Journal of Theoretical and Applied Information Technology
30th September 2014. Vol. 67 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURED DATA TRANSMISSION METHOD USING ENHANCED PROACTIVE SECRET SHARING SCHEME TO PREVENT BLACK HOLE ATTACKS IN MANETS

[1]K.SELVAVINAYAKI , [2]DR. E. KARTHIKEYAN

[1]Asst Professor, Karpagam Institute of Technology , Coimbatore, India,

[2] Asst Professor, Department of Computer Science, Govt. Arts College, Udumalpet, India

E-mail: [1] uk.selvavinayaki@gmail.com , [2]e_karthi@yahoo.com

ABSTRACT

Mobile Ad hoc Networks consist of mobile nodes which are running randomly. Nodes communicate with each other without any access point. Due to mobility of nodes, network is easily affected by several types of attacks. In particular black hole attack cause packet dropping, misrouting the information from source to destination. To reduce the effect of this attack, we propose a New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to detect the black hole nodes and to ensure the data confidentiality, data integrity and authenticity. In first phase of the proposed algorithm, the detection of black hole attack is achieved using trust active and recommendation of the nodes. In second phase of the work, Enhanced Proactive secret sharing scheme is used to provide the data authentication and integrity. The simulation results shows the proposed algorithm achieves the better packet delivery ratio, misbehaviour detection efficiency, fewer packets overhead and low end to end delay than the existing schemes.

Keywords – *MANET, Black Hole Attack, Enhanced Proactive Secret Sharing Scheme, End to End delay, Control overhead, Misbehaviour Detection Efficiency and Delivery ratio.*

1. INTRODUCTION

MANET (Mobile Adhoc Network) has not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of the application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks.[1]

1.2. Black Hole Attack

In this type of attack, node is used to advertise a zero metric to all destinations, which makes all nodes around it to route data packets towards it. The AOMDV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to share their routing tables among each other.

A malicious node may use the routing protocol to advertise itself of having the shortest path to the node whose packets it wants to intercept. When a source node wants to send data packets to a destination node, if there is no route available in its Routing Table (RT), it will initiate the routing discovery process.

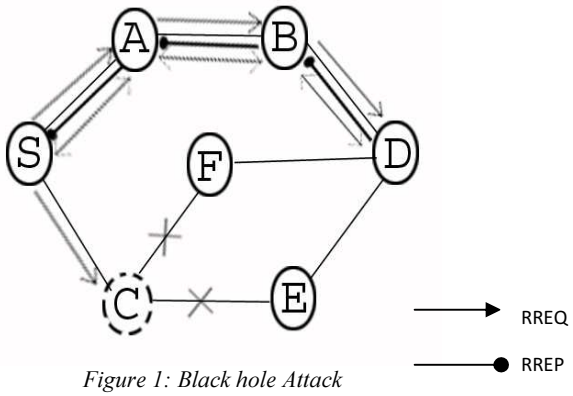

Figure 1: Black hole Attack

For example in Figure1, assume node C to be a malicious node. Using the AOMDV routing protocol, node C claims that it has the route to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

If the reply from a normal destination node reaches the source node of RREQ first, everything works well, but the reply from node C could reach the source node first, if node C is nearer to the source node. Moreover, node C does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node to think that the routing discovery process is completed and queues all other reply messages in the routing table, and begin to send data packets. The forged route has been created. As a result, all the packets through node C are simply consumed or lost. Node C could be said to form a black hole in the network, and we call it as the black hole attack.[10]

2. RELATED WORK

Latha Tamil Selvan et al [2] introduced the use of a Fidelity Table where in every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated.

D. Dhillon et al [3] porposed the methodology using the certificate authority . PKI (Public Key Infrastructure) based security is deemed more appropriate for MANETs.The Approach tightly couples the PKI with OLSR Routing protocol and Distributed Certificate Authority is fully implemented.

