Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.469 – 480

RESEARCH ARTICLE

Ant Colony Optimization Based Approach for the Detection of Black Hole Attack in WANET

Er. Navdeepak Kumar[#1], Er. Lipsa Walia[*2]

[#1]M.Tech Scholar, Electronics and Communication Department, RBIEBT, Mohali
Makkarnavdeepak@yahoo.com
[#2]Assistant Professor, Electronics and Communication Department, RBIEBT, Mohali
Walia_lipsa@yahoo.co.in

ABSTRACT: ***Wireless Ad Hoc Networks (WANETs) are self arranged networks whose nodes are free to shift randomly while being intelligent to converse with each other not including the help of an existing network infrastructure. Due to its dynamic behavior, one of the main safety problems in ad hoc networks called the black hole attack. It takes place when a fake node referred as black hole connects the network. The black hole node conducts its fake behavior during the process of route discovery. At present, several efficient routing protocols have been proposed for WANET. Most of these protocols assume a trusted and helpful environment. However, in the existence of malicious nodes, the networks are vulnerable to different kinds of attacks. In this paper we apply Dynamic Source Routing (DSR) and Optimized Link State Routing (OLSR) Protocols. The objective of this work is to design and implement OSLR and DSR protocol with Black hole attack and prevent the system from threat using Ant Colony Optimization with both protocols. The simulation is carried on MATLAB and the simulation results are examined on various network performance metrics such as bit error rate, throughput, end-to-end delay and packet delivery ratio.***

KEYWORDS: WANET, OLSR, DSR, Attacks, Routing Protocols.

1. INTRODUCTION

WANET, mutually with the behind information regarding network situation, is called a Routing Protocol. Wireless communication is a rising new technology that allows the users to access information and services automatically despite of their biological position. However, similar to other networks, WANET also vulnerable to many security attacks. WANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself. In WANET, security is a challenging issue due to the vulnerabilities that are associated with it [4].

Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes. The ranges of attacks that can be mounted on WANETs are also wider than in case of conventional static networks. In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network [11]. As a matter of fact, the boundary of the network is not properly defined. Nodes can intermittently come into the network or leave it. Moreover malicious nodes can flood the network with junk packets hampering the network service or intentionally drop packets. But these nodes can but these nodes can subtly manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious [9]. A wireless ad hoc network is a de-centralized type of wireless network. The net is ad hoc since it does not rely on a pre existing communications.

2. ROUTING IN WANET

Routing Protocol is second hand to find suitable routes between communicate nodes. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link [6]. Since the nodes are mobile, the network topology may change unpredictably over time. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes [2]. WANET routing protocols could be broadly secret into three major categories: Proactive, Reactive and Hybrid Routing Protocols.

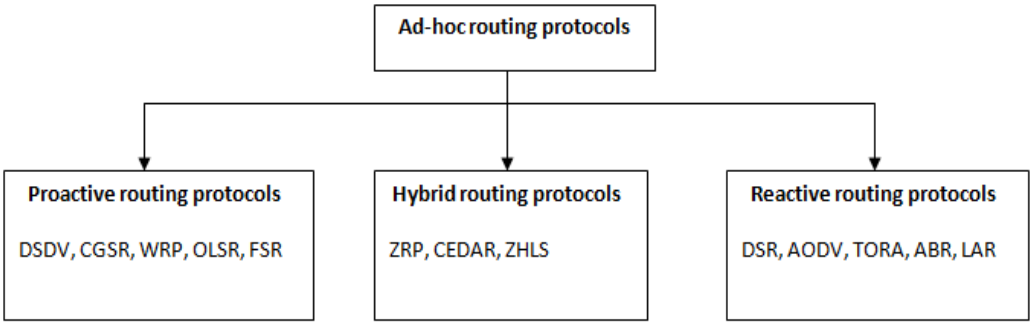

Figure 1: Classification of routing procotols

3. PROPOSED METHOD

We have used MATLAB R2010a in our evaluation. We have selected 1000 * 1000m in OLSR and 2500*2500m in DSR as our network size and generate 50 mobile nodes in both networks. To explain the various performance metrics required for evaluation of protocols, to reiterate the black hole attack, we begin with the overview of performance parameters that includes End-to-end delay, Throughput, Bit Error Rate and Packet Delivery Ratio. The parameters have to be measured against iteration.

