International Journal of Future Generation Communication and Networking
Vol. 9, No. 1 (2016), pp. 157-166
http://dx.doi.org/10.14257/ijfgcn.2016.9.1.15

Mitigation of Collaborative Blackhole Attack using TRACEROUTE Mechanism with Enhancement in AODV Routing Protocol

Nitin Khanna*

Assistant Professor, Department of Computer Science & Engineering,
College of Engineering & Management,
Kapurthala, Punjab,India
nitinkhanna300@gmail.com

Abstract

MANET is multi-hop network in which collection of mobile nodes is self configurable and co-operates together for communicating data without the need of any centralized component for management. Due to this dynamic nature of topology and infrastructure less frame in MANET, these nodes have to rely on each other for data transmission in multi-hop fashion and thus are prone to packet drop attacks like Blackhole attack, Co-Operative Blackhole attack, etc and various types of data security attacks. In this paper, Solutions are proposed to detect Collaborative co-operative Blackhole attack in MANET. We introduced the mechanism of TRACEROUTE that helps in detecting the source of collaborative Blackhole attack and thus break the collaboration by eliminating and marking source of Collaboration between those malicious nodes. AODV routing protocol is enhanced by introducing new field that helps in finding the optimal, secure and reliable routes. These Solutions are compared with W-AODV for Packet Delivery Ratio, Control load, accuracy in Blackhole detection and accuracy in Blackhole detection.

Keywords*: MANET, Enhanced AODV, Co-operative Blackhole Attack, TRACEROUTE*

1. Introduction

MANET is a decentralized ad-hoc network in which nodes are mobile in nature and are free to move in the region either in regular or irregular pattern. It is ad-hoc in nature as the routes are formed spontaneously as and when needed. Due to this nature, MANET is exposed to numerous security threats like packet drop attacks, spoofing, etc. As there is no centralized system it is very difficult to maintain ordered communication in network and various mechanisms has been postulated to detect and avoid these attacks.

Out of these various attacks, Blackhole attack is the most common type of attacks. It is a kind of packet drop attack in which the attacking node sends a fake RREP packet back to the source through various intermediate nodes in reply to the RREQ packet sent by source to find optimal path to a particular destination but attacking node does not have a legitimate path to the destination. The path advertised by attacker seems a legitimate one to source and it sends data packet through that path to the destination. When the packet reaches the attacking Blackhole node, it does not forwards it to the next hop in the route and thus the packet gets dropped and never reaches the destination.

To encounter this attack, mechanism like Watchdog [9] and Pathrater [9] are introduced that observe the forwarding pattern of next hop. In Watchdog, a special counter is maintained at every node for all its neighboring nodes. This counter is incremented by a node when it forwards the packet to the next hop but the next hop does not forwards it further before the timer gets expired. When after incrementing the counter,

ISSN: 2233-7857 IJFGCN

it reaches a particular pre-defined threshold value, the next hop is marked as Blackhole and source is notified about the detection and marking of Blackhole node. On the other hand, Pathrater [9] is a reputation based mechanism in which each node rates every other node and a path is formed that includes more reliable intermediate nodes based on their rating. Every node maintains a rating between 0 and 1 with 1 as maximum rating. When a node is marked as Blackhole, its rating is marked -100.

Watchdog [9] and Pathrater [9] can only detect simple Blackhole attack but fails to detect co-operative Blackhole attacks in which two or more nodes collaborate together in which one malicious node forwards packet to its collaborative malicious partner and the next node performs actual packet drop attack. In case of Watchdog mechanism it fails to detect this attack as fair node sees the next hop forwarding the packet to its successor in the path. This type of attack can produce disastrous impact on the overall working and efficiency of the network.

In this research paper, we will discuss the collaborative attack and how this attack affects the network. Further then we discuss a proposed solution to avoid as well as detect the source of collaborative balckhole attack.

