ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 8, August 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Performance Analysis on Secure Dynamic Source Routing over Mobile Ad hoc Networks

Mehak Rani[1]
MTech Scholar
Department of Computer Engineering
Om Institute of Technology & Management,
Hisar, Haryana – India

Dr. Anuj Kumar Sharma[2]
Associate professor (CSE)
Department of Computer Science and Engineering
Om Institute of Technology & Management,
Hisar, Haryana – India

Abstract: ***In this paper, we introduced a method to identify the Black hole attack over Dynamic Source Routing Protocol. Proposed scheme starts tracing the attack symptoms, if it finds the abnormal behavior over specific route paths. NS-2 was used for simulation purpose and results show its resistance against security threat and it is able to perform under various constraints i.e. PDR, Delay, Load and Throughput etc.***

Keywords: Security, Attacks, Black Hole, Gray hole, DOS, AODV, DSR.

I. INTRODUCTION

In MANET, wireless node communicates independently and performs network operations in open environment. Wireless signals can be intercepted easily and captured data can be further utilized to trigger the malicious activities over network. Active and passive both type of attacks can be used to degrade the network performance.

Black hole attack over mobile ad hoc networks is introduced by the malicious nodes by intercepting the route request and route reply messages in the network and does not utilize the route cache data which is used for route discovery. Malicious node sends fake reply for each request whereas all other legitimate nodes use the route cache.

After receiving the reply, sender node starts transmission and after all, all packets are dropped by malicious node. Impact of black hole attack also depends upon the density of malicious nodes in the given network size and this type of attack can degrade the performance of entire network [1][2][3][4][5].

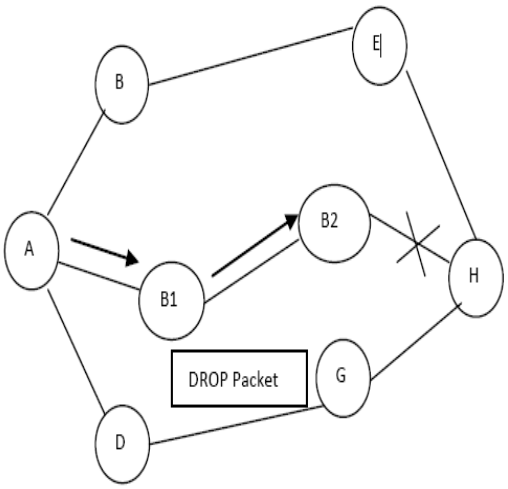

Figure 1: Black Hole Attack

II. LITERATURE REVIEW

Y. Liu et al. [6] introduced a truest based secure routing scheme for sensor networks. It supports reliable and scalable communication over network. It uses criteria of residual energy to discover multiple paths. Simulation results show its efficiency in terms of enhancing the probability of security and energy consumption.

H. Moudni et al. [7] enhanced the existing AODV routing protocol for resisting the Black hole attack over MANETs. It monitors the RREQ, RREP and Sequence numbers, if any node receives multiple control messages, it ignores the RREP messages after verification of each forwarding message. Simulation results show its performance in terms of improved PDR and minimum delay under the constraints of mobility in compromised network.

A. O. Alkhamisi et al. [8] introduced trust based secure routing for multiple paths routing over ad hoc networks. It defends against various attacks i.e. Flooding, Black hole and Gray hole attack. It analyzes control messages flow and adds trust value. Finally, Threshold statistics are used to identify the attacks. Simulation results show the its performance in terms of minimum route selection time, control overhead, trust non-utilization factor and energy efficiency etc.

H. Moudni et al. [9] investigated the impact of various attacks over the density of traffic, network size, node mobility under various performance constraints i.e. Delay, PDR and Throughput etc. Simulation results show that in case of Black hole attack, Throughput decrease where as Routing load increases. As compared to other attacks i.e. Rushing, flooding, Black hole attack has the highest impact over network performance.

S.Uma maheswari et al. [10] developed a solution to secure the network from Denial of Service attack. It can filter out the HELLO message flooding over network which can cause data transmission interruption and may result is packet loss at large scale. It offers minimum key exchange time and keeps the track of each control message exchange.

Emimajuliet.P et al. [11] presented a solution to secure the MANETs by intruders by identifying the transmission range and packet loss ratio over that particular range. Node level statistics are verified to know the most critical path which has the highest packet loss and finally, intruder over that path is discovered. Simulation results show that it can maintain network performance in the presence of malicious nodes.

