Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Denial of Service (DoS) and Black Hole Attack Prevention by Enhanced Watchdog Technique in MANET

Mayank Namdeo*
CSE & RGPV,
Bhopal, India

Prof. Dr. P. S. Patheja
Dean, MTech Course CSE & RGPV,
Bhopal, India

Abstract— The attacker in Mobile Ad hoc Network (MANET) is easily modified the routing procedure because of absence of centralized administrator and supervision system. The topology in MANET is frequently changes by that maintaining strong link connection establishment is not possible. The proposed enhanced watchdog IDS (Intrusion Detection System) security against attack is detects and prevent from malicious attacker to protect dynamic network. The routing misbehaviour of Blackhole attack and Distributed Denial Service attack (DoS) attack is different in network. Blackhole attack is consumes the all data packets after forwarding false reply of destination existence to sender. The DoS attacker is completely different from blackhole attacker, it floods huge amount of unwanted request packets in network that consumes unnecessary channel capacity and after some time the whole network channel capacity is reserve by unwanted packets. The major fault from that is capacity for data forwarding and receiving is also affected. In this research we proposed the new Intrusion and Detection System (IDS) to detect and prevent routing misbehaviour of blackhole attacker and DoS attacker. The attacker detection is based on the basis of packet dropping and packet flooding. The performance of research is measured in three scenarios like in attack, watchdog and proposed enhanced watchdog IDS. The performance of proposed IDS is compare with watchdog detection and prevention scheme and observes that the performance of proposed IDS is better. Then main advantage of this research is to protect both different behaviours of malicious attackers but watch dog is able to provide security against only blackhole attack. The performance of these three scenarios is measured from routing performance metrics, misbehaviour loss percentage.

Keywords— MANETs, IDS, DDoS, Watchdog Detection, Black hole Attack.

I. INTRODUCTION

Ad-hoc networks became increasingly the latest thing in recent years as they're quickly deployable and supply belongings no matter user’s geographical position. They’re adaptive wireless networks that don't have any fastened infrastructure [1]. In areas within which there's very little or no communication infrastructure or the prevailing infrastructure is pricey or inconvenient to use, wireless mobile users should still be ready to communicate through the formation of a commercial hoc network [2]. In such a network, every mobile node operates not solely as a number however conjointly as a router, forwarding packets for different mobile nodes within the network that will not be inside direct wireless transmission vary of every different. Owing to restricted communication vary, nodes communicate via multi-hop wireless links and thus, every node relays packets to look node and performs two roles of host and router. before the routing blessings in MANET security has become a primary concern to produce protected communication between mobile nodes in an exceedingly hostile atmosphere as MANET cause variety of nontrivial non trivial challenges to the protection style as they're a lot of vulnerable than wired networks. These challenges embrace open specification, shared wireless medium, strict resource constraints, and, extremely dynamic configuration.

A. Features of Mobile Ad-hoc Networks

MANETs is an IEEE 802.11 framework. It is an interconnected collection of wireless nodes where there is no networking infrastructure in the form of base stations, devices do not need to be within each other‘s communication range to communicate, the end-users devices also act as routers, nodes can enter and leave over time, data packets are forwarded by transitional nodes to their final destination.

1) *Characteristics of MANETs:* Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), Omni directional (broadcast), probably steer able, or some combination thereof. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, announcement power levels and co-channel meddling levels, a wireless connectivity in the appearance of a random, multi-hop graph or "ad hoc" network exists amongst the nodes. This ad hoc topology may adjust with time as the nodes move or adjust their transmission and reception parameters.

The description of these networks are brief as follows:

- Communication via wireless means

- Nodes can execute the roles of together hosts and routers
- Bandwidth-constrained, variable capacity links
- Energy-constrained Operation
- Limited Physical Security
- Dynamic network topology
- Frequent routing updates

2) *Advantages of MANETs:* The following are the advantages of MANETs:

- They present access to in sequence and services regardless of geographic position.
- These networks can be put up at any place and time.