Table 1 Simulation parameters

Property	Value
Routing Protocols	DSR, OLSR
Area Covered(DSR)	2500*2500m
Area Covered(OLSR)	1000*1000m
Coverage Set	250m
No. of Nodes	50
Observation Parameters	Throughput, End-to-End Delay, Bit Error Rate ,Packet Delivery Ratio and Iteration
Network Simulation	MATLAB
Optimization technique	ACO
No. Of Iteration	10
Population Size	500

Methodology:

For the design of the research work, well known meta-heuristic: ACO i.e. Ant colony optimization is used In order to optimize the energy, OLSR and DSR are used and their comparisons are used through routing.

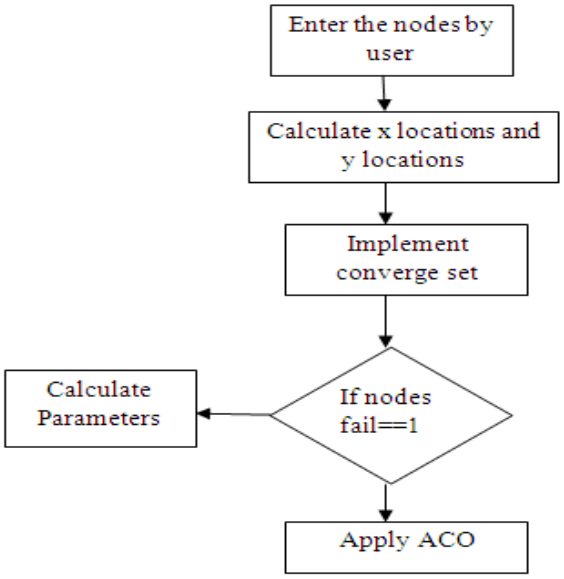

Figure 1: Evaluation of DSR

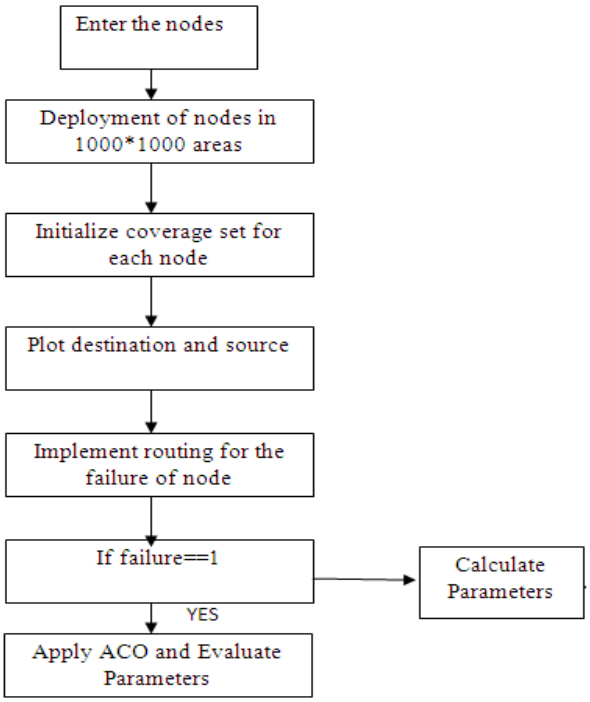

Figure 2: Evaluation of OLSR

4. RESULTS

The Result part is divided into two parts for two different protocols DSR and OLSR and finally their results have been analyzed in tabular form in table.

A. DSR RESULTS

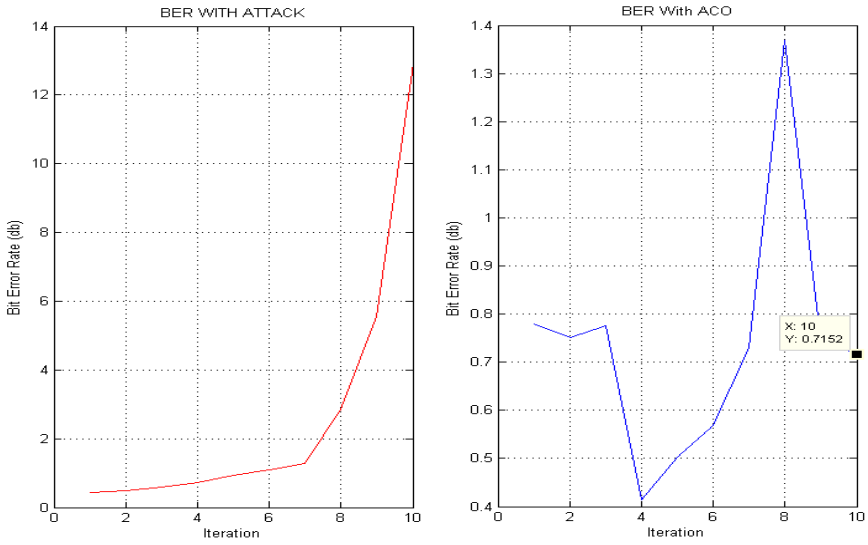

Figure 3: Comparison w.r.t BER

In Figure 3 shows the comparative relation of bit error rate in the presence of black hole attack and with optimization using ant colony optimization algorithm and shows that bite error measure is less with optimization as compared to the effect of attack in the network. This measure should be less for the efficient network.