Pooja et al. [12] presented a solution to detect the Black hole attack using Hint Based Probabilistic routing method under the constraint of various mobility models. Trusted authority is used to build the HINTS for each node which is participating in transmission and its HINT is compared against a predefined Threshold value, if HINT does not satisfy the Threshold value, it is marked as malicious node and hence neglected for routing purpose, finally communication is initiated using reliable and secure paths. Simulation results show that it is able to analyze the packet drop and overhead in the network and proposed solution can be further extended Black hole attack detection and removal.

J. Ponniah et al. [13] developed a protocol suit to guard the ad hoc networks from security threats. It can analyze the multiple layers and defines set of rules for each one and makes an assumption that intruder cannot intercept the data at all layers, in one attempt. It starts network tracing, when any node joins the network. It collects the node level statistics and compares it with the node's history. Statistic evaluation is used to detect the malicious node using consistency check algorithm which regulates the transmission and reception of data. It defines various models i.e. Node Model defines the terms for legitimate and malicious nodes on the basis of their states, Communication Model defines the terms for data transmission and reception and keeps the track of signal jamming also, Clock Model defines the timer for communication purpose, Key based security method assigns keys to each node which are use for secure communication, Utility function defines the Throughput rate and link rate vectors and if nay ode nodes which cannot fulfill this criteria, is not eligible for communication. Analytical analysis shows that combination of multiple features can provide the robust security for ad hoc networks.

B.Ballav et al. [14] developed a zone based routing solution to encounter the black hole attack over mobile sensor networks. It keeps the track of packet flow between base station and intermediate odes and uses acknowledgement for each packet. If node does not send ACK control packet and drops all packets, then it is identify as intruder. Simulation shows that it consumes less energy for monitoring purpose and is able to maintain the network performance under QoS constraints.

III. PROPOSED SCHEME

Proposed scheme stars traffic monitoring, only if it is essential to diagnose the network. On the basis of reasoning, decision is made to avoid that route. After blocking the route, network operates in normal environment till the detection of next node misbehavior. If there is any black hole attack, first of all intruder will alter the routing information and then acquiring the route, it will start packet drop, so all activities will be executed at same time, So we sub divide the packet drop into three different categories: Normal Packet , Packet Forwarding Drop and Unknown Packet Drop. In normal packet drop condition, packet drop may occur due to buffer over flow or due to route error but if it starts at the time when a packet is forwarded to next hop and intermediate node just drop it and after that it drops all the packets simultaneously. Thus result in the all types of packet drops i.e. Normal, forwarding and Unknown and its source can be detected using various routing attributes such as Current node index, current route length and NEXT Hop etc. Proposed scheme will trace the routes, if requested otherwise it will remain silent.

```
If (Black Hole Attack==1)
{
If (routing))
{Rl
Rl: Get Route->Length ()
I: Get Route->Index ()
N: Set Route->PKT->Drop Count (Rl, I, Normal)
F: Set Route->PKT->Drop Count (Rl, I, Forwarding)
U: Set Route->PKT->Drop Count (Rl, I, UNKNOWN)
If (N=1 && F==true && U ==true)
{For each Rl && I
TH++; Start (Trace Route (Rl, I, Node->Index);)
UpdateRouteTh (Rl, I, Node->Index);
Reasoning:
If (Th> x)
{
ignore Route (Rl, I, Node->Index); exit (Trace Route ())
}
}
}
}
```