3) *Disadvantages of MANETs:* Some of the disadvantages of MANETs are as follows:

- Limited resources and physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

II. RELATED WORK

Tarun Varshney,Tushar Sharmaa,Pankaj Sharma [1] “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network” in this title a network performance and reliability is broken by the attacks on ad hoc routing protocols. Many mechanisms have been proposed to overcome the Blackhole Attack. A malicious node or blackhole node send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender sends the data packet to this malicious node, it drops all the packet in the network. The propose watchdog mechanism detect this black hole nodes in a MANET. This method first detects a blackhole node in the network and then provides a new route to source node. In this, the

performance of original-AODV and modified AODV called as watchdog-AODV (or W-AODV) in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio and routing and control load.

A.Babu Karuppiah, T.Meenakshi, T.I.Mano Ranjitha & S.Vivitha,[2] " False Misbehaviour Elimination in Watchdog Monitoring System Using Change Point in a Wireless Sensor Network", In this paper an improved watchdog monitoring mechanism is proposed by using the process of change point detection. By implementing this change point detection algorithm in watchdog mechanism, the limitations of the existing watchdog mechanism are overcome. From this the exact malicious node can be found out and the data will be routed through a secure path bypassing the malicious node. Finally to analyze the efficiency of this algorithm, the results obtained from the proposed algorithm and the existing algorithms are compared.

S. Nishanthi,[3] "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm",in this title we have discuss a tendency to opt for Bio-Inspired Approach. In this paper, the clonal selection principle is implemented and develop the Watchdog based Clonal Selection Algorithm (WCSA).Using this WCSA, the intrusions in the network and monitoring multiple misbehaved nodes. Using this algorithm we can realize intruders and reduce the detector rate, and reduce generator value also will increase in throughput.

Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F.Loureiro and L.B. Ruiz,[4] "Decentralized Intrusion Detection In Wireless Sensor Networks "In Rule-based intrusion detection schemes is proposed for WSN, also called specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting the detection process. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase. In the following sub-sections, the key important schemes in this category are explored. Decentralized IDS in WSN propose the first and the most cited rule-based intrusion detection scheme for WSN to detect many different kinds of attacks in different layers. In this scheme, there are three main phases involved: data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis; the rule application phase, in which the pre-defined rules are applied to the stored data from the previous phase, if the message analysis failed any of the rules test, a failure is raised and the counter increased by one; the intrusion detection phase, a comparison is taken place between the number of raised failures produced from the rule application phase with a predefined number of occasional failures that may happen in the network. If the total number of the raised failures is higher, intrusion alarm is produced.

A.Rajaram. Dr. S. Palaniswami [5] “Malicious Node Detection System for Mobile Ad hoc Networks” in this title, we develop a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, we show that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay, high speed and overhead.

Md Tanzilur Rahman, Kunal Gupta,[6] “MANET: Security Aspects and Challenges” in this title we present the fundamental challenging issues, Security challenges and different types of Attacks associated with MANETs.

Md Tanzilur Rahman, Kunal Gupta,[7] “MANET: Security Aspects and Challenges” we present in this context a Sybil detection approach, based on received signal strength variations, allowing a node to verify the authenticity of other communicating nodes, ac- cording to their localizations. In addition, we define an estimated metric of the distinguish ability degree between two nodes, allowing to determine Sybil and malicious ones within VANET. The applicability of our contributions is validated through geometrical analysis, simulations and real measurements.

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones [8] “Identity-based Attacks Against Reputation-based Systems in MANETs” In this title, we will discuss these attacks and their countermeasures in the context of the reputation-based schemes. We will also discuss how our non-monetary, entry fee based scheme that is incorporated in a reputation system can deter these attacks.

Sukhbir Kamboj, Mohit Dua [9] “Comparison Study of Various DoS Node Detection Schemes in MANETs” in this title we define, many several efficient routing protocols has been proposed for MANET. Most of these protocols assume a cooperative and trusted environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious.

Sarosh Hashmi, John Brooke, [10] “Towards Sybil Resistant Authentication in Mobile Ad hoc Networks” In this title we present an authentication mechanism for MANETs that utilizes hardware id of the device of each node for authentication. An authentication agent is developed that verifies the hardware id of the authenticate node. A comprehensive defense model is employed to protect the authentication agent from various static and dynamic attacks from a potentially malicious authenticate node. Security of authenticate node is assured by involving a TTP that signs the authentication agent, verifying that it will perform only intended function and is safe to execute. With this minimal involvement of the TTP, the proposed authentication scheme offers increased resistance to the Sybil attack. The attacker is now required to either thwart agent protection mechanisms or to acquire multiple devices with different hardware ids, in order to gain multiple identities.