2. Related Work

In this section, some published works are reviewed that come from various authors that provides solutions for detecting and mitigating Blackhole attack [13] and provide security to the communicated information from passive attacks. Watchdog [9] and Pathrater [9] are the mechanisms that are widely used for detecting Blackhole attack. Watchdog is used to detect Blackhole nodes and Pathrater [9] mechanism is used to avoid forming routes that include Blackhole node. But standard Watchdog is not much accurate due to false positives and true negatives. A wide variation of standard Watchdog mechanism is formulated by different authors for more accurate Blackhole detection. Bayesian Watchdog [15] and Kalman Watchdog [5] uses filters that will help in minutely detect Blackhole and avoid false positives and true negatives. But these variation leads to high network overhead. Multilevel Threshold Secret Sharing [6], repository scheme [3] and Comprehensive security scheme using Bit masking [7] are solutions to the passive attacks and secure the information flowing through the network. These techniques lead to high security overhead. Collaborative Watchdog [4] is also used for precisely detect Blackhole attack and disseminate this information to other nodes in the network. In this collaborative Watchdog, if the attacks go undetected, this will prove more problematic than the standard Watchdog. Watchdog-AODV [16] is a fast mechanism which collaborate Watchdog and AODV routing protocol and improves the route discovery. It suffers from similar drawbacks as of standard Watchdog mechanism.

3. Methodology

In this section, we first introduced how AODV is enhanced by introducing a new field that helps in forming more reliable paths. After that we discuss the working of collaborative Blackhole attack and discuss its catastrophic effects. After then we present a solution proposed to tackle this form of Blackhole attack. We also discuss the importance of ACKnowledgement to maintain a special counter that helps in finding out when to trigger the proposed solution “TRACEROUTE”.

3.1 Enhanced Aodv

To enhance AODV routing protocol, we introduced a new field DR, with most significant bit is of the use. DR Field is introduced in route discovery control packets that will help in finding an authentic route to destination. It is a 1 bit field which is when set to 1 will force the RREQ packet [12] to go all the way to destination node and a new RREP

control packet [12] is generated by destination after incrementing its sequence number. When DR bit is set to 1 then no intermediate node can generate RREP control packet [12] by looking up in its route table or for attacking purposes. For ensuring that the RREP [12] is coming from the destination node itself, cryptography [14] techniques are used. The rest of the field is padded to provide alignment with rest of the packet.

3.2 Cryptography

Cryptography [12] in terms of public key cryptography using RSA signature [14] is used that helps in authenticating that the RREP packet [12] is generated by the destination only when the DR bit is set to 1. For that all the nodes must have information about each other's public key for authentication purpose.

3.3 Collaborative Black Hole Attack

Collaborative Blackhole attack [1] is a special type of Blackhole attack in which two or more malicious nodes collaboratively performs packet drop action and escaping from being caught by simple Watchdog mechanism. Firstly two or more nodes form a collaboration to act maliciously. Then they together initiate the collaborative Blackhole attack in the same way as in the Blackhole attack. Each node involved in collaboration reply to every RREQ packet [12] received by it with a fake RREP packet [12] that advertises the node with having the shortest route to the requisite destination. When the source stores this fake route and sends data packet through this route, the source of collaboration that replied with the fake RREP packet [12] forwards the packet to the next spurious node in the collaboration to avoid get detected by Watchdog mechanism. The next node in the collaboration then performs the actual Blackhole attack by dropping the packet without getting caught by Watchdog mechanism as the previous node itself is involved in the attack.

