An Effectual Data Transmission Approach to Prevent Black Hole Attack in Mobile Adhoc Networks

Dr.K.Selvavinayaki
Professor
Department of Computer Applications
Nehru Arts and Science College, Coimbatore
Email: uk.selvavinayaki@gmail.com

ABSTRACT

The dynamic nature of infrastructure in MANET makes security as a critical issue. 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 prevent a network from the effects of the black hole attack, we propose a most reliable data transfer scheme to detect the black hole nodes in the network and ensure the availability, reliability, confidentiality of the information. First, the proposed scheme detects the black hole node using trust active and node recommendation values. Second, the reliability and confidentiality of the information is achieved by using verifiable secret sharing scheme. The proposed algorithm is implemented on AOMDV protocol. The simulation results show the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packets overhead and low end to end delay than the existing schemes.

Keywords – MANET, Black Hole Attack, Verifiable Secret Sharing Scheme, reliability, AOMDV, End to End delay, Control overhead, Misbehavior Detection Efficiency and Delivery ratio.

1.INTRODUCTION

Mobile Ad-Hoc network is a self configurable, self organizing and infrastructure less multihop mobile wireless network. Security in MANET is a complex issue. This is because of insecure wireless communication link, absence of fixed infrastructure, node mobility, dynamic topology and bandwidth limitation. The main role of routing protocol is to establish an efficient, optimal and secure route between the nodes. Any kind of attack in MANET will disturb the entire communication and the total network can be collapsed. The security issues in MANET become tedious with multiple numbers of nodes. There are many attacks by the compromised nodes that collapse the network and make it unreliable for communication.

1.1. 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 [11]. The

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

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. For example, in Figure1.1, 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.

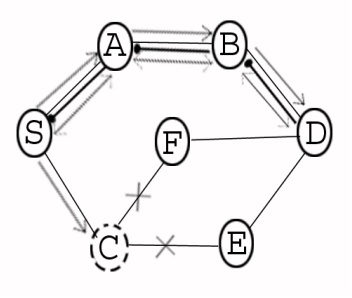


Figure1.1: Black hole Attack

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 first. 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.

1.2. AOMDV

Ad-hoc on demand Multipath Distance Vector Routing (AOMDV) protocol [18] is an extension to the AODV protocol for computing multiple loop-free and link disjoint paths. The routing entries for each destination contain a list of the next hops along with the corresponding hop counts. All the next hops have the same sequence number. This helps in keeping track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination. Each duplicate route advertisement received by a node defines an alternate path to the destination. Loop freedom is assured for a node by accepting RREQ te paths to destination if it has RREP) count than the advertised hop count for that destination. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a route advertisement is received for a destination with a greater sequence number, the next-hop list and the advertised hop count are reinitialized. The advantage of using AOMDV is that it allows intermediate nodes to reply to

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

RREQs, while still selecting disjoint paths.

1.3 Verifiable Secret Sharing Scheme.

Verifiable secret sharing scheme based on Shamir's secret sharing scheme [6] allow the shareholders to determine whether the dealer sent them valid shares of the secret, hence allowing them to come to a consensus regarding whether the secret was shared successfully. In this framework, the dealer is semi-trusted; it does not reveal the secret, but it might attempt to fool servers into accepting an invalid sharing of the secret. Verifiable secret sharing is an important component in many distributed secret sharing protocols involving untrusted participants because the protocols typically involve each node acting as a semi-trusted dealer to all of the others.[4]

2. RELATED WORK

Cachin et al.'s [2] Asynchronous Scheme is based on resharing the shares of the secret and combining the resulting subshares to form new shares of the secret. Their paper presents a protocol for asynchronous verifiable secret sharing, then shows how to build an asynchronous proactive secret sharing scheme by having each honest shareholder create its share. Cachin et al.'s [2] protocol requires that a significant amount of information to be broadcasted by each participant to each other participant even in the absence of faults. Moreover, their protocol does not support changing the set of shareholders.