Sanjay Ramaswamy, et al [5] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

Marti, S, et al [7] have proposed a Watchdog and Path rater approach against black hole attack which is implemented on top of source routing protocol such as DSR (Dynamic Source Routing).

S. Djahel et al [6] proposed a three hops acknowledgment based scheme to cope with the cooperative black hole attack in OLSR. This scheme adds two extra packets to OLSR, Hello rep packet which is a slight modification to Hello message and a small acknowledgment packet. In this solution, each MPR node M acquires the list of its 3-hop neighbors reached through a distinct pairs of two consecutive MPR nodes (M1, M2), where M2 is the MPR node of M1 and this latter is the MPR of the node M. Afterwards, the node M selects one node, from this list, to which it requests an authenticated acknowledgment as a confirmation of the reception of the data.

Soufiene Djahel et at [9] made a comprehensive survey investigation on the state-of-the-art countermeasures to deal with the packet dropping attack. Furthermore, Authors examined the challenges that remain to be tackled by researchers for constructing an in-depth defense against such a sophisticated attack.

Umang et al [4] proposed a novel approach for enhanced intrusion detection system for malicious node to protect against attacks in ad hoc on-demand distance vector routing protocol. The proposed approach employs a method for determining conditions under which malicious node should be monitored. Apart from identification of malicious node, it has been observed that this approach leads to less conservation and less communication breakage in ad hoc routing.

Stanislaw Jarecki et al[8] proposed proactive RSA signature scheme which is assumed to be secure as long as no more than an allowed threshold of participating members is simultaneously corrupted at any point in the lifetime of the scheme. In this paper, the authors has shown an attack on this proposed proactive RSA scheme, in which an admissible threshold of malicious group members can completely recover the group RSA secret key in the course of the lifetime of this scheme.

Amol A. Bhosle et.al [10] proposed the watchdog mechanism to detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provides a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. They also proposed the time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.

N.Bhalaji et.al [11] presented a trust based routing model to deal with black hole and cooperative black hole attacks that are caused by malicious nodes. We believe that fellowship model is a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyze the cooperative black hole attack over the proposed scheme to analyze its performance. The next step will consist of analyzing the protocol over Grey hole and cooperative grey hole attacks.

Djamel Djenouri et al [14] presented a hybrid solution that considers both directed and broadcast control packets. It combines two different approaches, two-hop-ACK and the watchdog, to building a combined solution able to deal with both directed and broadcast packets.

The paper is organised as follows. The Section 1 describes the introduction about the overview of MANETs and Black Hole Attacks. Section 2 deals with the related work which describes about the previously available solution to overcome the black hole Attack. Section 3 describes the implementation of the proposed algorithm. Section $ describes the Performance analysis of the proposed algorithm and Last section includes the conclusion of the work.

3. IMPLEMENTATION OF PROPOSED ALGORITHM

New Enhanced Proactive Secret Sharing Scheme (NPSSS) is implemented in terms of two stages like Black Hole Attack detection and Secret Sharing Procedure to ensure the authenticity of information being carried between source and destination node.
NEPSS is implemented on AOMDV protocol. The key concept in AOMDV is computing multiple loop-free paths per route discovery. With multiple redundant paths available, the protocol switches routes to a different path when an earlier path fails. Thus a new route discovery is avoided. Route discovery is initiated only when all paths to a specific destination fail. For efficiency, only link disjoint paths are computed so that the paths fail independently of each other. Multi path routes can be used to reduce the routing overhead rather than load balancing.[12]. As per the NEPSS scheme RREQ packet and RREP packets are modified to hold additional information which is discussed below.

