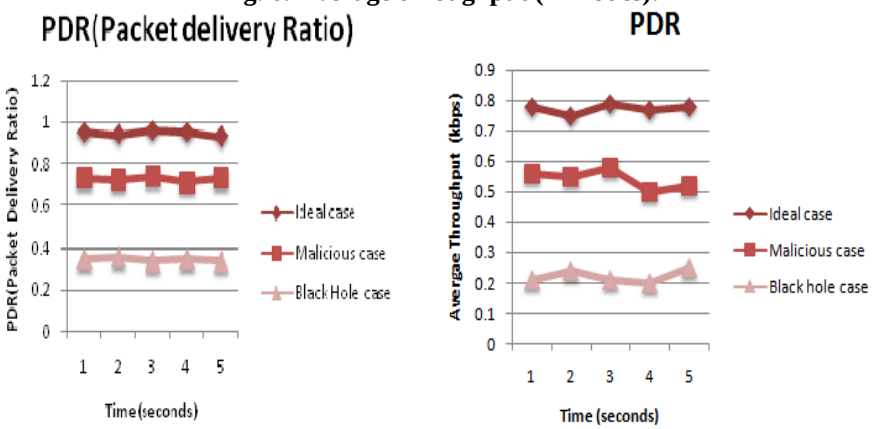
(a) AODV protocol **(b) DSDV protocol**

Fig. 5. Packet delivery ratio (12 nodes).



(a) AODV protocol **(b) DSDV protocol**

Fig. 6. Average throughput (24 nodes).



(a) AODV protocol **(b) DSDV protocol**

Fig. 7. Packet delivery ratio (24 nodes).

5. Conclusion

In the presented paper, performance of network system is assessed on the basis of throughput and packet delivery ratio. Furthermore, comparison of these parameters is made by using different routing protocols (AODV, DSDV). The primary focus of the paper is per node analysis instead of per flow analysis. Knowledge based learning aids in determination of the most stable or reliable path by the parameter Relay number which possess an inverse relation with mobility of node. Moreover, the reliable path is tempered by malicious and black hole attack so as to analyse the network environment under adverse conditions; the loss of data packets and link failure. Finally, by the attainment of best reliable path under favourable and adverse conditions it can be concluded that AODV routing protocol is the preferable routing protocol in comparison with DSDV. Due to its dynamicity and loop avoidance approach towards routing of data made it more feasible and reliable. Irrespective of the number of nodes in the network setup AODV provides better results in comparison with DSDV.

References

1. Aggarwal, S.; Ahuja, A.; Singh, J.P.; and Shorey, R. (2000). Route lifetime assessment based routing protocol for mobile adhoc networks. *Proceedings of First International Conference on Communications.* New Orleans, LA, 1697–1701.
2. Dube, R.; Rais, C.D.; Wang, K.Y.; and Tripathi, S.K. (1997). Signal stability based adaptive routing for ad-hoc mobile networks. *IEEE Personal Communications*, 4(1), 36-45.
3. Su, W.; Lee, S.J.; and Gerla, M. (2001). Mobility prediction and routing in ad hoc wireless networks. *International Journal of Network Management*, 11(1), 3-30.
4. Jones, C.E.; Sivalingam, K.M.; Agrawal, P.; and Chen, J.C. (2001). A survey of energy efficient network protocols for wireless networks. *Wireless Networks*, 7(4), 343-358.
5. Ali, A.H. (2013). Centrally Coordinated power aware route selection for MANET. *Proceedings of International Conference on Open Source Systems and Technologies*, Lahore, Pakistan, 87-90.
6. Tseng, Y.C.; Li, Y.F.; and Chang, Y.C. (2003). On route lifetime in multihop mobile adhoc networks. *IEEE Transactions on Mobile Computing*, 2(4), 366-376.
7. Basarkod, P.I.; Manvi, S.S.; and Albur, D.S. (2014). Mobility based estimation of node stability in MANETs. *Proceedings of International Conference on Emerging Trends in Computing, Communication and Nanotechnology* , Tirunelveli, India, 126-130.
8. Sarkar, S.; and Adamaou, M. (2003). A framework for optimal battery management for wireless nodes. *Proceedings of 21st Annual Joint Conference of the IEEE journal on selected areas in communications*, 21(2),179-188.
9. De Couto, D.S.J.; Aguayo, D.; Bicket, J.; Morris, R. (2003). A high throughput path metric for multi-hop wireless routing. *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, San Diego, USA, 134-146.
10. Muthuramalingam, S.; Janani, P.; Bavya, B.; and Rajaram R. (2009*).* An energy conserving topology maintenance algorithm for MANET. *Proceedings of First International Conference on Network and Communications*, Chennai, India, 101-106.
11. Chiasserini, C.F.; and Rao, R.R. **(**2001). Energy efficient battery management. *IEEE journal on selected areas in communications*, 19(7), 1235-1245.
12. Rodoplu, V.; and Meng, T.H. (1999). Minimum energy mobile wireless network. *IEEE Journal on selected areas in communication*, 17(8), 1333-1344.
13. Forman, G.H.; and Zahorjan, J. (1994). The challenges of mobile computing. *Journal Computer*, 27(4), 38-47.
14. Kahlid, S.; and Mehboob, A. (2003). Design and implementation of ID based MANET auto-configuration protocol. *International Journal of Communication Networks and Information Security*, 5(3),141-151.
15. Ghouti, L.; Sheltami, T.R.; and Alutaibi, K.S. (2013). Mobility prediction in mobile adhoc networks using extreme learning machines. *Procedia Computer Science Journal*, 19(2), 305-312.