III. PROPOSED IMPROVED WATCHDOG IDS

A. Problem Statement

Cooperative Misbehavior of nodes may cause severe damage, even fails whole of the network. In proposed work we create a new protection scheme against cooperative misbehaviour of nodes. In this scheme first analyze the routing behaviour of malicious nodes against the behaviour of black hole attack and Black hole attack, then apply the proper well planned security scheme on it that block the whole misbehaviour of cooperative malicious nodes and enhance the network performance. To show the effectiveness and results of proposed approach, implementation work on Network Simulator -2.

The whole procedure of attack behavior and identification are represents by figure 4.1. Here the black hole nodes represent the packet consumption and the red node represents the heavy flooding of packets with dotted arrow.

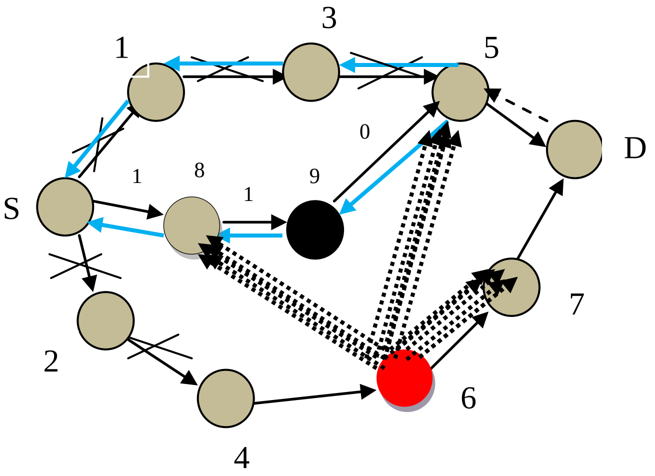

Fig. 1 Represents the Scenario of Attacker

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node flow the routing procedure of routing protocols keeps the records of packets that it has received and uses it to check if the received packet was received before from the same originating source or not. The DoS attackers are completely squeeze the capability of data forwarding. Proposed watchdog IDS identifies heavy data flooding of only a single or multiple attackers that are floods heavy traffic. It means it is the only sender that that do that kind of activity in network.

In secure Intrusion detection system (IDS), every node needs to have two additional small-sized tables that maintaining the routing records in network. One to keep the information of data forwarding (blackhole detection) and another is maintaining the information of fake messages (from node through node i.e. DoS attack). These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the record of packets received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the route information of received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

1) *Algorithm Step for Enhance Watch DOG Base attack Prevention:* In this algorithm we detect and prevent from blackhole and DOS (denial of service attack) using enhanced watch dog mechanism, in this section define the algorithm in step by step process.

```
Initialization:
N: set of devices
S: set of Sender Nodes
R: Set of Receiver Nodes
Watch-DOG node: w є N
a є N : set of attacker nodes
Threshold: Th
w provide open access є N and watch behavior of neighbour
a interact to w or send data to other nodes
a access w resource & data or capture data
if (a update data of s node)
        {
                Check update data by w
                If(update > Th && modified receiver ID )
                {
                Identifies (infected data value, node number, symptoms)
        While (symptoms != normal)
        {
                If (symptoms == DOS attack)
                {
                        Capture node number , new symptoms
                        Analyze behaviour
                        Trace time of data update
                }
                Else if (symptoms != blackhole)
                {
                        Identifies attacker $a_n$
                        Abnormal data set identification
                        Trace time
                }
                Else if (symptoms == new)
                {
                        Watch symptoms behaviour
                        Attacker node a
                        New behaviour table generate
                        Assign-name of attacker
                }
        }
Prevention-manager (attack type, abnormal-table)
                }
        }
Prevention-manager (a-t, a-table)
        {
                Analyze attack type with abnormal table
                Send normal treat msg to a
        If (a profile == normal-profile)
        {
                a є normal profile node
        }
        Else
        {
                Block the node with symptoms
        }
Broadcast attacker node info and its symptoms to all connected node
New path established for communication
Analyze the new network behaviour
Calculate performance of the network
            }
```

The normal routing profile is shows the attacker free routing in network. In this network the attacker is not in active mode because the attacker is inactivate by secure proposed watchdog mechanism.