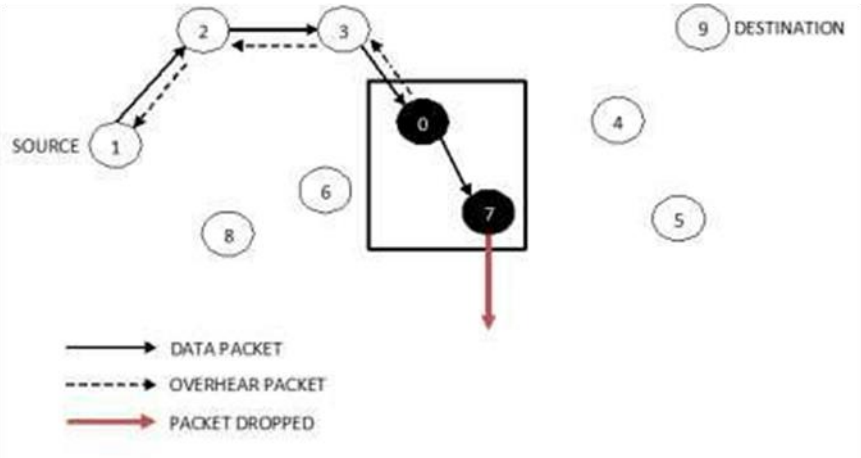


Figure 1. Illustration Of Collaborative Blackhole Attack [1]

In the above figure node 0 and 7 performs the collaborative Blackhole attack where node 0 acts as malicious forwarding node while node 7 performs actual packet drop action.

3.4 TRACEROUTE

In this mechanism, the source node sends a Trace packet on the path to the destination and sets a timer for Reversetrace. On receiving the Trace packet each intermediate hop forwards the trace and set the timer for Reversetrace. If the timer expires before the

Reversetrace is received, then the node marks the next hop as collaborative Blackhole node and send Reversetrace to source through previous nodes.

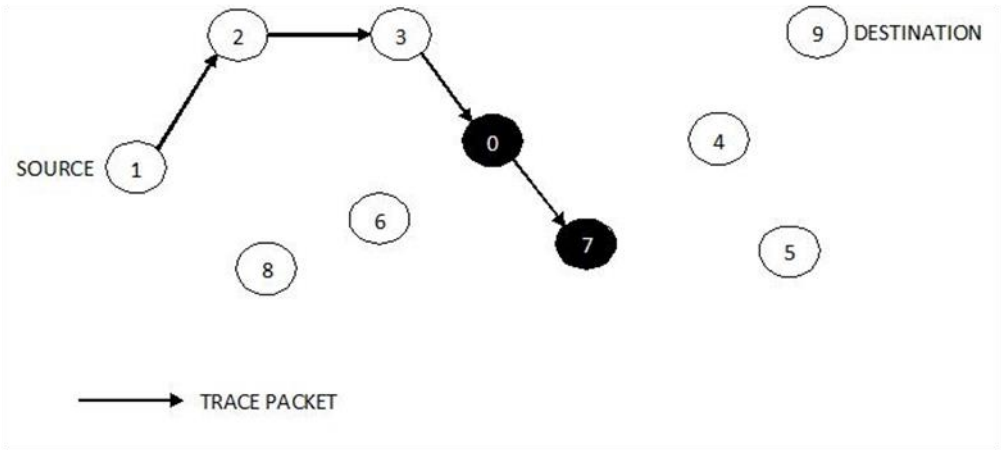


Figure 2. Source Sending Trace Packet

In the above figure, source node is sending a Trace packet up to the last node on the path to find out the collaboration of nodes that are performing Black hole attack.

One out of several collaborative Blackhole nodes, the node which is next hop of a fair node will send a Reversetrace marking one of the collaborative nodes as collaborative Blackhole to save itself from being marked. So this will help in marking a collaborative Blackhole and breaks their collaboration for packet drop attack. Next time, the same collaboration of Blackhole will not work as in Reversetrace, it will be checked that whether the marked node in Reverse trace is already marked as collaborative Black hole or not. And if it happens, then the node marks the next hop (node) as collaborative Black hole.