Wong, Wang, and Wing et al [8] improved the work of upon Desmedt and Jajodia in two significant ways. First, they provide a complete, implementable, network protocol. Second, their scheme is verifiable, so cheating old shareholders can't compromise the validity of the share or prevent it from completing the share. However, their scheme relies upon all of the new shareholders being honest for the duration of the protocol, which is an unrealistic assumption. Furthermore, their scheme is inefficient in the presence of malicious old shareholders because it gives the new shareholders no way to determine which old shareholders sent the wrong information.

Latha Tamil Selvan et al [21] 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 it is eliminated.

D. Dhillon et al [12] proposed 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 [14] proposed a method for identifying multiple black hole nodes. They are the first to propose solution for cooperative black hole

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

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.

Umang et al [13] 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 [20] 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 have 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 [17] 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 found 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.

Djamel Djenouri et al [19] 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.Soufiene Djahel et at [16] 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.

3. PROPOSED METHODOLOGY

The Proposed Method is implemented in terms of two stages like Black Hole Attack detection and Secret Sharing Procedure to ensure the confidentiality and reliability of information is being carried between source and destination node. The method 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

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

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. As per the proposed method RREQ packet and RREP packets are modified to hold additional information.[3],[22],[23].

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, D's id, a sequential number and Pb D [S_{id}].[22]

Pb D [S_{id}] is the Source's id encrypted by Destination's public key and Trust Active value. With Pb D [S_{id}], the public key PK and a master secret key SK are generated. For the given public/private master key pair, a private key k_{ID} for the identity ID is generated. ID can be an arbitrary string. Here the ID is assumed as the IPAddress. RREQ packet is modified as following:[22]

{RREQ (seq_num, P_b D [S_{id}], D_{id}, 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 would decay during this time gap. Let A^TB (t1) be the trust value of node A to node B at time t1 and A^TB (t2) be the decayed value of the same at time t2.

Then trust active is defined as follows,

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

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[Kid], 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 of the node. Evaluating the recommendation is given by R_N^M which is node M's evaluation to node N by collecting recommendations,

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

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

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

Figure 1, A and B are the intermediate nodes):

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

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, it uses 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 [12]. The dealer maintains the Trust threshold value based on trust active and node proposal to detect the attacks. The Trust threshold value is calculated as follows Each node keeps track of the number of packets it has forwarded through a route. Let Ps be the number of RREQ packets to be sent. Pr be the number of packets received.

$$TR = ps/pr. \quad (3)$$

TR is the success transmission ratio. The ThresholdTrust value is calculaed as

$$\text{Thresh value } T = TA * TR + R_N^M \quad (4)$$

For any node *nk* , if *Tr k* <*TRmin* , where *TR*min is the minimum transmission ratio , the node recommendation value is further decremented by α1. Otherwise, the recommendation value is increased by α1. Here α1 is the small step value.

For a node *nk* , if *Thresh value T* <*Tmin* , where *Thresh value T* is the trust threshold value, then that node is considered and marked as black hole node.

3.2 Share Generation.

Once the authenticated route is formed, the intermediate nodes in the Route will form the group of share holders. We use Proactive secret sharing scheme to generate the shares.

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. This feature prevents the compromisers to reveal the secret. To ensure the confidentiality of the shares we use modified proactive secret sharing scheme.

Let (S_1, S_2, ……...S_n) be an (t,n) secret shares of the secret key S of the service with the node k having S_k.When S_k, is defined from a finite field D = Z_r and g is a primitive element in F. Node K (K ∈{1,2, 3…. n}) which randomly generates S_k's sub shares like (S_{i1}, S_{i2}, …... S_{in}) for (t.n) sharing. All subshares S_{kp} (p ∈{1,2, 3,. n}) is distributed to node p through the secure link. When node j gets the sub shares {$S1_k$, $S2_k$, …... Sn_k}. It computes a new share from these sub shares and its old share with an equation.[5]

$$S_p^{'} = S_p + \sum_{k=1}^{n} S_{k,p} \quad \text{..... (5)}$$

Source Node A sends its Secret sharing flag M_start to all the share holder

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

nodes. All Share holder nodes send the M_start_ack flag to the share holder node M. Sharing procedure is initiated.[15]. Once if the shares are generated, Compute the encryption of the shares under the public key PK parameterised by the identity ID, and return the Cipershare c.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.