3.1.Detection of Black hole attacks

As in Figure1, Assume Source S wants to communicate with Destination node D. Here A and B are the intermediate nodes. Source broadcasts the request message RREQ. RREQ includes the level of security it requires and D's id, a sequential number and Pb D [Sid] is the Source's id encrypted by Destination's public key and Trust Active. RREQ packet is modified as following :{ RREQ, seq_num, Pb D [Si d], Did, TA}. Where TA is a time-dependent Trust Active value. Initially node A have the trust value on node B at time t1.But after a certain period, node B may travel to another zone which is out of radio range of node A ,due to nodes mobility in MANET. At time t2, node B happens to be back in node A's radio range again. The trust value should decay during this time gap. Let ATB (t1) be the trust value of node A to node B at time t1 and ATB (t2) be the decayed value of the same at time t2. Then trust active is defined as follows,

$$ {}_AT_B(t_2) = {}_AT_B(t_1) * e^{-({}_AT_B(n)\Delta t)^{2k}} \quad (1) $$

Node A receives RREQ. It looks up its trust list for the trust values of the neighbours. And A will encrypt its own id with proper policy and append in the message. The message which is sent by A will be in the form of :{RREQ, seq_num, Pb D[Pv A[Aid], PbD[Sid], Did , R_N^M } where Pv A is the private key of A. Where Node proposal R_N^M is also used to identify the malicious behavior. Evaluating the recommendation is given by R_N^M which is node M's evaluation to node N by collecting recommendations,

$$ R_N^M = \frac{\sum_{\upsilon \in \gamma} V \mid M \rightarrow P \mid * V \mid P \rightarrow N \mid}{V \mid M \rightarrow P \mid} \quad (2) $$

γ is a group of recommenders.
$V \mid M \rightarrow P \mid$ is trust vector of node M to P.
$V \mid P \rightarrow N \mid$ is trust vector of node P to N.
Now Node B receives the RREQ from Node A and repeat the same procedure followed by Node A.

D receives RREQ from B. It uses its private key and the public key of the intermediate nodes to authenticate them. D checks whether there are any malicious nodes. If they are all trusted, D generates a flow Fid , and broadcasts the following message (As in Figure 1, A and B are the intermediate nodes):

{RREP,Pb B[Fid , Pb A[Fid , Pb S[Pv D[Fid]]]};

Journal of Theoretical and Applied Information Technology
30th September 2014. Vol. 67 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Intermediate node that receives the RREP uses its private key to decrypt the message and gets the flow id. Then it updates its route table with Fid designated to destination D.S receives RREP, uses its private key to decrypt the message and D's public key to identify the destination. Afterwards, it will send message with the flow id Fid.Cluster Head maintains the Trust threshold value based on trust active and node proposal to detect the attacks. If any nodes have the value below the Trust threshold value then that node is encountered by a black hole attack.