In Figure 4 shows the throughput measure with attack and after optimization and shows that this measure is having high throughput after optimization. The throughput is defined as the network performance with the successful delivery of the packets from source to the destination in an efficient manner.

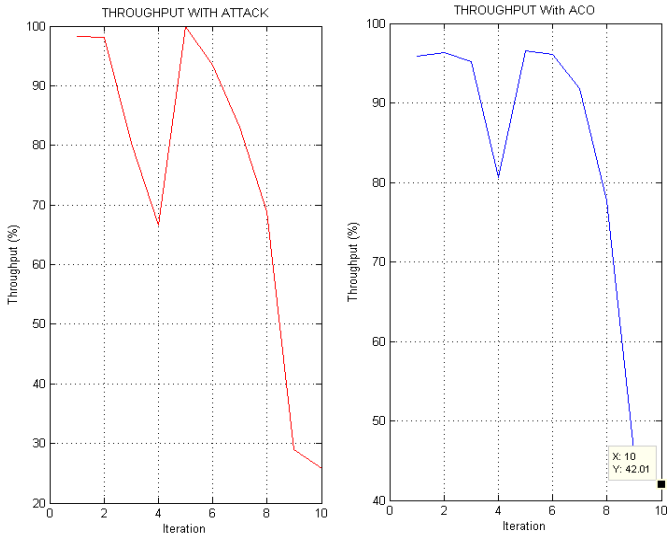

Figure 4: Comparison w.r.t. throughput

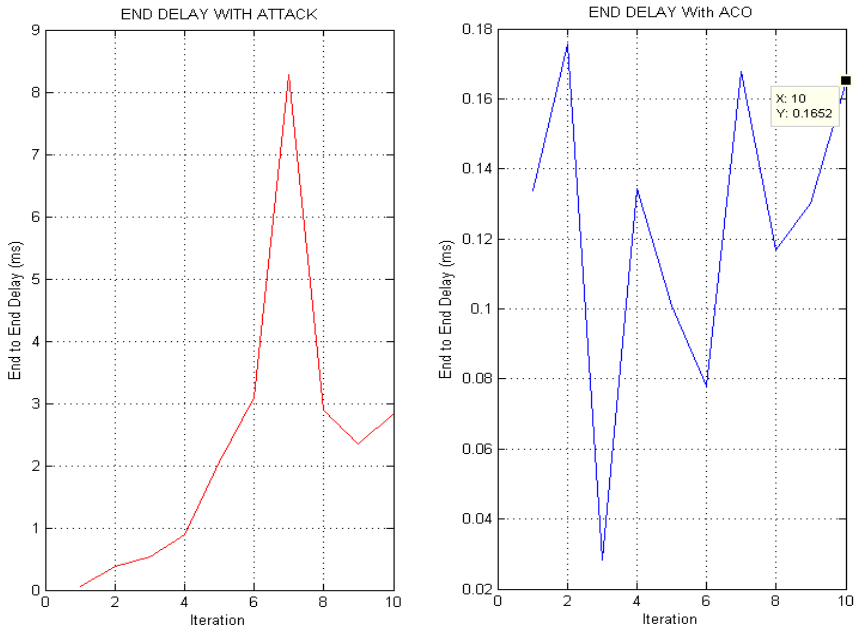

Figure 5 : Comparison w.r.t to End to End Delay

In Figure 5 shows the End to End delay measure with attack and after optimization and shows the packets are delivered in less interval of time to increase the network lifetime. The end delay is defined as the amount of packets received to the destination in fewer intervals of time with less error rate.

