Mitigating Blackhole and Security attacks in MANET using Enhanced W-AODV with Trueness Level and Cryptography

Nitin Khanna[1], Parminder Singh[2]
Department of Computer Science and Engineering
Ramgarhia Institute of Engg. & Technology,
Phagwara, Punjab, India

***Abstract*—**MANET is multi-hop network in which collection of mobile nodes is self configurable and co-operates together for transmission of data without the need of any centralized component for management. Due to this dynamic nature of topology and no fixed infrastructure in MANET, these nodes have to rely on each other for data transmission and thus are prone to packet drop attacks like Blackhole attack. MANET is also prone to some passive attacks such as eavesdropping and masquerading, due to its multi-hop and ad-hoc nature. In this paper, Solutions are proposed to detect both Blackhole attacks and all types of passive attacks. We introduced the mechanism of Enhanced W-AODV, which is the collaboration of standard Watchdog mechanism and Enhanced AODV routing protocol. Enhanced AODV helps in finding out the most optimal, secure and reliable routes and Watchdog mechanism helps in detecting Blackhole attacks. The new mechanism Trueness Level mechanism is used to find the most reliable path that contains nodes that have good reputation in forwarding packets. These Solutions are compared with W-AODV for Packet Delivery Ratio, Control load, accuracy in Blackhole detection and reliability of paths.

Keywords*—*MANET, Blackhole Attack, Trueness Level, AODV Routing Protocol, Enhanced W-AODV, Cryptography, Security.

I. INTRODUCTION

Mobile Ad-hoc NETwork is a multi-hop network that gained popularity in the modern era due to its self configurable and no infrastructure nature. Due to these features, MANET can be easily used in military operations, rescue operations and in many other fields in which it is very difficult to place a central infrastructure. Due to mobility, ad-hoc nature and dynamic topology, MANET is prone to various routing attacks like Blackhole attack [13], wormhole attack [13], collusion attack [13], etc. These attacks hinder smooth routing in MANET that can result into hazardous reactions. Blackhole attack is an attack in which a malicious node advertises itself to have the shortest and fresh route to the intended destination by sending RREP packet in reply to the RREQ packet. Due to this, the source accepts this path and start sending packet through this path and when packet is received by this malicious node, it drops the packet. Blackhole attack can be detected through Watchdog mechanism. In this mechanism, a counter for every other node is used which is incremented by 1 for every packet which is not forwarded by the nexthop node. If the counter after increment reaches the threshold value, then that corresponding nexthop node is marked as Blackhole and the source is notified.

MANET is not only exposed to routing attacks. Due to multi-hop nature and wireless medium used in MANET, passive attacks like eavesdropping, masquerading, etc can also take place in MANET. Due to wireless medium, any malicious node can easily hear to the traffic in the network that is within the range of that node without even coming into notice of any other node of the network. This proves to be catastrophic if no measure is taken for security of sent data and the information communicated through the network needs confidentiality and authentication. For taking measures against these attacks, Cryptographic techniques like RSA signature, Diffie–Hellman Algorithm for secret key Generation and Symmetric key cryptography are used that helps in securing the data communicated through the MANET. For mitigation of Blackhole attacks, TRUENESS LEVEL along with Enhanced W-AODV and cryptographic techniques are used.

II. 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 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.

III. PROPOSED SOLUTION

To mitigate blackhole attacks, we have enhanced W-AODV [16] and introduce the concept of TRUENESS LEVEL. To avoid attacks against security of data, we used cryptographic techniques. All these mechanisms are explained as follow:-

A. Trueness Level

This mechanism is a hybridization of path rating mechanism and trust mechanism. In this every node holds the trust in terms of Trueness Level on each and every node in the MANET. The Level can be any of falling in the range of 0 to 7 with 7 is the highest Trueness Level and 0 is the Lowest Trueness Level that depicts the Trueness Level of a misbehaving node.