IV. RESULT

A. Simulation parameter of case study

The simulation of blackhole attack and DoS attack together, watchdog detection and proposed IDS is based on the following simulation parameters. These parameters are taken according to the nature of MANET. Mobile Nodes has random mobility and direction decided in the considered simulation area.

Table I Simulation Parametre

Dimension of Simulated Area	800×800
Mobile Nodes	50
Routing Protocol	AODV
Simulation time (seconds)	100
Attack Type	Blackhole, DOS
Prevention Type	Watchdog, IDS-Proposed
Transmission Range	550m
Transport Layer Protocol	TCP, UDP
Traffic type	FTP, CBR
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	Random

B. Results Description

The attackers (blackhole attack and DoS) in network is dumping the whole performance of network. The results are shows the poor performance of network. In this section the result description of simulation of blackhole, secure watchdog technique and proposed IDS analyzed and observed that the performance of proposed scheme is better than the watchdog detection technique.

1) *Packet Delivery Ratio Analysis:*The attacker is easily affecting the performance of MANET because of the open medium of network. The blackhole attacker and DoS attacker are the very powerful attacker and their combined effort of routing misbehaviour is really harmful for the network. In this performance the PDR performance of proposed secure IDS is excellent for the detection and prevention of these attacks in MANET. The watchdog security scheme performance is also evaluated in network but it is suitable for the detection of blackhole attack. The PDR performance of proposed IDS is about 95 % up to end of simulation and the attacker PDR is only 35% and the watchdog is 85% this is slightly less than proposed enhanced watchdog IDS. Initially the PDR is reaches to 70% but due to attacker's effect it will we continuously own in network but proposed IDS is prevent the network from attacker and provide better network performance.

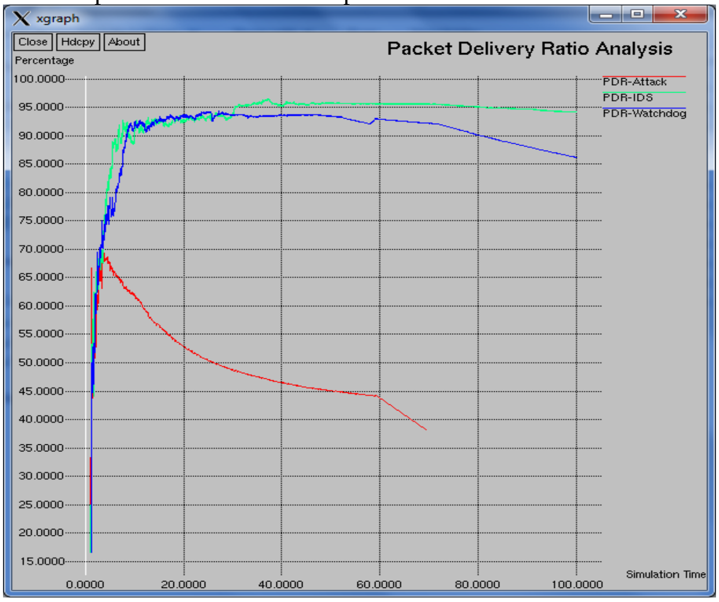

Fig: 5.3 PDR Analysis

2) *Routing Load Analysis:* The routing protocols are required in network to establish the connection in between sender and receiver. AODV routing protocol is considered in this research is for routing the packets. The sender is following the routing strategy of AODV protocol and first establishes connection to receiver and then sending the data to receiver. The request packets for connection establishment is flooding are network are routing packets. The quantity of less or routing packets as compare to data is shows the better network performance. In this research the routing packets is minimum in attack scenario due to link consumption of DoS attacker and blackhole data packets dropping but their routing load is greater than 2 that shows degradable performance of network. But the packets receiving in proposed enhanced watchdog IDS is highest due to that the routing packets are more flooded but the routing load is less than watchdog security scheme that shows better network performance.