3.3 Share Verification.

Once the shares are received, receivers decrypt the shares. To decrypt the shares, receiver use the private key kID .PK is the public key and SK is the master secret key. After the shares are decrypted, they are verified for the authenticity of the shares.

The digital signature (pk,sk,id) is verified .Here the k_{ID} ,ID ,C ,(PK,SK) are given as input for the verification process. The validation of the digital signature is the outcome of the process. This operation will succeed if and only if c is a valid result of Encryption of the shares and k is the valid private key of (PK, SK, ID) for the same PK and ID. [1], [10], [7]. Verify the signature on the message using the sender's public key. If the signature is valid, then the message truly has come from the sender, and if not the sender is a black hole node.It is essential to Check that the sender provided its correct private key for decrypting the messages sent to it. This can be accomplished by encrypting a random message using the sender 's well-known public key, then decrypting it with the supplied private key and comparing the result to the original random message.

Decrypt the encrypted contents using the private key provided by the sender. On decryption it returns the original message of the share. This operation will succeed only if the Cipershare c is a valid result of the encryption of the share. And the private key kID $_{is}$ the valid output for *PK* and *ID*. If the contents are not in the appropriate format or do not decrypt properly, the sender is a malicious node. [9].

3.4 Share Redistribution.

Once if any malicious node is found in the current route, the current route is skipped and alternate route can be selected from the routes that is been already discovered by the AOMDV protocol. Once if the black hole nodes are identified in the current route, then we can redistribute the shares to the new route. The intermediate nodes in the current route will be the old group of nodes. And the intermediate nodes in the alternate route will form the new group of nodes. The new group of nodes are completely disjoint from the old group of nodes. The proactive secret sharing scheme is modified in such way to redistribute the shares from the old group to the new group with out revealing any information about the shares. Since the black hole nodes can corrupt up to *t-1* in a group of nodes, in

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

this system it can control *2t* nodes between the two groups. The members of the old and new groups must be distinct sets of distinct nodes. Let *Si* refer to the ith member of the old group and Tk refer to the kth member of the new group.

The set of nodes identifier for the old group be {*a1, a2, . . ., an*} and the set of nodes identifier for the new group be {*b1, b2, . . ., bn*}. Hence, ai is the identifier of node Si and *bk* is the identifier for *Tk,* and there is the restriction that for all i and k, ai is not equal *bk* unless Si is the same machine as Tk. This notation allows us to refer to both the old and new group members using the indices 1 through n, even though their identifier sets are disjoint and need not follow any particular pattern.

While generating the shares, instead of computing *P(ak)+Q(ak)* in the old group and sending it to Tk, each old node Si computes *P(ai) +Q(ai) + Rj(ai))* and sends this point to Tk. Upon receiving at least t+1 such points, Tk can interpolate to obtain the polynomial P + *Q* + *Rk*, then evaluate this polynomial at _k to obtain *P(bk) + Q(bk) + Rj(bk) = P(bk) + Q(bk) = P′(bk*).[24].

Since Rj is random everywhere except at *bk*, this polynomial provides the new node *Tk* no additional knowledge except P′(bk). Furthermore, the old nodes learn nothing about the new share *P′(bk)* because each old node only knows a single point on any given polynomial *P +Q+Rk*, and this polynomial is random and independent of P′ except at bk. No old shareholder and new shareholder have the same identifier. Otherwise, Si would be able to learn *Q(aj) = Q(aj) + Ri(aj)* and compute *P′(aj) = P(aj)+Q(aj).* One way is to give each node an identifier that is unique across the entire system. This identifier might simply be a cryptographic hash of the node's public key. Hence this scheme ensures the reliability of the messages by using a secure distribution scheme which does not allow the black hole node to learn any information about the shares.