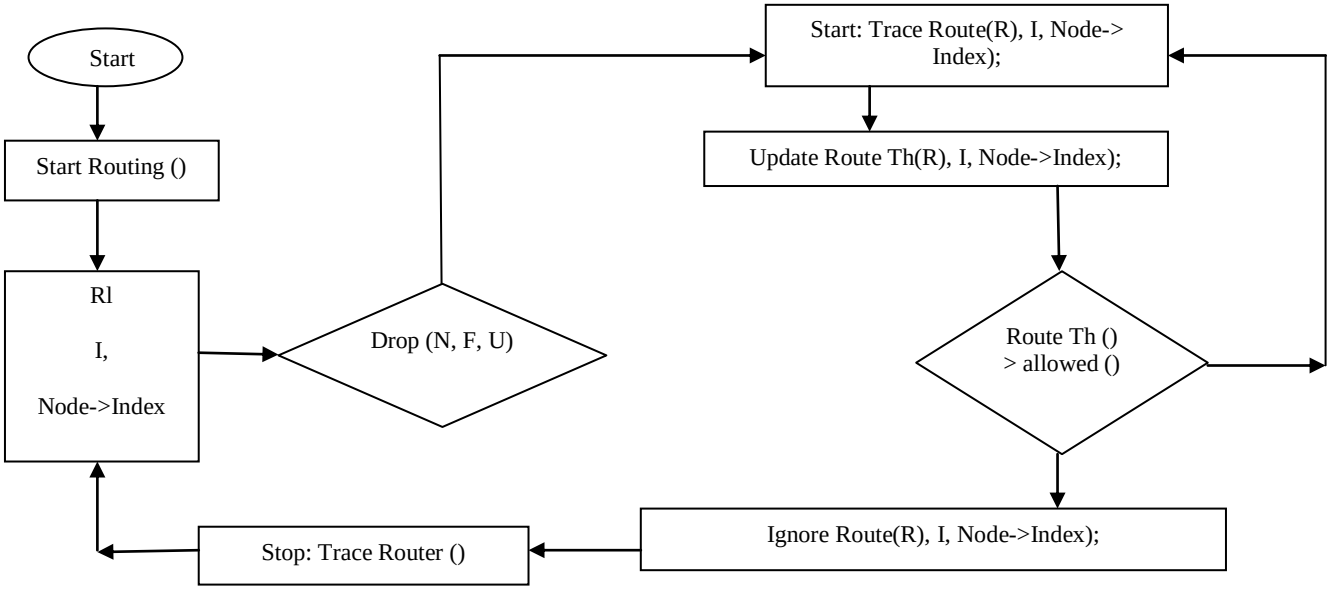

Figure 2: Proposed Scheme

IV. Simulation Analysis and Results

SIMULATION CONFIGURATION

Simulation Parameters	Values
Routing Protocol	DSR
Wireless Terrain	1200x1200
Node Density	30
MAC Protocol	MAC 802.11
Traffic Type	CBR
Packet Size	1024
Sampling Interval	0.05 seconds
Simulation Time	10 seconds
Network Simulator	NS-2.35
Simulation Scenario(s)	• Open Network Environment (NDSR) • Black hole Attack (BDSR) • Prevention Scheme (PDSR)

SIMULATION SCENARIOS

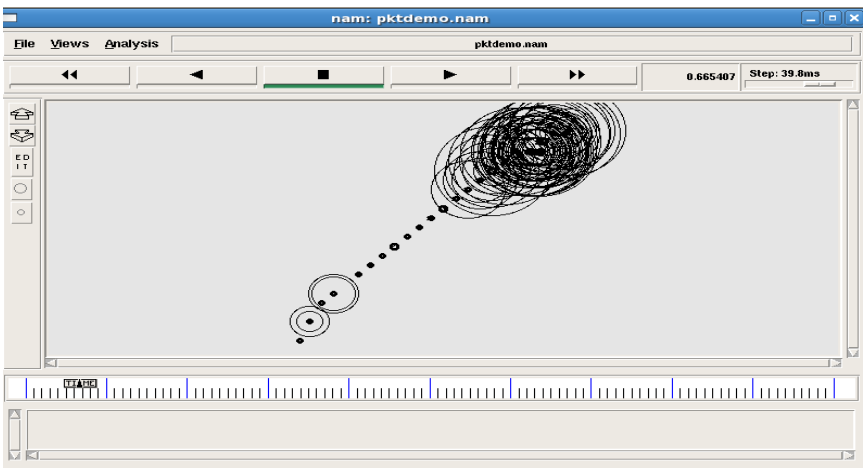

Figure 3: Simulation-Normal Network Environment (NDSR)

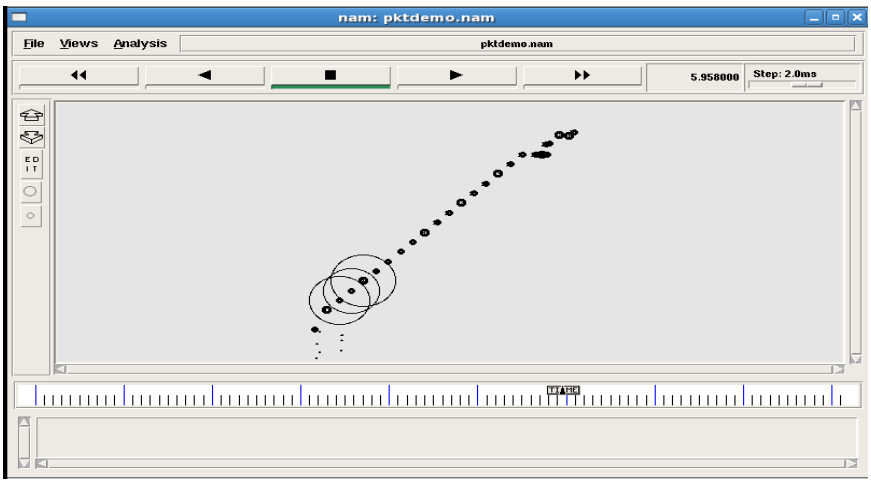

Figure 4: Simulation-Blackhole Attack (BDSR)