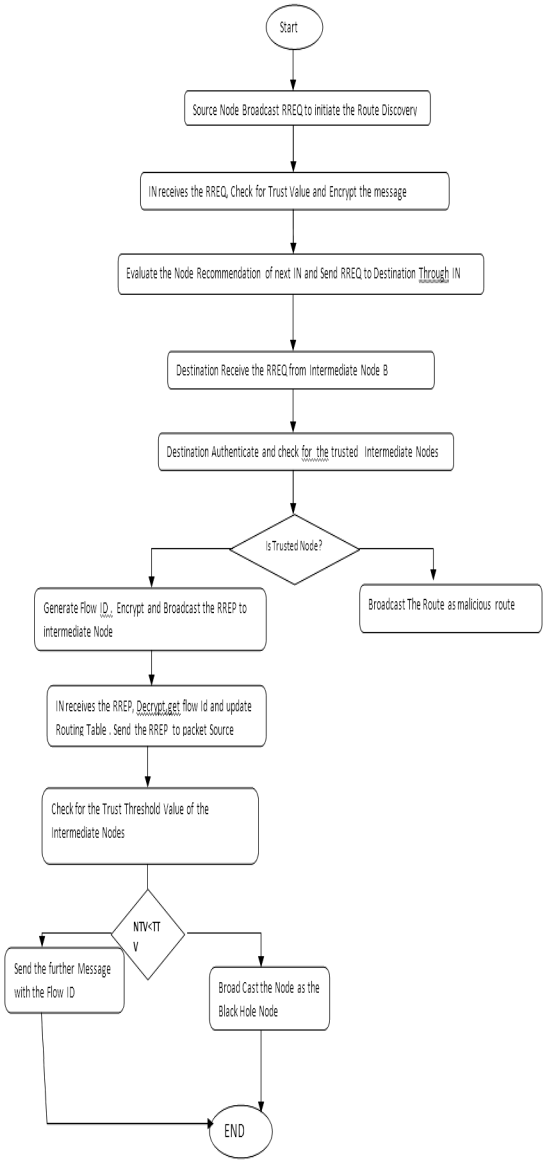

Figure2 : Flow chart for Black Hole Node Detection Process.

Figure 2 clearly illustrates the Black Hole Detection process during the Route Discovery process.

2.2. Enhanced Proactive Secret Sharing Procedure for Authenticated Information Transmission.

Proactive secret sharing scheme is a method used to update the shares in the secret sharing scheme periodically, so that the attackers have less time to comprise the secret. The sub shares from secret can be constructed and old shares are invalidated.[15]. This feature unable the compromisers to reveal the secret. To ensure the authenticity of the information transferred we propose the Enhanced proactive secret sharing scheme. Various stages of Enhanced proactive secret sharing scheme is as follows.

A. Secret share generation.
B. Initiation of the Sharing process.
C. Verify and authenticate the digital signature.

2.2.1. Secret share generation

Let (S1, S2, ……..Sn) be an (t,n) secret shares of the secret key S of the service with the node k having Sk[13]. When Sk, is defined from a finite field D = Zr and g is a primitive element in F. Node K (K $\in$ {1,2,3,….n}) which randomly generates Sk's sub shares like (Si1, Si2, ….. Sin) for (t.n) sharing. All subshares Skp (p $\in$ {1,2,3,….n}) is distributed to node p through the secure link. When node j gets the sub shares {S1k, S2k, ….. Snk}. It computes a new share from these sub shares and its old share with an equation.

$$S_p^{'} = S_p + \sum_{k=1}^{n} S_{k,p} \quad (3)$$

2.2.2. Initiation Of The Sharing Process

Source Node A sends its Secret sharing flag M_start to all the share holder nodes. All Share holder nodes send the M_start_ack flag to the share holder node M. Sharing procedure is initiated.
The intermediate node sends the refresh flag to all share holder nodes . All nodes refresh its share to send shares to other share holder nodes with digital signature and encrypted public key of destination nodes.

Journal of Theoretical and Applied Information Technology
30th September 2014. Vol. 67 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1.3.3.Verify and authenticate the digital signature.

The digital signature is verified using the proposed digital signature algorithm. Here, the public key F, message m, signature (p,q) is used in the input of signature verification. In output, the validation of digital signature is performed.

The verification procedure is followed as,
The signature (p,q) is the integers in between the interval [1,N-1]. If any verification fails, then the signature will be rejected. N is the order of the system.
The encryption value is calculated by

$$e = H(m) \quad (4)$$

H denotes a hash function whose outputs has bit length not more than that of N.

The integer value is calculated as

$$v = q^{-1} \bmod N \quad (5)$$

This integer is used to calculate the value of order of N. It is used to verify the signature of the q with respect to order N of the system.

Convert the u_1 coordinate of U in to an integer $\bar{u}_1$.

Determine $y = \bar{u}_1 \bmod N$. (6)

If a signature (p,q) presents on the message m which is generated by the signer (destination node signature), then q =s-1 (e+cp) (mod N).

The shares are reshuffled as
s= p-1 (e+cp) = p-1e+p-1cp = ve+vcp = z1 + z2c (mod N). (7)

Thus X = (z1 + z2c) W = sW, and y=p as required. If y=p then the signature is accepted. Otherwise it is rejected.