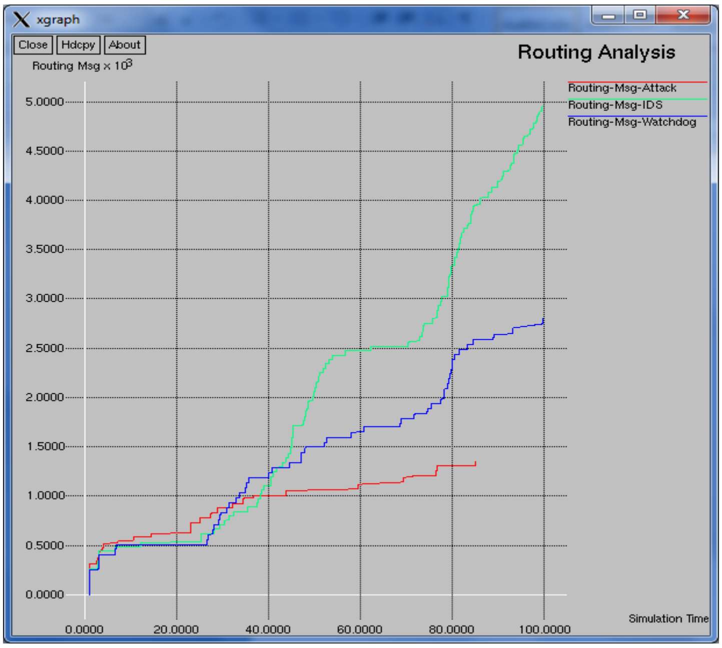

Fig: 5.4 Routing Overhead Analysis

3) *Attack Analysis without Watchdog:* The attacker aim is to dump the network performance by consumes resources and dropping packets through routing misbehaviour. In this graph the observe the loss percentage of DoS attacker, routing attack i.e. blackhole attack and loss in case of watchdog applied on DoS attack. That result shows the deficiency of watchdog security mechanism. The infection of DoS is about 23% and the infection of routing attack is about 24% but the infection in watchdog applied on DoS is also count in network it is about 9% in network. That shows the Watch dog minimizes the DoS effect but not fully protect from them. The infection of proposed enhanced watchdog IDS security is counting zero that sows the reliability and better performance in existence of attacker.

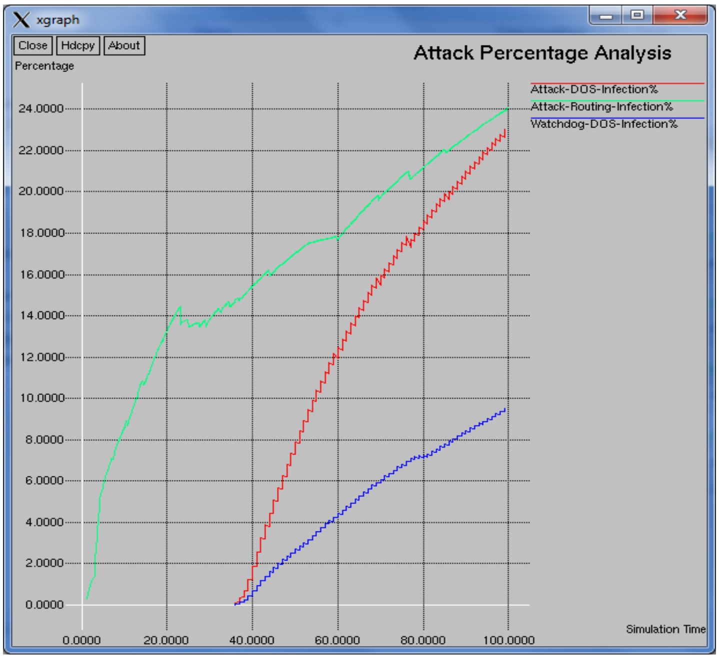

Fig. 5.5 without Wathchdog Attacker Analysis

4) *Throughput Analysis:* The throughput of the network is shows the better data sending and receiving in network. The data packets receiving are important in network because of the better performance. The packets receiving in a unit time is represents the throughput performance in network. The attacker is loss the data in the middle of link by consuming the bandwidth and by not forwarding to destination if bandwidth is available. In this graph the throughput performance of attacker is very poor and only countable up to 70 seconds. Only about 500 packets receiving is highest counting at starting of simulation and after that the performance is continuously down with respect to time. The throughput performance of proposed IDS scheme is highest and provides better about more than 1200 packst/second in network. The watch dog performance is slightly less due to the presence of DoS attacker in network but proposed IDS is suitable for both attackers.