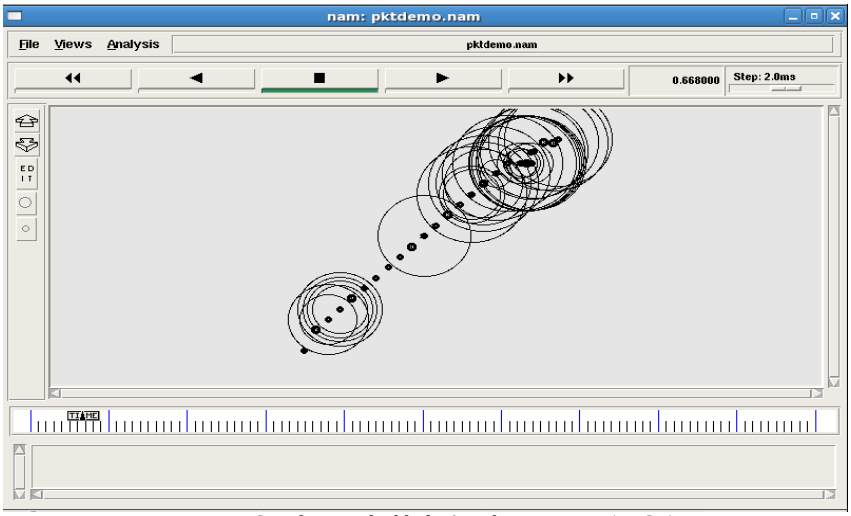

Figure 5: Simulation-Blackhole Attack-Prevention (PDSR)

PERFORMANCE ANALYSIS

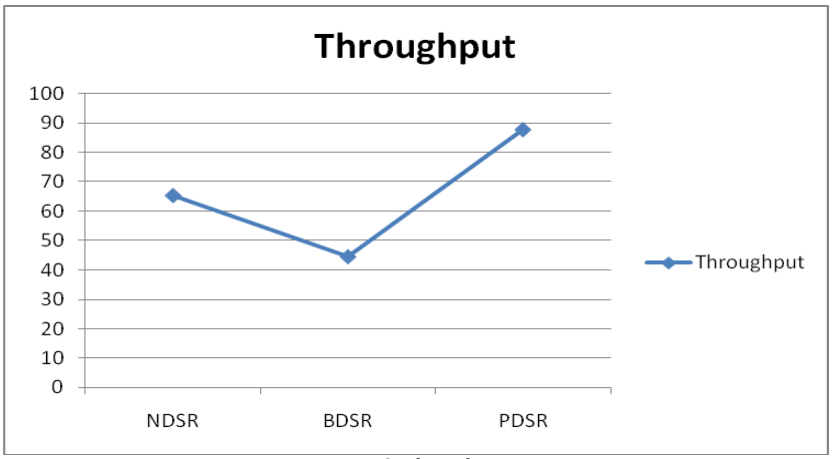

Figure 6: Throughput

Figure 6: above shows the Throughput of DSR using different scenarios i.e. In case of normal network operations (NDSR), it is 65.3 bps which is reduced up to 44.6 bps by Black hole attack (BDSR) and it is recovered by proposed scheme up to 87.6 bps.