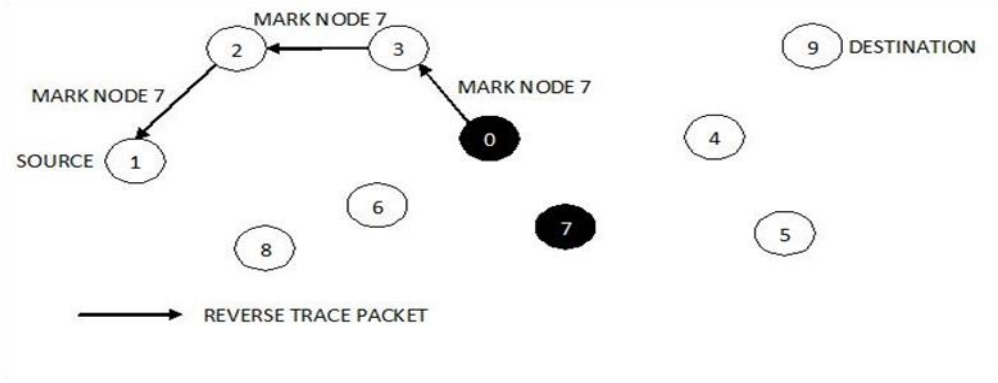


Figure 3. Source of Collaborative Blackhole Attack Sending Reverse Trace Back To Source Node Marking Its Partner

In the above figure, the acting fair node in Collaborative Blackhole attack is marking its collaborator as Blackhole and sending Reversetrace all the way to source node. If the node 0 does not marks node 7 as Blackhole and sent Reversetrace, the previous hop of it will mark it as Blackhole and send Reversetrace to node after timeout of receiving Reversetrace from next hop.

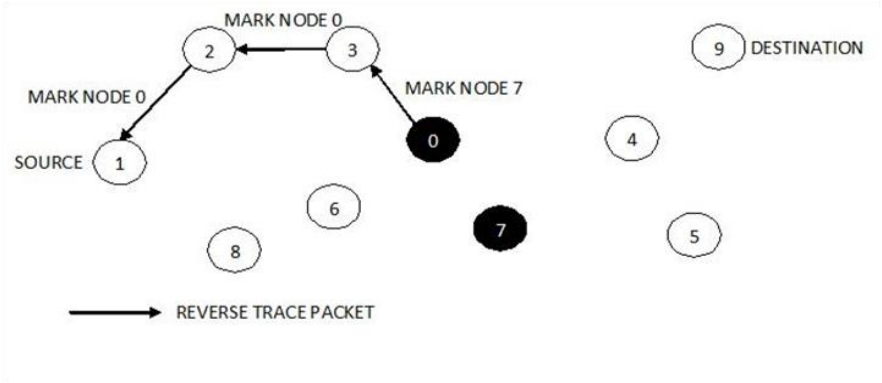


Figure 4. Source of Collaborative Black Hole Attack Sending Reverse Trace Back to Source Node Marking its Partner But Get Caught

In the above figure, node 7 is again marked as Blackhole by node 0 and Reversetrace is send back. But as the node 7 is already marked as Blackhole, so the fair node will easily understand that node 0 is performing Collaborative Blackhole attack and mark it as Blackhole and send back Reversetrace packet to source node through previous intermediate node.

3.4.1 Algorithm for TRACEROUTE

1) Declare TIMER,hopcount, next, source, destination, nexthop, transmissiontime, processingtime, blacklist,sourcearg

```
Set sourcearg := source;
      Set next := nexthop[source][destination]
   WHILE(source!=destination)
      /* set timer for reversetrace*/
      Set TIMER :=( hopcount+1)*2*(transmissiontime + processingtime)
            Hopcount := hopcount-1
            source=next
            next := nexthop[source][destination]
   END WHILE
      /* if reversetrace not received before timer expires */
   IF(TIMEDOUT)
      /* Mark next hop as collaborative Blackhole */ Set
      blacklist[next] := TRUE
   END IF
   Set source := sourcearg
      next := nexthop[destination][source]
      /* send reversetrace to source through nodes on the path */
   WHILE(destination!=source)
      destination := next
      next := nexthop[destination][source]
   END WHILE
END;
```