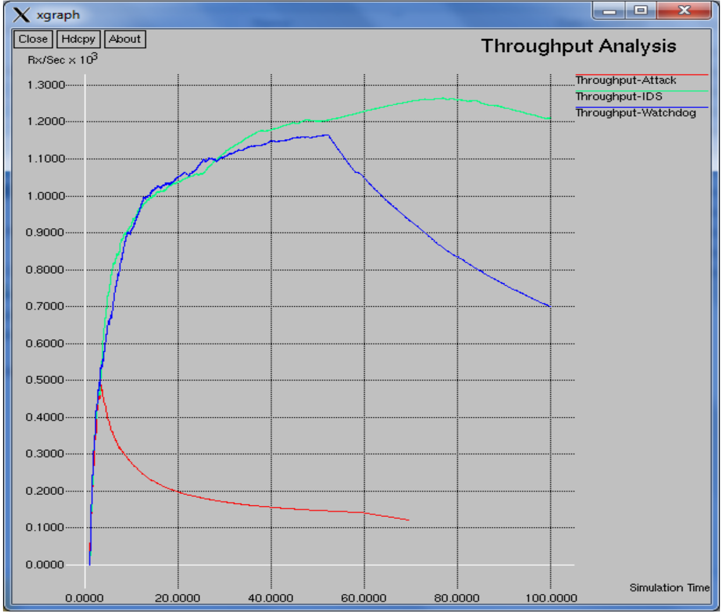

Fig:5.6 Throughput Performance Analysis

5) *UDP Transmission Analysis:*The good quantity of transmission of packets is shows the senders are not restricted for communication to receiver in dynamic network. They are free and send their data to receiver at any time. The User Datagram Protocol (UDP) is the transport layer unreliable protocol for communication. In this protocol the senders are continuously sends the data up to end of simulation, without any confirmation of receiving. If the network conditions are not supportive then in that case the performance degradation is sure in network. The packets transmission of senders in attacker scenario is negligible to count network performance. It is only 80 packets. The packets transmission of watchdog is not much better in presence of attackers but the performance of proposed enhanced watchdog IDS transmission is much better that is the sigh of secure routing.

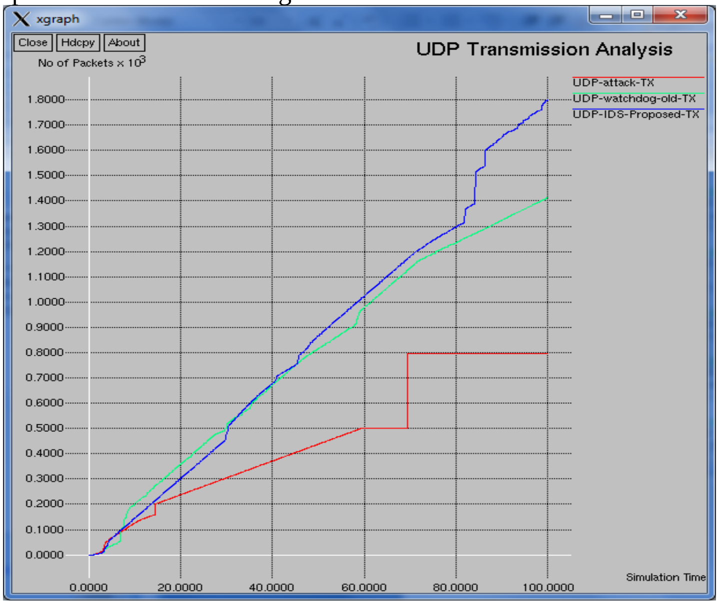

Fig. 5.7 UDP Packets Transmission Analysis

6) *UDP Receives Analysis:*The better quantity of packets receiving after better sending is shows the excellent routing performance and network conditions. The UDP end to end performance is better, if the no obstacle is

exist in network. If the attacker is dropping the packets after false reply or consumes the bandwidth from flooding then in that case UDP are continuously performs their original role. In this graph due to attackers the performance of network is degrades and only 40 packets are received in network. In watchdog prevention scheme the packets receiving is better about 1080 packets but in proposed secure enhanced watchdog IDS the packets receiving is more than 1300 packets up to end of simulation that shows the better network performance.