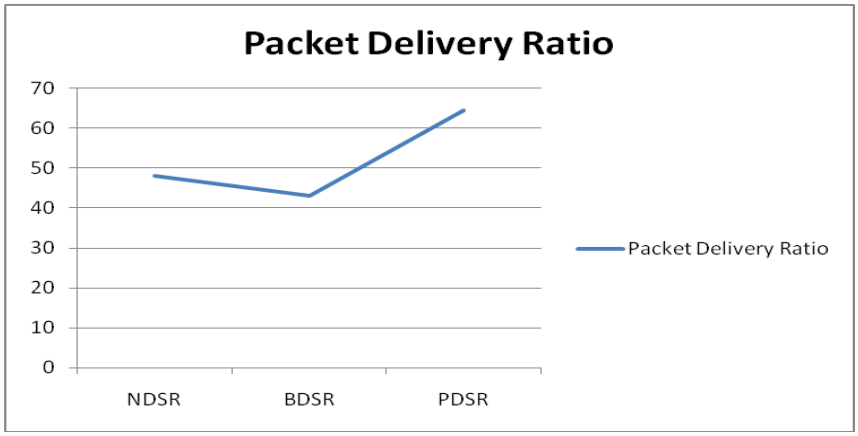

Figure 7: Packet Delivery Ratio

Figure 7: above shows the PDR of DSR using different scenarios i.e. In case of normal network operations (NDSR), it is 48.12085483 which are reduced up to 43.05019305 by Black hole attack (BDSR) and it is recovered by proposed scheme up to 64.36443791.

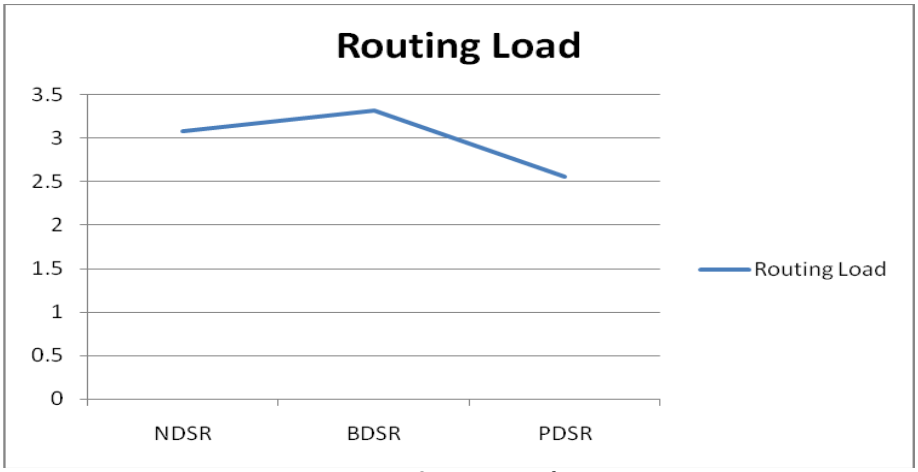

Figure 8: Routing Load

Figure 8: above shows the Routing Load of DSR using different scenarios i.e. In case of normal network operations (NDSR), it is 3.078101072 which is increased up to 3.322869955 by Black hole attack (BDSR) and it is reduced by proposed scheme up to 2.553652968.

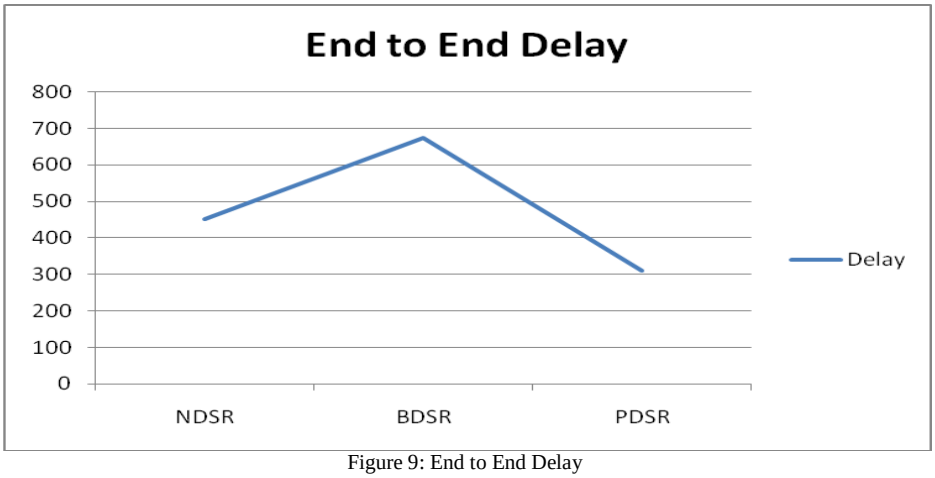

Figure 9: End to End Delay

Figure 9: above shows the End to End Delay of DSR using different scenarios i.e. In case of normal network operations (NDSR), it is 451.825ms which is increased up to 674.062ms by Black hole attack (BDSR) and it is normalized by proposed scheme up to 309.641ms.