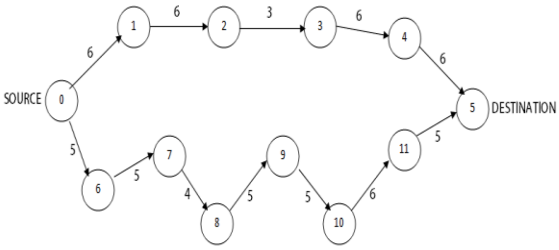

Fig.1: Nodes with their Trueness Level on next hop in MANET

The Trueness Level is used in following two ways:-

Trueness Level as Trust Mechanism

In this, the Trueness Level helps in collaboration of Watchdog mechanism report about a particular misbehaving node and helps the nodes in network to decide whether to trust the report of Watchdog mechanism of another report or not. It helps node in avoiding false watchdog reports that involves false positives or true negatives.

Trueness Level as Path Rating Mechanism

In this the rating of path is calculated through following function:-

$$\text{TL of Path} = \text{MINIMUM } (TL_{ij}) \text{ for all i and j on the path} \quad (1)$$

Where TL_{ij} is Trueness Level that node i have on node j.

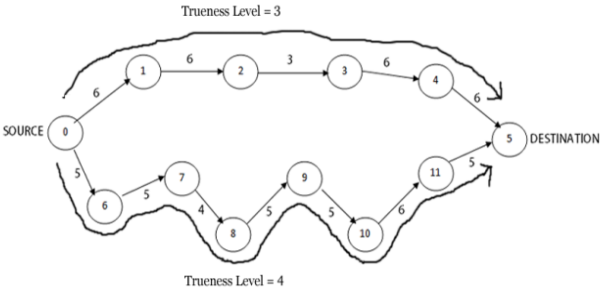

Fig.2: Trueness Level of Paths to Destination 5 from Source 0

It uses the MINIMUM function to rate the fairness and reliability of the path. Minimum function will set the Trueness Level of path to the minimum Trueness Level among nodes in the path. So the Trueness Level is set to the weakest link in the path.

Algorithm for TRUENESS LEVEL

```
1)   /*   Initialization of Trueness Level Array   */
Declare TL, n      /*n is total number of nodes and TL is 2D array for Trueness Level */
For i = 1 to n
    For j = 1 to n
        /*Every node set trueness level 7 for itself */
        IF(i=j)
            Set  TL[i][j]:=7 /* highest Level */
        ELSE
            Set TL[i][j]:=3  /* neutral Level */
        END IF
    END FOR
END FOR

2)   /* Calculate the Trueness Level of Path */
Declare pathTL, linkTL,nexthop,source,destination,next
/* pathTL holds the Trueness level of path and nexthop is a 2D array for storing nexthop for destination*/
Set pathTL := 7
/* setting Trueness Level to minimum of Trueness Level among links on path */
WHILE(source!=destination)
next := nexthop[source][destination]
linkTL := TL[source][nexthop]
            IF(linkTL < pathTL)
                        pathTL := linkTL
            END IF
            source := next
END WHILE

3)   /*   Updating the values of Trueness Level        */
Declare packetsent, packetforwarded,percentage        /* packetsent is the number of packet sent to the node and packetforwarded is number of packet forwarded by node*/
FOR i = 1 to n
    FOR j = 1 to n
            Set percentage := packetforwarded/packetsent*100
            /* for no communication*/
        IF(percentage is UNDEFINED)
                Break;
        ELSE
                IF P = 100
                        Set TL[i][j] := level[i][j]+2
                ELSE IF P < 100 and P > 95
                        Set TL[i][j] := TL[i][j]+1
                ELSE IF P <= 85 and P > 80
                        Set TL[i][j] := TL[i][j]-1
                ELSE IF P <= 80 and P >= 75
                        Set TL[i][j] := TL[i][j]-2
                ELSE IF P < 75
                        Set TL[i][j] := 0.
                 ELSE
                        No change in TL[i][j].
                 END IF
        END IF
    END FOR
END FOR
```

4) /* Collaboration of Ttrueness Level with Watchdog for accuracy in dissemination of information*/

```
Declare informer, PBH, blacklist,node  /* informer is node sending information, PBH is potential Blackhole node */
/* for checking if PBH is already marked as blackhole*/
IF(blacklist[node][PBH]==0)
        /* Comparing Trueness Level of informer and PBH for action */
        IF(TL[node][informer] > TL[node][PBH]
                Mark PBH as blackhole and send information to neighbourhood
        ELSE IF(TL[node][informer] +2 <= TL[node][blackhole])
                Mark informer as blackhole and send information to neighbourhood
        END IF
END IF
```