Send end flag to all share holder nodes. After receiving this end flag, send_ack flag again and send refresh_end flag to all share holder nodes.

The secret key is reconstructed. If Sk holds shares (m1, n1) and Sp hold shares (m2, n2), then the share holder node reconstructs the secret. If m1 = m2, then the secret is n1, otherwise the secret is n2. The reconstructed share reaches the destination. This verified secret shares cannot be intruded by any of the black hole node.

4. PERFORMANCE ANALYSIS

Network Simulator (NS2.34) tool is used to simulate our proposed algorithm. In our simulation, 100 mobile nodes move in a 1200 meter x 1200 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in Table 1.

Table 1. Simulation Settings and Parameters

No. of Nodes	100
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Package rate	5 pkt/s
Protocol	AOMDV

4.1. Performance Metrics

We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is the ratio of packet received to packet sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the sink receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the sink is also important because based on that number the sink, can possibly take an appropriate action to reduce the redundancy.

Journal of Theoretical and Applied Information Technology
30th September 2014. Vol. 67 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Throughput: It is defined as the number of packets received successfully.

4.2. Results and Discussion

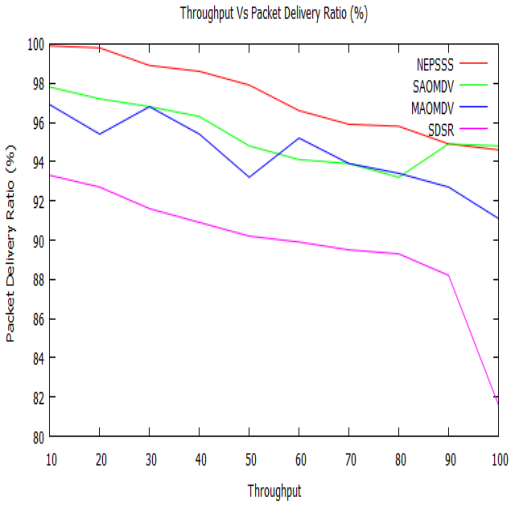

Figure 3.Throughput Vs Data delivery ratio

Figure 3 shows the results of packet delivery ratio for varying the throughout from 10 to 100. From the results, we can see that NEPSSS scheme has higher delivery ratio of range from 99.9 to 94.6. SAOMDV has the packet delivery ratio in the range of 97.8 to 93.2. MAOMDV has the packet delivery ratio in the range of 96.9 to 91.1 and SDSR has the packet delivery ratio in the range of 93.3 to 81.6. NEPSSS has highest packet delivery ratio because of the reliable data delivery by using the secret sharing scheme.

Figure 4 shows the results of detection efficiency for varying the mobility from 0 to 50. From the results, we can see that NEPSSS scheme has higher detection efficiency than the SAOMDV, MAOMDV and SDSR schemes. NEPSSS has the Higher detection efficiency in the range of 45.2 to 99.3. SAOMDV has the detection efficiency in the range from 26.2 to 88.3 . MAOMDV has the detection efficiency in the range of 16.4 to 80.3. SDSR has lower detection efficiency in the range of 15.5 to 67.3.