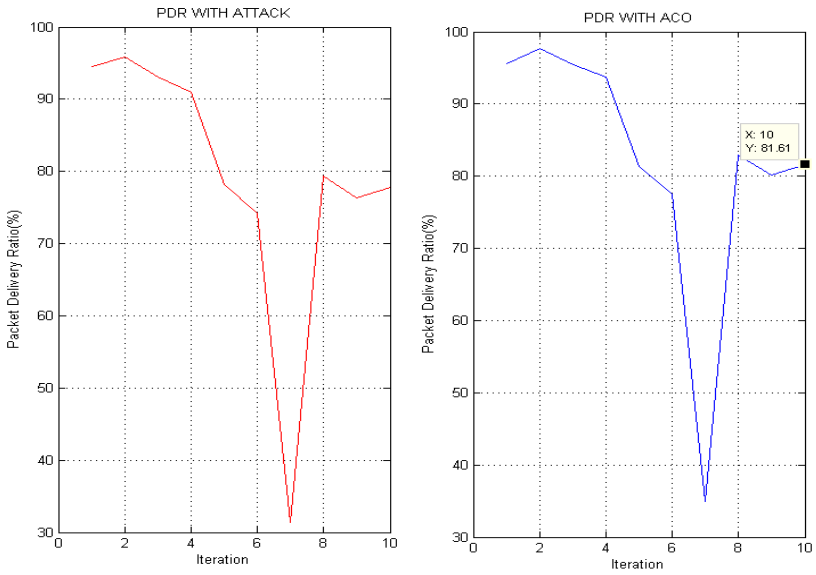

Figure 6: Comparison w.r.t PDR

Figure 6 shows the packet delivery rate in the presence of black hole attack and after optimization with ant colony optimization and shows that the more packets are delivered in efficient manner. The packet delivery rate is defined as the amount of packets successfully received to the destination node and the result graph of DSR shows that the 15% more packets are delivered than the network in the presence of attack.

B. OLSR PROTOCOL RESULTS

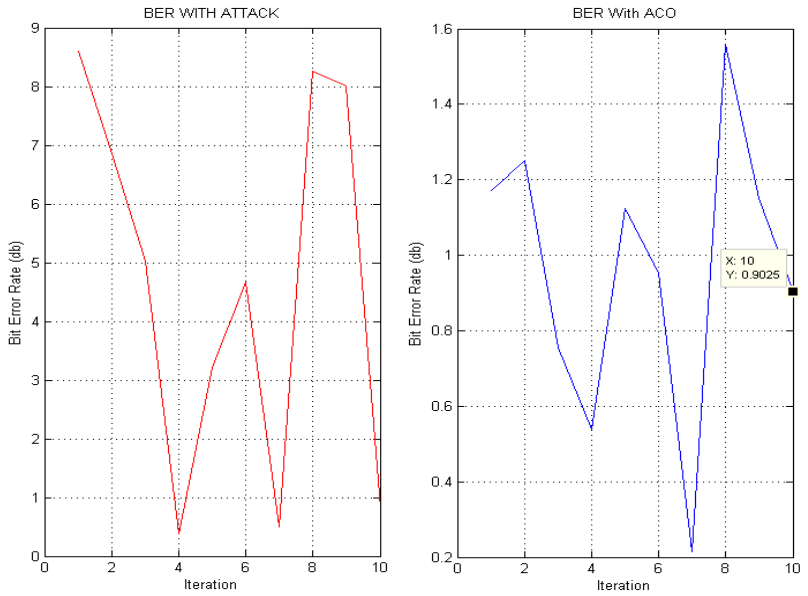

Figure 7: Comparison w.r.t BER

The above Figure 7 shows the comparative relation of bit error rate in the presence of black hole attack and with optimization using ant colony optimization algorithm in optical link state routing protocol and shows that the bit error rate is having maximum BER with attack is 8.26 db and after optimization the maximum BER value is 1.55db.

Figure 8 show the throughput measure using black hole attack and after optimization using ant colony optimization and this measure should be high for the appropriate working of the output. The result figure shows throughput of OLSR with ACO improves the Results. After applying the ACO in OLSR the results are 54% more efficient.