B. Enhanced W-AODV

W-AODV [16] is a collaboration of AODV routing protocol with standard Watchdog mechanism that helps in finding a route as soon as a Blackhole node is detected for a particular destination. Enhancement in W-AODV is divided into three stages as follow:-

1. Reverse path establishment
2. Introducing a new DR bit in control packets
3. Use Trueness Level for reliable path establishment

Reverse Path Establishment

In this, during route discovery, the nodes in the network not only look for finding route from source to the destination but also look for finding route from destination to source. When a reliable path from source to destination is established through sending RREP control packet from destination or an intermediate node to source, just during that time a reverse path is established in the same way from destination to source in which the role of source and destination are interchanged and previous hop in forward path for a node become next hop for that node in reverse path.

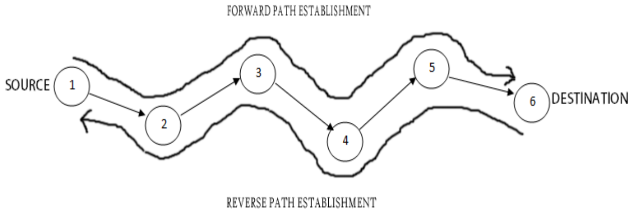

Fig.3: Reverse and Forward Path Establishment in Enhanced AODV

DR Field in control packet

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 to go all the way to destination node and a new RREP control packet 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 by looking up in its route table or for attacking purposes. For ensuring that the RREP is coming from the destination node itself, cryptography techniques are used.

Use Trueness Level for Reliable Path Establishment

Trueness Level of path is used in the same way as hop count is used for establishing paths. If any intermediate node already has a route to a destination node and it receives a RREP packet with same sequence number then it checks whether the path advocated by RREP has higher Trueness Level then the Trueness Level of already stored path. If it is then the route table for that destination entry is updated otherwise RREP control packet is discarded. If the Trueness Level of both paths is same then the traditional approach in which minimum hop count path is selected is used.

C. USE OF CRYPTOGRAPHY

Cryptography is the base of security measures in this approach. Various techniques of cryptography and the way in which these techniques are used are explained as follow:-

Diffie-Hellman Algorithm for Symmetric key Generation

Diffie-Hellman algorithm [14] is used to generate symmetric key between two end nodes to ensure confidentiality of information communicated through data packets. When the two nodes need to communicate for the very first time, the source node initiates Diffie-Hellman Algorithm by sending parameters for calculation of symmetric shared key. Then destination after authentication, continue the algorithm and generate a common secret shared key. The authentication process is done through the use of RSA Signature.

Additive Cipher for encryption/decryption process

Whenever a node needs to send data packets to a destination node, it uses additive cipher [14] to encrypt the message data using secret key which it has earlier exchanged and created along with the destination node using Diffie-Hellman algorithm.

Message Digest using MD5 algorithm

Message digest [14] is used to ensure the integrity of data packets that are transmitted from source node to the destination node. Although the integrity is somewhat ensured through the use of Watchdog mechanism but still there are some loop holes in that process so that is why Message Digest is used. So that if any discrepancy is found in received data that must not go undetected. For generating digest of the message MD5 algorithm is used.

RSA Signature

RSA signature [17] algorithm plays a very important role in maintaining security, authentication and identification of attacks in MANET. First of all, RSA signature is used to ensure the security of secret key generation. It is used to sign Diffie-Hellman parameter to ensure that the base of communication between two end nodes is secured. RSA signature will help in avoiding blackhole nodes to generate fake RREP control packet when DR bit is set to 1. In that case, when DR bit is set to 1, the source will accept RREP packet that comes all the way from destination itself which is authenticated through RSA signature algorithm. If the secret key is already generated then the RREP control packet will include RSA signature on the digest of secret key or if it is the first communication then it must include RSA signature on Diffie-Hellman parameter. The third role of RSA signature is to help in ensuring authenticity of sender as the data sent by the source node is officially signed by the source through its private key and packet is accepted only after validation of signature through public key of sender node.