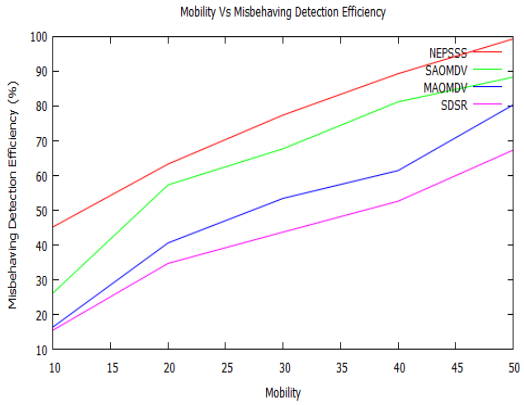

Figure 4.Mobility Vs Misbehaviour Detection Efficiency

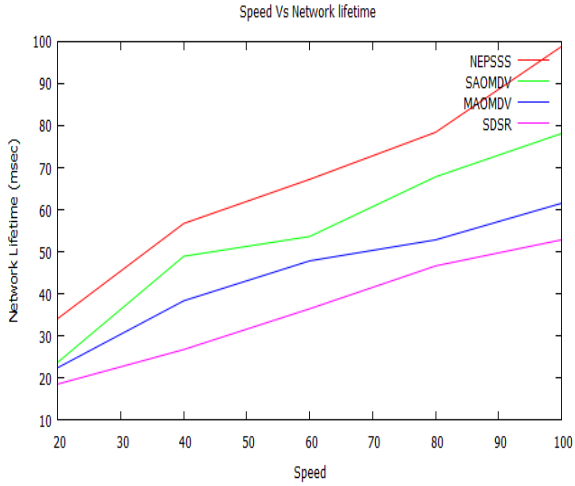

Figure 5.No.of nodes Vs Network Lifetime

Figure 5 shows the results of network lifetime for varying the mobility from 20 to 100. From the results, we can see that NEPSSS scheme has network lifetime than the SAOMDV, MAOMDV and SDSR. The network life time of NEPSSS lies in the range of 34.1 to 98.8 secs.SAMODV has the life time of 23.7 to 78.1 secs. MAOMDV has the life time of 22.4 to 61.5 secs and SDSR has the life time of 18.5 to 52.8 secs.

Figure 6 shows the results of Time Vs End to end delay. From the results, we can see that delay of NEPSS is lower than the SAOMDV, MAOMDV and SDSR while varying the nodes form 10 to 100.NEPSSS has the delay value in the range of 1.8 to 14.2 msecs.SAOMDV has the delay value of 8.2 to 48.8 msecs. MAOMDV has the delay ratio lying between 7.4 and 22.1 msecs. SDSR has the delay value in the range of 9.7 to 77.3 msecs.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