3.4 ACK Counter

This counter helps in identifying whether the packet is delivered safe and sound to the destination or not. When the sender node sends a data packet to a particular destination it increments the ACK counter and this counter is decremented when an ACK packet is received by the sender from the receiver side that ensures delivery of the data packet to it. If the ACK packet is not received within a pre-specified interval, the packet is assumed to be dropped and the counter is not decremented. When the counter reaches a specified threshold, TRACEROUTE mechanism gets triggered for the detection of source of collaborative Blackhole attack and thus breaking the co-operation among them by marking one of the nodes involved in collaboration.

4. Result and Discussion

All the simulations and analysis of result is done in MATLAB 2013a. The proposed work has been compared with the published work W-AODV [11] for various network evaluation parameters. The assumed environment and parameters used for simulation of proposed work are described in the table below:-

Table 1. Simulation Environment and Parameters

PARAMETERS	VALUE
NUMBER OF NODES	25,30,35,45
SPEED OF NODES (m/sec)	5,10,15,20
ANTENNA TYPE	OMNI-DIRECTIONAL
% OF BLACK HOLES	10%
AREA	2000m X 2000m
NEIGHBOUR TIME	1s
SCENARIOS	18
WIRELESS INTERFACE	802.11
ROUTING PROTOCOL	Enhanced W-AODV
% OF COLLABORATIVE BLACKHOLES	5%
TRANSMISSION RANGE	250m
TRANSPORT PROTOCOL	TCP
MOBILITY MODEL	RANDOM WAY POINT

4.1 Packet Delivery Ratio V/S Node Density

Packet Delivery Ratio is defined as the ratio of total number of packets that are received by intended destination and the total number of packets that are generated by the source node.

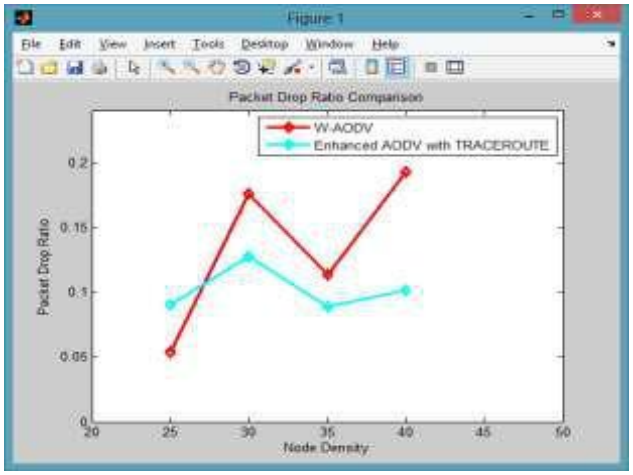


Figure 5. Packet Delivery Ratio V/S Node Density

With it is observed that our proposed solution maintains a good reputation in Packet Delivery ratio with high Packet Delivery Ratio and less fluctuation with changing parameters like node density and mobility.

4.2 Normalized Control Load V/S Node Density

Normalized Control Load is defined as a parameter that is calculated as the ratio of total number of Control Packets generated by nodes in the network to the total number of Data Packets received and accepted by the destination node.