IV. SIMULATION ENVIRONMENT

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

PARAMETER	**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

V. RESULTS AND DISCUSSION

A. *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.

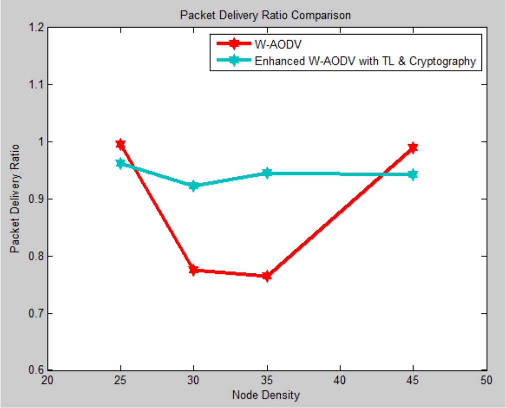

Fig.4: Packet Delivery Ratio v/s Node Density

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.

B. *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.

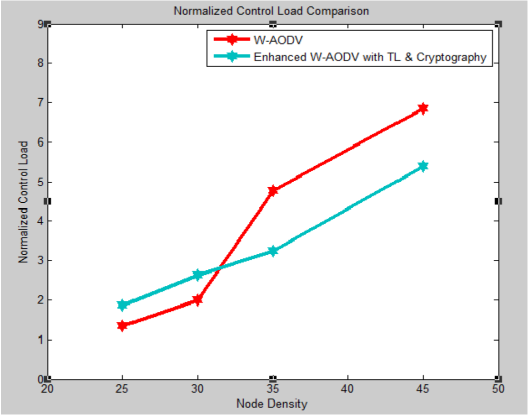

Fig.5: Normalized Control Load v/s Node Density

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].

C. 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.

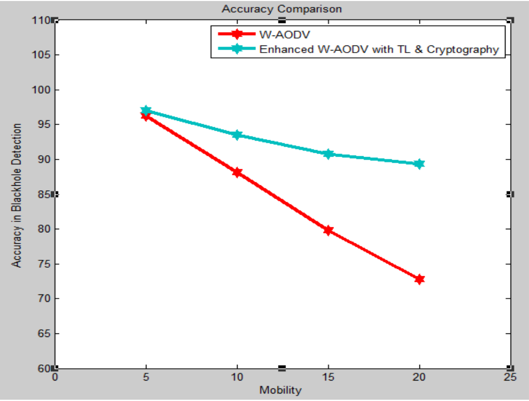

Fig.6: Accuracy in detection of Blackholes v/s Node Density

Accuracy also deals with how well the mechanism helps in identifying misbehaving nodes only and not the fair nodes that are co-operating well, that is, accurate detection of false positives along with true negatives. Our proposed solution provides a very high accuracy in all circumstances.

D. 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.

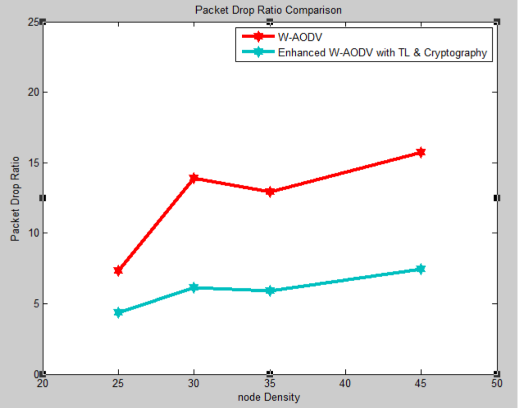

Fig.7: Packet Drop Ratio v/s Node Density

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

E. Reliability of PATH v/s Quarter of Simulation

Reliability of path is measured as security of the path and its freedom from blackhole, misbehaving nodes and potential misbehaving nodes. It defines how reliable the path is in long run and so no packet dropping attack takes place in the path.

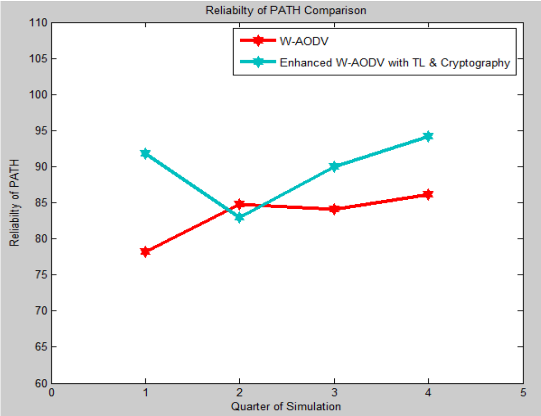

Fig.8: Reliability of PATH v/s Quarter of Simulation

Due to the use of TRUENESS LEVEL and enhancements in routing protocol, the reliability of formed paths is of high degree.