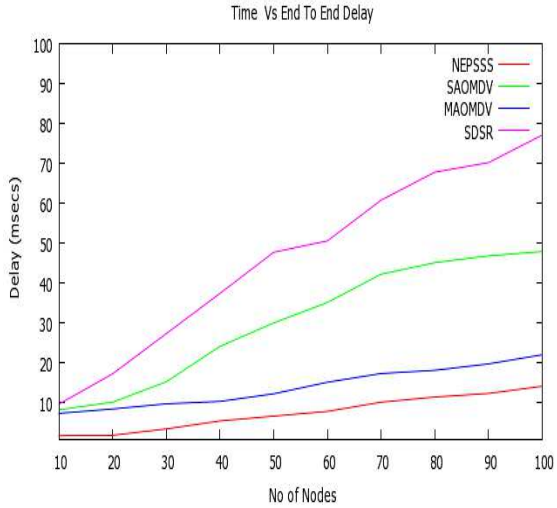

Figure 6.Time Vs End to end delay

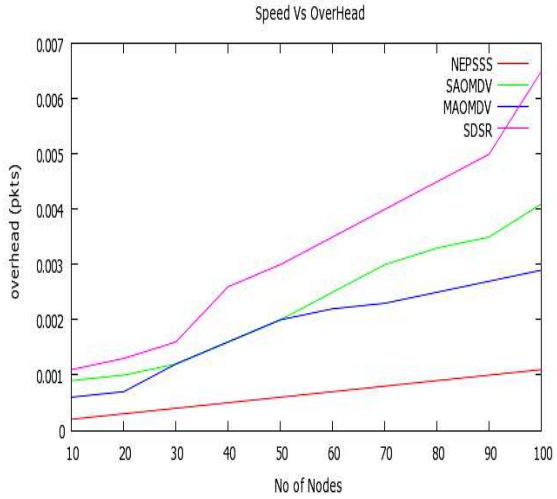

Figure 7.Speed Vs Overhead

Figure 7, presents the comparison of overhead and speed. It is clearly shown that the overhead of NEPSSS is a low overhead than the SAOMDV, MAOMDV and SDSR schemes. NEPSSS has the lowest overhead in the range of 0.0002 to 0.0011(pkts). SAOMDV has the overhead in the range of 0.0009-0.0041(pkts). MAOMDV has the over head ratio in the range of 0.0006-0.0029(pkts) and SDSR seems to have higher over head which is in the range of 0.0011-0.0065 (pkts).NEPSSS has the lowest overhead because the route discovery process is not initiated as soon as the route to the destination fails. Instead the alternate route is selected.

5. CONCLUSION

Mobile Ad hoc Networks consist of mobile nodes without any centralized infrastructure. Here node may be affected by several attacks. It may cause the packet dropping, misrouting the information to another destination. In our proposed work, we focus on detection of the black hole attacks. This attack degrades the performance of the mobile ad hoc networks. So that, we propose the New Enhanced Proactive Secret Sharing scheme to detect the black hole attacks. In first phase, the black hole attack is detected and isolated. In second phase, the authentication of data packets and data integrity is provided using the proposed secret sharing scheme. In third phase of the scheme, the energy consumption model is proposed to make minimum energy consumption of the nodes. By using the extensive simulation results, the proposed scheme achieves better results than the existing schemes SAOMDV, MAOMDV and SDSR schemes.

REFERENCES

[1] D.Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4,4th Quarter 2005.

[2] Tamilselvan, L. Sankaranarayanan.V, Prevention of Blackhole Attack in MANET,JournalOfNetworks ,Vol.3,No.5,May2008.

[3]Dhillon,D.Randhawa,,T.S.Wang,M.Lamont.L,,Implementing a fully distributed certificate authority in an OLSR MANET, IEEE. Wireless Communications and Networking Conference,2004.-WCNC2004

[4] Umang, S. Reddy, B.V.R.Hoda M.N.,Enhanced Intrusion Detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption Communications,IET,**Vol:**4 ,Issue:17 November2010

[5] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ,Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks,2003 International Conference on WirelessNetworks (ICWN‟03), Las Vegas, Nevada, USA.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] S.Djahel, F. Na¨ıt-Abdesselam and A. Khokhar,, An Acknowledgment-Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol, In Proc. of the InternationalConference on Communication (ICC 2008), beijing, China, May 2008

[7] Marti, S.,Giuli,T.J.,Lai,K.,& Baker, M.(2000),Mitigating routing misbehavior in mobile ad-hocnetworks, Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom).

[8] Stanisław Jarecki and Nitesh Saxena, On the Insecurity of Proactive RSA in the URSA Mobile Ad Hoc Network Access Control Protocol, IEEE Transactions On Information Forensics And Security, Vol. 5, No.4, DECEMBER 2010

[9] Soufiene Djahel, Farid Naıt-abdesselam, and Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, IEEE Communications Surveys & Tutorials, vol. 13, no. 4, Fourth Quarter 2011

[10] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012, pp.45-54.

[11] N. Bhalaji and A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, Vol.50, No.1, 2011, pp.6-15.

[12] Mahesh K. Marina Samir R. Das , On-demand Multipath Distance Vector Routingin Ad Hoc Networks- WIRELESS COMMUNICATIONS AND MOBILE COMPUTING Wirel. Commun. Mob. Comput. 2006; 6:969–988Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.432.

[13] A. Shamir, How to Share a Secret, Communications of the ACM, 22(11):612-613, November 1979.

[14] Djamel Djenouri,Mohamed Bouamama and Othmane Mahmoudi, Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks, Int. J. Security and Networks, Vol. 4, No. 4, 2009.

[15] Yevdokimov, Aleksey . "Dynamic system of proactive security". Application of Information and Communication Technologies, 2009. AICT 2009.