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 m x 1200 m square region for 60 seconds simulation time.

4.1 Results and Discussion

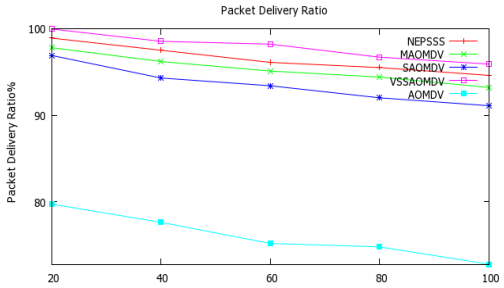
The Performance of the proposed algorithm is evaluated based on the various performance metrics like Packet delivery ratio, Average End to End Delay time, Routing Overhead, Average Through put, Misbehavior Detection Efficiency Ratio, Network Life Time. The simulation is carried out by varying the parameter like number of black hole nodes, Speed of the nodes and mobility of the nodes.

4.1.1 Packet Delivery Ratio of VSSAOMDV

Figure 4.1 shows the results of packet delivery ratio for varying the number of black hole nodes from 20 to 100. From the results, it is observed that the VSSAOMDV scheme has higher

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

delivery ratio of range from 99.95 to 95.9. It has got the highest packet delivery ratio due to its reliability. NEPSSS scheme has got the range between 98.9 to 94.6 percentages in packet delivery. MAOMDV has the packet delivery ratio in the range of 97.8 to 93.2. and SAOMDV has the packet delivery ratio in the range of 96.9 to 91.1%. VSSSAOMDV has highest packet delivery ratio because of the reliable data delivery by using the secret sharing scheme.



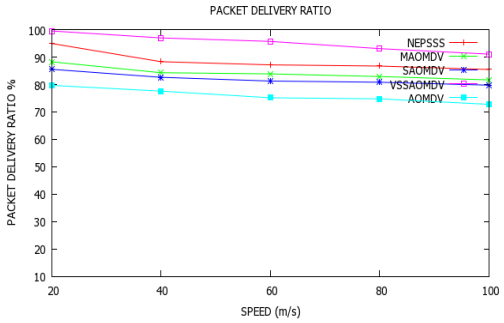


Figure 4.1: Packet Delivery Ratio Vs No of Black Hole Nodes Figure 4.2: Packet Delivery Ratio Vs Speed

Figure 4.2 shows the results of packet delivery ratio for varying the speed of the nodes from 20m/s to 100m/s. VSSAOMDV scheme has higher delivery ratio in the range from 99.624 to 91.151%. It has got the highest packet delivery ratio at speed variation due to the fact of share back tracking and redistributing share in the alternate route. NEPSSS scheme has got the range between 95.053 to 85.5302 percentages in packet delivery. MAOMDV has the packet delivery ratio in the range of 88.363to 81.74%. SAOMDV has the packet delivery ratio in the range of 85.603 to 79.809%.

4.1.2. Misbehavior Detection Efficiency of VSSAOMDV

Figure 4.3 illustrates the node misbehavior detection efficiency ratio by varying the speed and mobility of the nodes. At the speed of 20m/s VSSAOMDV has achieved high detection efficiency ratio of 95.9 %. The detection efficiency ratio is 58.44% at 100 m/s. At the same range of speed NEPSSS achieves the detection efficiency ratio of 91.3 to 38.5%. MAOMDV has the detection efficiency ratio in the range of 80.3 to 29.2%. SAOMDV has the low detection efficiency ratio in the range of 70.3 to 15.66%. SDSR has the least detection efficiency ratio with the range of 53.3 to 11.5%. It is clearly depicted that VSSAOMDV has achieved the high detection efficiency ratio because of enhanced black detection process at route discovery and data transmission process. The black hole nodes are detected even during the share verification process.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