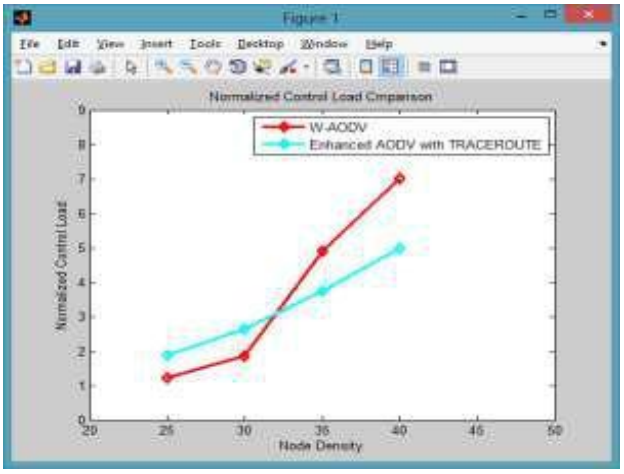


Figure 6. Normalized Control Load V/S Node Density

Our proposed solution exhibits higher control load for small values of parameters like mobility and node density. This is due to some fixed overhead caused due to enhancement in security of MANET and the use of Cryptography. But as these parameters value increases to the real MANET parameters, the control load increases in lesser amount than W-AODV [16].

4.3 Accuracy in Detection of Blackholes V/S Node Density

Accuracy can be calculated through finding the total number of cases in which the node is actually misbehaving or there seems to be potency of node to be Blackhole and how well the mechanism performs in identifying and marking those Blackhole nodes.

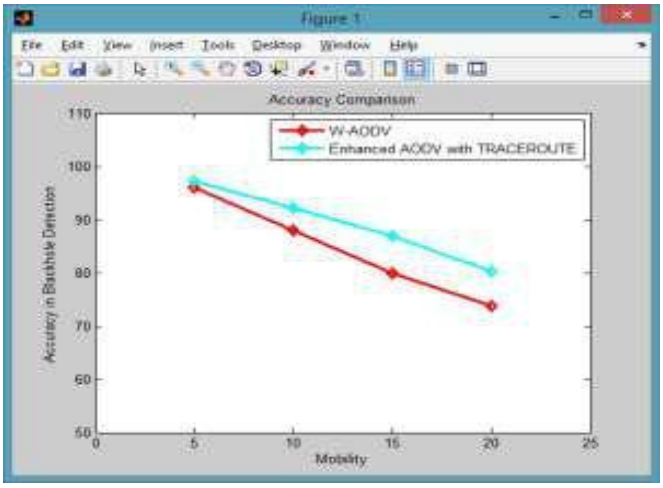


Figure 7. Accuracy in Detection of Blackholes V/S Node Density

Accuracy also deals with how well the mechanism helps in identifying all types of Blackhole nodes that are involved in packet drop action, that is, accurate detection of false positives along with true negatives. Our proposed solution provides a very high accuracy in all circumstances.

4.4 Packet Drop Ratio V/S Node Density

Packet Drop Ratio is defined as ratio of total number of packet dropped in the network to the total number of packet sent or generated by the source node in the network.

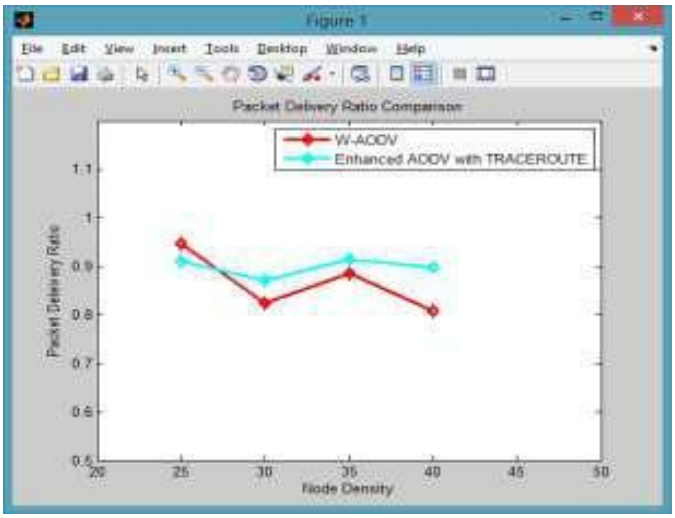


Figure 8. Packet Drop Ratio V/S Node Density

Our proposed solution provides markedly less Packet drop under any size of MANET and any mobility speed.