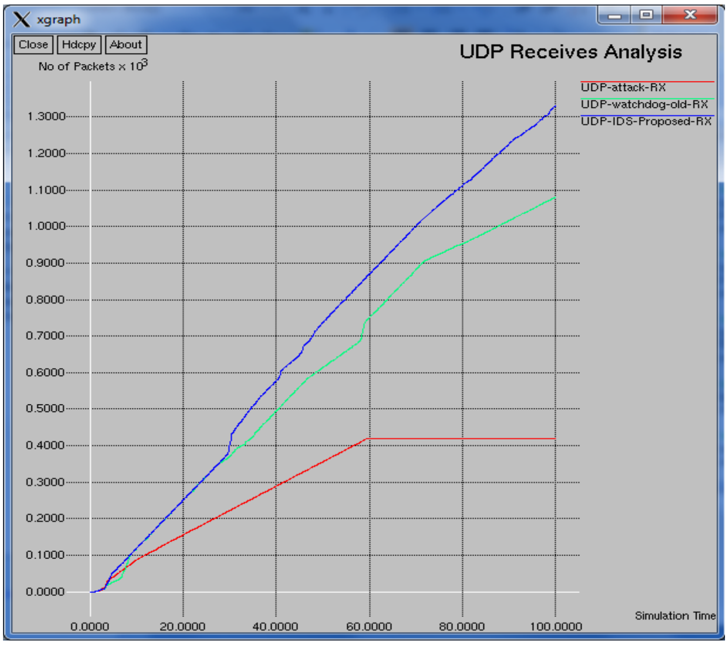

Fig. 5.8 UDP Packets Receiving Analysis

7) *Attackers Loss Analysis:*The loss in percentage in presence of blackhole and DoS attacker is mentioned in table 5.2. In this results analysis the one node 49 is of DoS attacker and the 28 and 34 is the blackhole attacker nodes. These attackers are performing their actions in network to degrade the routing performance. After applying prevention no infection from attacker is count in network.

Table 1: Attackers Loss

Attacker Analysis Without Prevention		
DOS Attacker	Packet Capture	Percentage of Infection
49	1108	22.85
Routing Attacker	Packet Capture	Percentage of Infection
28	641	13.22
34	525	10.83

8) *DoS Attacker Loss with Watchdog Mechanism:* The watchdog is not able to detect any other attack, is prove from the infection count after applying it against DoS attack. It is able to provides the security from blackhole attack surely but only minimizes the loss of DoS attack not prevent from it.

Table 2: Watchdog Analysis

Attacker Analysis With Prevention(Watchdog)		
DOS Attacker	Packet Capture	Percentage of Infection
49	1108	9.44

9) *Summarized Routing Analysis:* The better routing performance is also shows the better of network performance. The summarized routing performance of combined effect of blackhole and DoS, Wathchdog security and proposed secure IDS is mentioned in table 5.4. The evaluated values are clearly shows the performance degradation in presence of attacker and the proposed enhanced watchdog IDS is completely remove the existence of attacker that shows the efficient routing performance but the existence DoS attacker is not removed by watchdog scheme by that their performance is slightly lower.

Table 3: Summarizes Performance Analysis

Parameter	Attack Case	Watchdog Case	Proposed Case
SEND	1807	4591	7286
RECV	491	3957	6864
ROUTINGPKTS	1350	2800	4952
DOS Attack	1108	1108	0
Routing Attack	1166	0	0
PDF	27.17	86.19	94.21
NRL	2.75	0.71	0.72
Average e-e delay(ms)	88.71	195.5	172.93
No. of dropped data (packets)	1314	634	421
No. of dropped data (bytes)	1341000	646960	431460

V. CONCLUSIONS AND FUTURE SCOPE

Mobile ad-hoc network routing strategies is one of the challenging task to establish route between sources to receiver. In this thesis we analyze the routing attack protection and provide reliable communication. Initially we identify reason of data drop and detect attacker node. After that we prevent the network by attack symptoms based message sending mechanism and get 100 percent recovery through attack behavior and measure quality of service with the help of packet delivery ratio. Result concludes that if we apply message sending based collaborative security mechanisms, our network quality of service is excellent where attack node is present in the network and protected by our technique. In future we can also apply ODMRP routing and Dream location base routing and minimize overhead of the network. Further we can also detect denial of service, wormhole attack etc. using updated security approach.