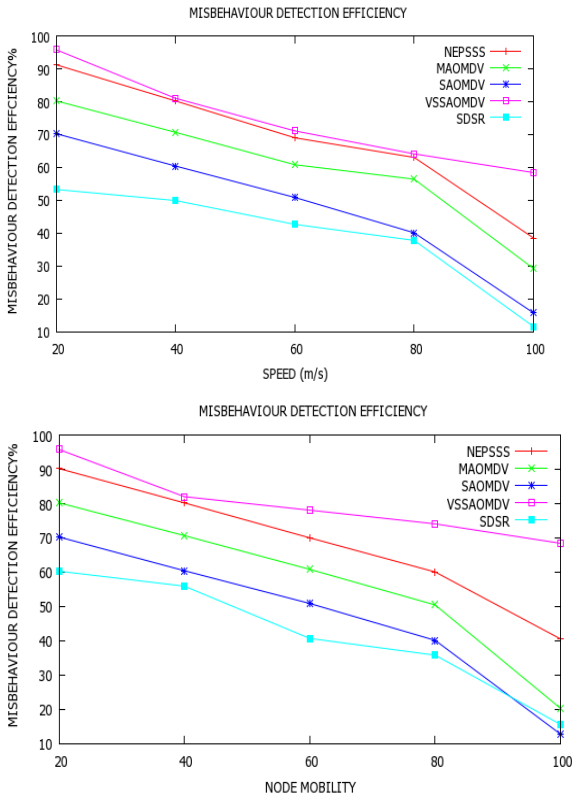
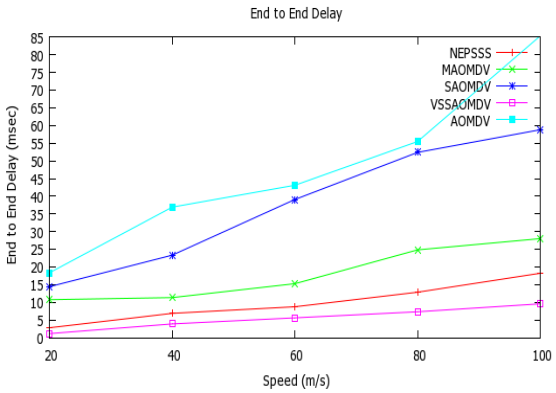


Figure 4.3: VSSAOMDV: Misbehavior Detection Efficiency Vs Speed and Node Mobility

4.1.3. End to End Delay Time of VSSAOMDV

The end-to-end delay time of VSSAOMDV is analyzed by varying the number of black hole nodes, speed of the nodes and mobility of the nodes. The Performance of VSSAOMDV is compared with other schemes like NEPSSS, MAOMDV, SAOMDV and AOMDV. The delay time increases when the participation of black hole nodes increases. Figure 4.4 illustrates the delay time of VSSAOMDV by varying the number of black hole nodes. It shows VSSAOMDV has the delay time of 1.1337 msecs at the rate of 20 black hole nodes. The delay time increases to 9.564msecs when the black hole nodes increase to 100. NEPSS has the delay time of 1.8 to 14.2 msecs. MAOMDV has the delay time of 7.727 to 22.2 msecs. SAOMDV has the delay time in the range of 8.418 to 48.8 msecs for 20 to 100 black hole nodes. AOMDV has the high delay time of 13.350 to 79.564 msecs. It shows that VSSAOMDV has the least delay time by varying the black hole nodes from 20 to 100 nodes. The share redistribution scheme of VSSAOMDV has minimized the delay time of data packet to reach the destination.