V. CONCLUSION

MANETs are wireless based networks of mobile nodes with limited resources like computation power, communication range and storage capabilities, shared channel, usually for economical reasons. There is no centralized authority to monitor the nodes and nodes can join and leave the network any time. So if any malicious node joins the network then it is very difficult to trace that node. So it is necessary to detect and isolate that node from entire network for smooth operations. To secure the communication over MANETs there must be a method which can ensure the detection and prevention from the attacks like Black Hole. Mobile ad hoc network resources suffer from this attack. This research work analyzes the impact of black hole attack over MANET and proposed a method which is able to handle black hole attack over DSR.

We analyzed the MANET performance using DSR under the constraints of performance parameters i.e. Throughout Packet delivery Ratio, Routing Load, end-to-end delay etc. In case of normal network operations (NDSR), Throughput of DSR is 65.3 bps which is reduced up to 44.6 bps by Black hole attack (BDSR) and it is recovered by proposed scheme up to 87.6 bps.

In case of normal network operations (NDSR), it is 48.12085483 which are reduced up to 43.05019305 by Black hole attack (BDSR) and it is recovered by proposed scheme up to 64.36443791.

In case of normal network operations (NDSR), it is 3.078101072 which are increased up to 3.322869955 by Black hole attack (BDSR) and it is reduced by proposed scheme up to 2.553652968.

In case of normal network operations (NDSR), it is 451.825ms which is increased up to 674.062ms by Black hole attack (BDSR) and it is normalized by proposed scheme up to 309.641ms.

As per discussion, it can be observed that Black hole attack has reduced the Throughput and PDR and increased the Routing Load and End to End Delay. Simulation results show the efficiency of PDSR in terms of improvement of performance parameters i.e. Throughput, PDR, Routing Load and End to End Delay etc. It detects the Black hole attack at early stages and recovers the network from compromised condition and also reduces the Routing Load and Delay etc. Finally, it can be concluded that PDSR performs well and recover the network from Black hole attack under the constraints of performance parameters.

For future work, we can also introduce: Intelligent mobile agents which can protect the network from this type of attack.

References

1. Ashutosh Bhardwaj, "Secure Routing in DSR to Mitigate Black Hole Attack", ICCICCT-IEEE-2014, pp.985-989.
2. Prachee N. Patil, Ashish T. Bhole, "Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching", IEEE-2013, pp.1-6.
3. Mahmood Salehi, Hamed Samavati, "DSR vs. OLSR: Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms under the Effect of New Routing Attacks", International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE-2012, pp.100-105.
4. D. A. Malt z, J. Broch, J. Jet cheva, and D. B. Johnson, "The effects of on-demand behavior in routing protocols for multi-hop wireless adhoc networks," in IEEE Journal on Selected Areas in Communications special issue on mobile and wireless networks, August 1999.
5. Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Attacks against AODV Routing Protocol in Mobile Ad-Hoc Networks", International Conference Computer Graphics, Imaging and Visualization, IEEE-2016, pp.385-389.
6. Y. Liu, Mianxiong Dong, Kaoru Ota, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, IEEE-2016, Vol.11 (9), pp.2013 – 2027.
7. H. Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack", IT4OD, IEEE-2016, pp.1-4.
8. A. O.Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", International Conference on Advanced Information Networking and Applications, IEEE-2016, pp.212-219.
9. H. Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks", ICEIT, IEEE-2016, pp.536 – 542.
10. S.Uma maheswari, N.S.Usha, E.A.Mary Anita, K.Ramaya Devi, "A Novel Robust Routing Protocol RAEED to Avoid DoS Attacks in WSN", ICICES-IEEE-2016, pp.1-5.

11. Emimajuliet.P, Thirilogasundari.V, "Defending Collaborative Attacks in Manets Using Modified Cooperative Bait Detection Scheme", ICICES, IEEE-2016, pp.1-6.
12. Pooja, R. K. Chauhan, "AN ASSESSMENT BASED APPROACH TO DETECT BLACK HOLE ATTACK IN MANET", ICCCA, IEEE-2015, pp.552 – 557.
13. J. Ponniah, Yih-Chun Hu, P. R. Kumar, A System-Theoretic Clean Slate Approach to Provably Secure Ad Hoc Wireless Networking, TCNS-IEEE-2016, pp.206 – 217.
14. Bikram Ballav, Gayatree Rana, Dr. Binod Kumar Pattanayak, "Investigating the effect of Black Hole attack on Zone Based Energy Efficient Routing Protocol for Mobile Sensor Networks", ICIT, IEEE-2015, pp.113-118.