VI. CONCLUSION

In this paper, we have analyzed our solution Enhanced W-AODV with TL and Cryptography under various scenarios in MANET for detection and mitigation of Blackhole and security attacks. Our solution provides more accuracy in detection of Blackhole nodes with minimal false positive and no true negative. With the results, it is clear that our solution gives better Packet Delivery Ratio, reduces Control Load on the network and more reliable path formation along with data security provided by the cryptographic techniques.

VII. FUTURE WORK

As future work, we want to test this work for identifying and mitigating Gray Hole attacks which is similar to Blackhole attack that drops data packet selectively. 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.

VIII. REFERENCES

[1] Punya Peethambaran and Dr. Jayasudha J. S. (2014) “SURVEY OF MANET MISBEHAVIOUR DETECTION APPROACHES”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No. 3, May 2014.

[2] Gaurav, Naresh Sharma Himanshu Tyagi (2014) “An Approach: False Node Detection Algorithm in Cluster Based MANET”, International Journal of Advanced Research in Computer Science and Software Engineering Vol. 4, Issue 2, February 2014.

[3] K. Sahadevaiah, Prasad Reddy P.V.G.D. (2011) “Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks”, MacroThink Institute, Vol. 3, No. 4, 2014.

[4] Enrique Hernández-Orallo, Manuel D. Serrat, Olmos Juan-Carlos, Cano Carlos, T Calafate, Pietro Manzoni (2013) “A Fast Model for Evaluating the Detection of Selfish Nodes Using a Collaborative Approach in MANETs”, Springer , 2 August 2013.

[5] Tushar Sharma, Mayank Tiwari, Prateek kumar Sharma, Manish Swaroop, Pankaj Sharma (2013) “An Improved Watchdog Intrusion Detection Systems In Manet”, International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 3, March 2013.

[6] Lein Harn Miao Fuyou (2014) “Multilevel threshold secret sharing based on the Chinese Remainder Theorem”, Information Processing Letters 114, ELSEVIER, 2014, Pg 504–509.

[7] Amarjit Malhotra, Vikas Yadav, Nikhil Tanwar, Naresh Sherwal and Ashish Bardhan (2014) “A Comprehensive Security Scheme on MANETs”, ELSEVIER.

[8] Vrutik Shah, Nilesh Modi (2013) “An inquisition based Detection and Mitigating Techniques of AODV Protocol in Existence of Packet Drop Attacks”, International Journal of Computer Applications (0975 – 8887), Volume 69, Issue No.7, May 2013.

[9] D.Anitha1, Dr.M.Punithavalli (2013) “A Collaborative Selfish Replica with Watchdog and Pathrater in MANETS”, IJCSMC, Vol. 2, Issue. 3, March 2013, pg.112 – 119.

[10] Carlos de Morais cordeiro and Dharma P. Aggarwal (2002) “Mobile Ad-hoc Networking”.

[11] Andreas Tonnesen (2004) “Mobile Ad-hoc Networks”.

[12] Charles E Perkins Elizabeth M Royer (1999) “Ad hoc On Demand Distance Vector Routing”.

[13] Rashid Hafeez Khokhar Md Asri Ngadi Satria Mandala (2008) “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”.

[14] Behrouz A Forouzan (2006) “Data Communications and Networking 4th Edition”, Tata McGraw Hill Companies.

[15] Serrat-Olmos, M.D. Hernandez-Orallo, E. ; Cano, J., Calafate, C.T., Manzoni, P. (2012), “Accurate detection of black holes in MANETs using collaborative bayesian watchdogs”, Wireless Days(WD), IEEE Conference, Nov. 2012, pg. 1-6.

[16] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma (2014), “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network”, IEEE International Conference on Communication Systems and Network Technologies, June, 2014, pg. 217-221.

[17] R.L. Rivest, A. Shamir, and L. Adleman, (1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM 21 vol. 2, pg. 120–126.

NITIN KHANNA received the B.Tech. degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, in 2013, Currently, He is doing research work in the field of ad-hoc networks for the award of degree of M.Tech. from Punjab Technical University, Jalandhar, Punjab.