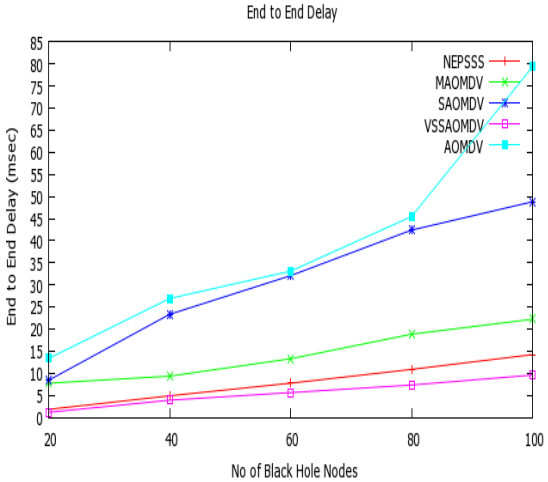


Figure 4.4: End to End Delay Time Vs No of Black hole nodeS Figure 4.5: End to End Delay Time Vs Speed.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

Figure 4.5 illustrates the end to end delay time of VSSAOMDV by varying the speed of the nodes. The result shows that VSSAOMDV has the delay time of 1.1337 msecs at 20m/s. At 100 m/s the VSSAOMDV has the delay time of 9.564 msecs. At the same range of speed , NEPSSS has the delay time in the range of 2.8 to 18.2 msecs. MAOMDV has the delay time in the range of 10.77 to 28.1 msecs. SAOMDV has the delay time in the range of 14.418 to 58.8msecs. AOMDV holds the highest delay time in the range of 18.350 to 85.3433 msecs. It is observed that VSSAOMDV has the least delay time on comparing to other schemes.

4.1.4. Routing Overhead of VSSAOMDV

Figure 4.6 illustrates the routing overhead of the VSSAOMDV scheme by varying the number of black hole nodes**.** It is clearly shown that the overhead of VSSAOMDV is the low overhead than the other schemes. VSSAOMDV has the lowest overhead in the range 0.00026 to 0.00119 packets. NEPSSS has got the overhead in the range of 0.00067 to 0.00292 packets. SAOMDV has the overhead in the range 0.0011 to 0.0041 (pkts). MAOMDV has the over head value in the range of 0.0095- 0.0033(pkts) and AOMDV seems to have higher over head with the range of 0.0033 to 0.0051(pkts). VSSAOMDV has the lowest overhead because the route discovery process is not initiated as soon as the route to the destination fails. Instead of that the alternate route is selected. The shares are not generated repeatly. The shares can be transferred from old group of share holders to new group of share holders. This scheme uses only certain needed information from the digital signatures. It is not necessary to store the digital certificates as in SAOMDV.

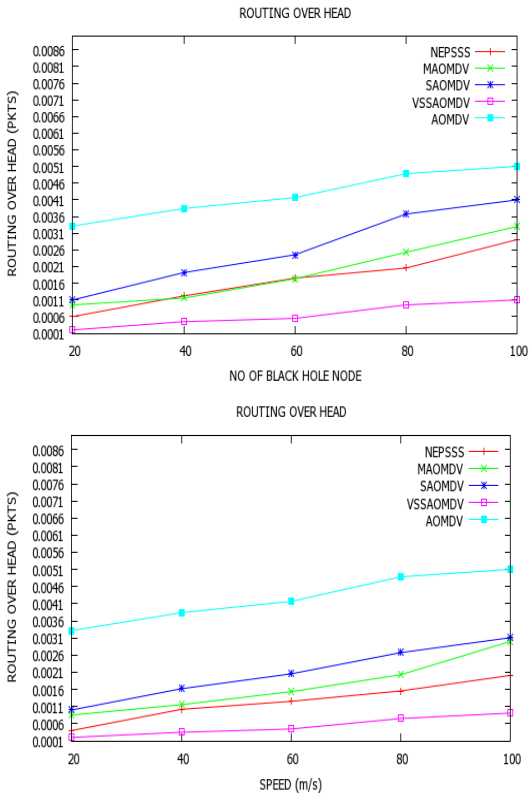


Figure 4.6: Routing Overhead Vs No of Black hole nodes Figure 4.7: Routing Overhead Vs Speed

Figure 4.7 illustrates the routing overhead of VSSAOMDV by varying the speed of the nodes. VSSAOMDV has the overhead of 0.0002 at 20 m/s and 0.00091(pkts) at 100 m/s. NEPSSS has the overhead in the range of 0.0004-0.00201 (pkts). MAOMDV has the overhead in the range of 0.0008509-0.0030 (pkts). The overhead range of

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

SAOMDV is 0.0010-0.00311(pkts). AOMDV has the overhead of 0.00331-0.0051(pkts). It is observed that VSSAOMDV has the least overhead than NEPSSS, AOMDV, SAOMDV and AOMDV.