REFERENCES

[1] Tarun Varshney,Tushar Sharmaa,Pankaj Sharma “Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network” 2014 Fourth International Conference on Communication Systems and Network Technologies.

[2] A.Babu Karuppiah, T.Meenakshi, T.I.Mano Ranjitha & S.Vivitha, " False Misbehaviour Elimination in Watchdog Monitoring System Using Change Point in a Wireless Sensor Network", An International Journal on Graduate Research in Engineering and Technology (GRET), pp. 31-35, 2013.

[3] S. Nishanthi, "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.

[4] Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F.Loureiro and L.B. Ruiz, "Decentralized Intrusion Detection In Wireless Sensor Networks" Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, (QSSWMN; 25), pp: 16-23, 2005.

[5] Xie, M., S. Han, B. Tian and S. Parvin, "Anomaly detection in wireless sensor networks: A survey" Journal of Network and Computer Application, pp.1302-1325, 2011.

[6] A.Rajaram. Dr. S. Palaniswami “Malicious Node Detection System for Mobile Ad- hoc Networks” A.Rajaram et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85.

[7] Md Tanzilur Rahman, Kunal Gupta, “MANET: Security Aspects and Challenges” International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6–June 2013.

[8] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “Identity-based Attacks Against Reputation-based Systems in MANETs” ISBN: 978-1-902560-25-0 2011 PGNet.

[9] Sukhbir Kamboj, Mohit Dua “Comparison Study of Various DoS Node Detection Schemes in MANETs” Sukhbir Kamboj et al. / International Journal on Computer Science and Emerging Trends (IJCSET) Vol. 02, No.01, 2013, 8-15.

[10] Sarosh Hashmi, John Brooke, “Towards Sybil Resistant Authentication in Mobile Ad hoc Networks” 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies.

[11] R. Ogier, F. Templin, and M. Lewis, "Topology dissemination based on reverse path forwarding (TBRPF)," in IETF RFC 3684, Feb. 2004.

[12] Martha Steenstrup, “Routing in communication networks”. New Jersey, Prentice Hall. ISBN 0-13-010752-2.

[13] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance- Vector Routing (DSDV) for Mobile Computers", Comp. Comm. Rev., Oct. 1994, pp.234-244.

[14] Larry L. Peterson and Bruce S. Davie, “Computer Networks -A Systems Approach”. San Francisco, Morgan Kaufmann Publishers Inc. ISBN 1-55860- 368-9.

[15] http://wiki.uni.lu/secan-lab/Ad-Hoc+Protocols ($28) Classification ($29).html.

[16] David Johnson, David Maltz, Yih-Chun Hu: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, draft-ietf-manetdsr- 10.txt, work in progress, pp. 153-181, July 2004 .

[17] Vincent D. Park and M. Scott Corson, “Temporally-Ordered Routing Algorithm (TORA) Version 1: Functional specification”. Internet draft, draft-ietf-manettora- spec-01.txt, August 1998.

[18] Josh Broch, David B. Johnsson, David A. Maltz, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks”. Internet Draft, draft-ietf-manet-dsr- 00.txt, March 1998.

[19] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. "A review of routing protocols for mobile ad hoc networks. Technical report", Telecommunication and Information Research Institute, University of Wollongong 2003.

[20] zygmunt j. Haas, marc r. Pearlman, prince samar the Zone Routing Protocol (ZRP) for Ad Hoc Networks, July 2002.

[21] V. Rishiwal, M. Yadav, S. Verma, S. K. Bajapai, “Power Aware Routing in Ad Hoc Wireless Networks", Journal of Computer Science and Technology, vol. 9, no. 2, pp. 101-109, October 2009.

[22] Sonia Boora, Yogesh Kumar, Bhawna Kochar, “A Survey on Security Issues in Mobile Ad-Hoc Networks”, International Journal of Computer Science & Management Studies, Vol. 11, Issue 02, August 2011 .