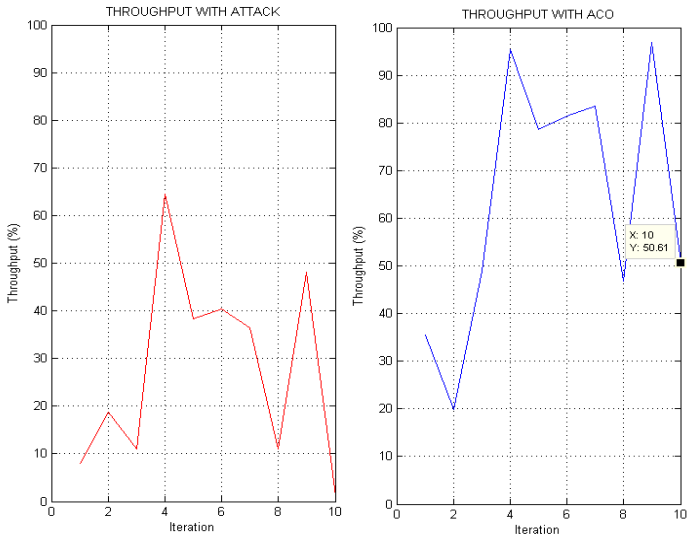

Figure 8: Comparison w.r.t Throughput

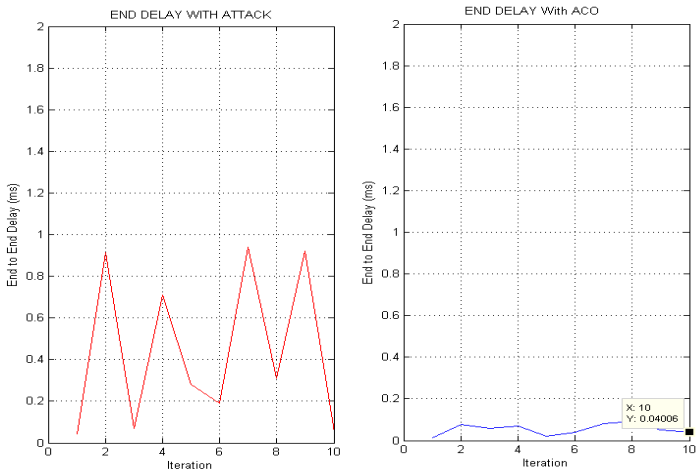

Figure 9: Comparison w.r.t End to End Delay

Figure 9 shows the End to End delay measure with attack and after optimization using ant colony optimization in link state routing protocol and shows the delivery of packets in an efficient manner in short interval of time to increase the network lifetime. ACO improves the results up to 69% that is very effective improvement for a protocol.

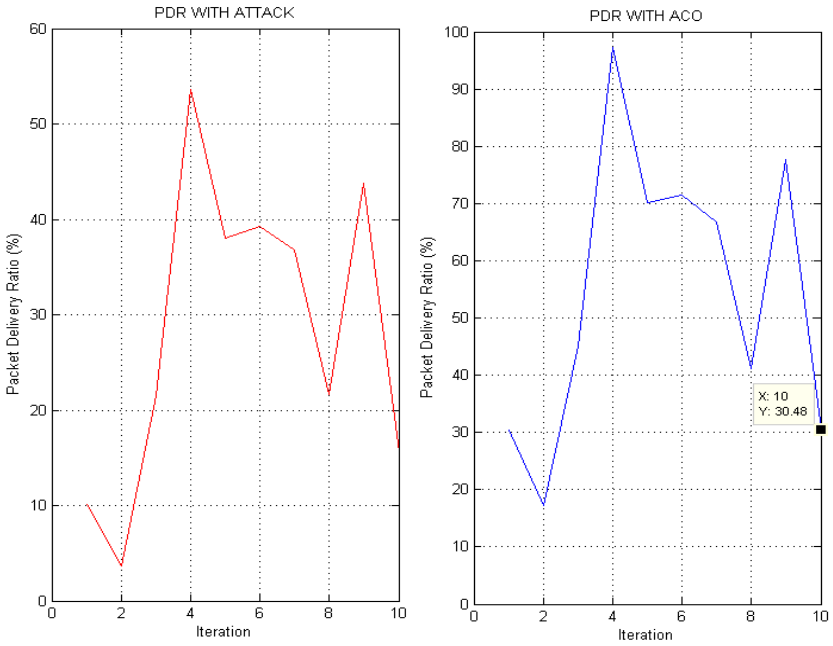

Figure 10: Comparison w.r.t PDR

The above Figure 10 shows the packet delivery rate in the presence of black hole attack and after optimization with ant colony optimization in the optimal link state routing protocol and shows that the 10 % packets are delivered in the presence of attack and using ACO the measure is 95 % which shows the effect of optimization to increase the lifetime of the network.

C. COMPARISON OF DSR AND OLSR ROUTING PROTOCOL USING ACO

In table 2 we have compared the average values of DSR and OLSR with ACO. In this we have used the four different no. of nodes 50, 60, 70 and 80, then we count the average value of all four parameters with 10 iterations for those nodes. At last the proactive and reactive routing protocols parameters with their nodes have been compared.