4.1.5. Network Life Time.

The network life time of the node is analyzed by varying the speed and mobility of the nodes. The network life time decreases as the traffic load increases.

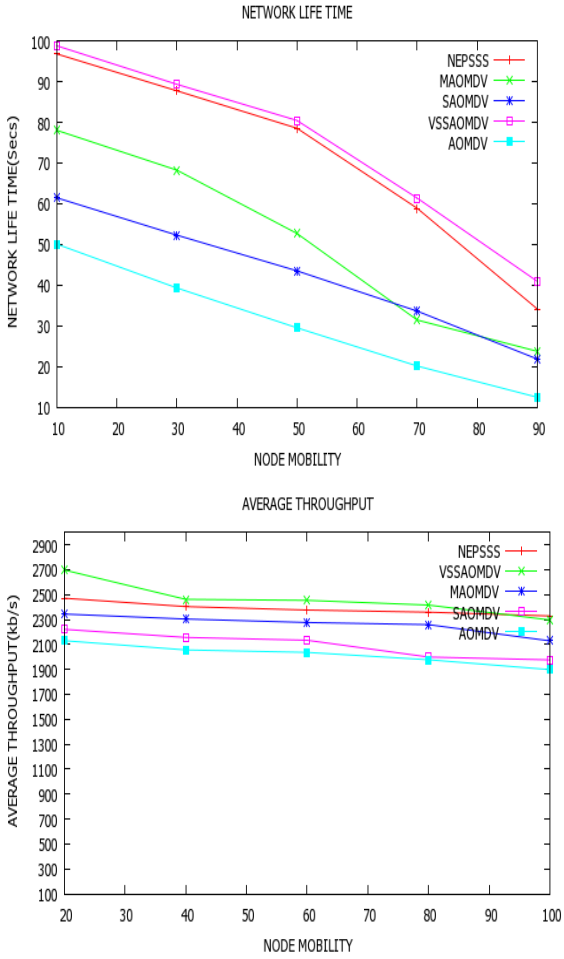


Figure 4.8: Network Life Time Vs Node Mobility Figure 4.9: Average Throughput Vs Node Mobility

Figure 4.8 illustrates the evaluation of the network life time metric of the VSSAOMDV by varying the mobility of the nodes. It is observed that VSSAOMDV has the life time in the range of 98.9 to 40.90secs. NEPSSS has the life time in the range 96.9 to 34. 1secs.The life time of SAOMDV is in the range of 61.5 to 21.8 secs. MAOMDV has the network life time of 78.1 to 23.8 secs. AOMDV has the least range of lifetime value of 12.4 to 50.18 secs. The high mobility of the nodes at the high speed makes the network topology highly dynamic. This dynamic nature of the network makes the protocol to spend considerable amount of energy in route discovery specifically at the high traffic load. The excessive energy consumption leads to premature failure of the nodes. The simulation result shows that VSSAOMDV has the high network life time than the other schemes due to the fact that VSSAOMDV has adapted share redistribution strategy. The share redistribution minimizes the energy consumed for regenerating the shares when the current route fails. The alternate path selection also minimizes the new route discovery process thereby reducing amount of energy spend on new route discovery process. Hence the network life time of the nodes are increased by minimizing the energy consumption of the nodes.