Conclusion

In this paper, we have analyzed our solution Enhanced AODV with TRACEROUTE mechanism provides more accurate detection and mitigation to collaborative Blackhole attack under various scenarios in MANET. Our solution provides more accuracy in detection of Blackhole nodes with minimal false positive and no true negative. Our solution does not only act reactively but proactively to avoid attacks beforehand and restrict it from occurring as long as possible. With the results, it is clear that our solution gives better Packet Delivery Ratio, reduces Control Load on the network and more accuracy in detection without hampering smooth flow of data packets.

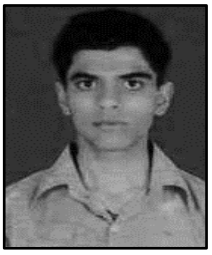
Future Work

The overhead caused due to enhancement in W-AODV and Cryptography causes some constant overheads in route maintenance. We propose improvement in the approach to reduce overheads. We propose enhancements in mechanism to detect and mark all the nodes that are involved in co-operation for packet drop action.

References

[1] P. Peethambaran and J.S. Jayasudha, "SURVEY OF MANET MISBEHAVIOUR DETECTION APPROACHES", International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 3, **(2014)**.
[2] Gaurav, N.S.H. Tyagi, "An Approach: False Node Detection Algorithm in Cluster Based MANET", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 2, **(2014)**.
[3] K. Sahadevaiah, Prasad Reddy P.V.G.D, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks", MacroThink Institute, vol. 3, no. 4, **(2014)**.
[4] E. Hernández-Orallo and M.D. Serrat, O. Juan-Carlos, C. Carlos, T. Calafate and P. Manzoni, "A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs", Springer , **(2013)**.
[5] T. Sharma, M. Tiwari, P.k. Sharma, M. Swaroop and P. Sharma, "An Improved Watchdog Intrusion Detection Systems in Manet", International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 3, **(2013)**.
[6] L.H.M. Fuyou, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem", Information Processing Letters 114, ELSEVIER, **(2014)**, pp. 504–509.
[7] A. Malhotra, V. Yadav, N. Tanwar, N. Sherwal and A. Bardhan, "A Comprehensive Security Scheme on MANETs", ELSEVIER, **(2014)**.
[8] V. Shah and N. Modi, "An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks", International Journal of Computer Applications (0975 – 8887), vol. 69, no. 7, **(2013)**.
[9] D. Anitha1, M. Punithavalli, "A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS", IJCSMC, vol. 2, no. 3, **(2013)**, pg.112 – 119.
[10] C.d.M. Cordeiro and D.P. Aggarwal, "Mobile Ad-hoc Networking", **(2002)**.
[11] A. Tonnesen, "Mobile Ad-hoc Networks", **(2004)**.
[12] C.E. Perkins and .E.M. Royer, "Ad hoc On Demand Distance Vector Routing", **(1999)**.
[13] R.H. Khokhar, A. Ngadi and S. Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", **(2008)**.
[14] B.A. Forouzan, "Data Communications and Networking 4th Edition", Tata McGraw Hill Companies, **(2006)**.
[15] M.D. Serrat-Olmos, E. Hernandez-Orallo, J. Cano, C.T. Calafate and P. Manzoni, "Accurate detection of black holes in MANETs using collaborative bayesian watchdogs", Wireless Days(WD), IEEE Conference, **(2012)**, pp. 1-6.
[16] T. Varshney, T. Sharmaa and P. Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network", IEEE International Conference on Communication Systems and Network Technologies, **(2014)**, pp. 217-221.
[17] R.L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21, vol. 2, pp. 120–126.

Authors



Nitin Khanna, He received the M.Tech. Degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, in 2015, Currently, He is doing research work in the field of ad -hoc networks for the institute CEM college, Kapurthala and is working as Assistant Professor in the department of Computer Science & Engineering affiliated to Punjab Technical University, Jalandhar, Punjab.