Table 2 Comparison of simulation Results

PARAMETERS	No. of Nodes							
	50		60		70		80	
	DSR	OLSR	DSR	OLSR	DSR	OLSR	DSR	OLSR
Throughput	78.72	58.83	79.88	62.42	88.84	46.73	80.68	37.18
End-to-End Delay	0.133	0.064	0.124	0.049	0.151	0.064	0.110	0.052
Bit Error Rate	0.763	1.044	0.808	3.984	0.499	1.003	0.867	1.133
Packet Delivery Ratio	86.69	51.48	66.46	53.39	76.47	41.94	75.06	38.27

For throughput on 50, 60, 70 and 80 no. of nodes the DSR performs 25%, 21%, 47% and 53% better results than the OLSR. Overall DSR gives 36% improved results.

For end-to-end delay on 50, 60, 70 and 80 no. of nodes the OLSR shows 51%, 60%, 57% and 52% better results than DSR. Overall OLSR shows 50% better performance. So DSR has high delay.

For bit error rate on 50, 60, 70 and 80 no. of nodes the DSR results 27%, 79%, 50% and 23% improved than OLSR. DSR have 44% faster bit error rate.

For packet delivery ratio on 50, 60, 70 and 80 no. of nodes the DSR shows 41%, 19%, 45% and 49% better performance than OLSR. The DSR deliver packets 34% faster.

5. CONCLUSION AND FUTURE SCOPE

The simulation results show that when the black hole node exists in the network, it can affect and decrease the performance of OLSR and DSR routing protocol which can be optimized by using ACO optimization algorithm. By using ACO, the performance parameters are showing better results.

In summary table 2 we have compared the average values of parameters on 50, 60, 70 and 80 nodes. Based on the research and Analysis of experimental result the drawn conclusion is that for the throughput, bit error rate and packet delivery ratio, DSR behaving much better and as far as end to end delay is concerned OLSR is taking less delay.

So, the detection and prevention of black hole attack in the network exists as a challenging task.

As future work, we intend to simulate and analyze the effect of the black hole attack in other routing protocols and can use ACO for better path detection with max-min optimization. There are many more other optimization techniques which performs better in future like GA, PSO, BCO, FSO etc. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior can be carried out for further research.

REFERENCES

[1]. K. Devi et.al," Energy Efficient Path Determination in WANET", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2015.

[2].ShailyGoyal," A review on routing protocols based on zone mechanism for wanet",International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 2, Issue 11, November 2013.

[3]. Mansuri Anwar Mohd, Khan Mohd Imran, Sheikh Heena," Mobile Ad-Hoc Networks Extensions to Zone Routing Protocol", Vol. 2, Issue 5 September 2011, IJCST.

[4].Nogueira, Michele, et al. A security management architecture for supporting routing services on WANETs." Network and Service Management, IEEE Transactions on 9.2 (2012): 156-168.

[5].Goyal, Shaily, and Vinay Kumar Nassa. "A REVIEW ON ROUTING PROTOCOLS BASED ON ZONE MECHANISM FOR WANET."

[6].Shendre, Ashwini, and P. S. Mohod. "Using SG-PKM Improve security mechanism for Supporting Routing Services on WANET." International Journal of Computer Science & Information Technologies 5.4 (2014).

[7].Vishwakarma, MsDharmistha D. "Method of Performance Evaluation of WANET Using NS-2."

[8].Malkeet Singh, et al. "A survey of routing attacks in mobile ad hoc networks." Wireless communications, IEEE 14.5 (2007): 85-91.

[9].Singh, Suresh. "Challenges: wide-area wireless Networks (WANETs)."Proceedings of the 14th ACM international conference on Mobile computing and networking. ACM, 2008.

[10].Patil, Prachee N., and Ashish T. Bhole. "Black hole attack prevention in mobile Ad Hoc networks using route caching." Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on. IEEE, 2013.

[11].JaydipSen, SripadKoilakonda, ArijitUkil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks" in Proceedings of the 2nd International Conference on Intelligent Systems, Modeling and Simulation IEEE, 2011.

[12].LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET", 2nd International Conference on WIRELESS Broadband Ultra Wideband Communication, (AUS Wireless). IEEE, 2007.

[13]. Wahane, Gayatri, and Savita Lonare. "Technique for detection of cooperative black hole attack in MANET." 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). IEEE, 2013.Zhu Xialonget.al , "A location privacy preserving solution to resist passive and active attacks in VANET", IEEE, Vol.11, pp. 60-67, 2014.