4.1.6. Average Throughput of VSSAOMDV.

The Average throughput of the proposed protocol scheme is evaluated by varying the mobility of the nodes. Figure 4.9 illustrates the average throughput of

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

VSSAOMDV by varying the mobility of the nodes from 20m/s to 100 m/s. It is observed that VSSAOMDV outperforms with the higher throughout at the low mobility of the nodes than NEPSSS, SAOMDV, MAOMDV and AOMDV. When the mobility of the nodes increases the throughput decreases. The selection of alternate path without the black hole node maximizes the throughput of the proposed protocol scheme. The simulation result shows that the proposed protocol scheme using the verifiable secret sharing scheme improve the efficiency in black hole node detection with minimum end to end delay time and routing overhead.

5. CONCLUSION

Mobile Ad hoc Networks consist of mobile nodes without any fixed infrastructure. The dynamic nature of the nodes makes the security of data transmission as the critical issue. The nodes 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 highly secured data transmission scheme using the verifiable secret sharing scheme to detect the black hole nodes and to provide reliable data transmission form the source to the destination. The method is implemented in AOMDV protocol to reduce the routing over head. This share redistribution scheme reduces the load of the dealer on share generation. It is not necessary for the dealer to generate the shares repeatedly. The time delay in packet delivery in terms of availability of black hole nodes is reduced. This method ensures the reliability of the messages by using a secure distribution scheme which does not allow the black hole node to learn any information about the shares. This scheme also ensures the availability of the information by delivering the shares to the destination through the alternate route in minimum time.

REFERENCES

[1] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key en-cryption scheme. In Eli Biham, editor, Advances in Cryptology—EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science,pages 255–271. Springer-Verlag, 4 – 8 May 2003.

[2] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems. In Proc. 9th(ACM) conference on Computer and Communications Security, pages88–97. (ACM) Press, 2002.

[3] Desmedt and S. Jajodia. Redistributing secret shares to new accessstructures and its applications. Technical Report ISSE TR-97-01, GeorgeMason University, July 1997.

[4] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In Proceedings of the Nineteenth Annual ACM Symposium on Theoryof Computing, pages 427–437, New York City, 25–27 May 1987.

[5] Stanislaw Jarecki. Proactive secret sharing and public key cryptosystems.Master's thesis, Massachusetts Institute of Technology, Cambridge, MA,September 1995.

[6] A. Shamir. How to share a secret. Communications of the (ACM),22:612–613, 1979

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

[7] Adi Shamir. Identity-based cryptosystems and signature schemes. InG. R. Blakley and David Chaum, editors, Advances in Cryptology: Pro-ceedings of CRYPTO 84, volume 196 of Lecture Notes in Computer Sci-ence, pages 47–53. Springer-Verlag, 1985, 19–22 August 1984

[8] T. M. Wong, C. Wang, and J. Wing. Verifiable secret redistribution forarchive systems. In Proceedings of the 1st International IEEE Securityin Storage Workshop, 2002.

[9] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya. ID-based encryptionfor complex hierarchies with applications to forward security and broad-cast encryption. In ACM Conference on Computer and CommunicationSecurity, pages 354–363, 2004.

[10] Lidong Zhou, Fred Schneider, and Robbert van Renesse. APSS: Proactivesecret sharing in asynchronous systems. ACM Transactions on Information and System Security, 8(3):259–286, aug 2005

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

[12] 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.

[13] 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.

[14] 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.

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

[16] 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

[17] 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.

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

[19] 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.

[20] 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.

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

[22] K. Selvavinayaki, Dr.E. Karthikeyan, “A Reliable Data Transmission Approach to Prevent Black Hole Attack in MANET”, *International Journal of Computer Science*

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

and Telecommunications, vol. 3, issue 3, March 2012
[23] K. Selvavinayaki, Dr.E. Karthikeyan "A Secured Data Transmission Method Using Enhanced Proactive Secret Sharing Scheme to Prevent Black Hole Attacks in MANETs" Journal of Theoretical and Applied Information Technology ,30th September 2014. Vol. 67 No.3

SSN (Print): 2204-0595
ISSN (Online): 2203-1731