A Secured Data Transmission Method using Enhanced Proactive Secret Sharing Scheme to Prevent Blackhole Attack in MANETs - A Review

Jasmeen Kaur
M.Tech Scholar
Department of Computer Science and Engineering
Amritsar College of Engineering and Technology
(Manawala) Amritsar

Tanupreet Singh, PhD
Professor and Head of Department
Department of Electronics and Communication Engineering
Amritsar College of Engineering and Technology
(Manawala) Amritsar

ABSTRACT
Mobile Ad Hoc Networks are the collection of Self-organizing, Independent nodes that can interact with one another by creating radio network. In multi-hop wireless ad hoc networks, the nodes not in direct range rely/dependent upon intermediate nodes to interact. For securing its limited resources or to organize Denial of Service (DoS) attack, the middle node for instance the intermediary node drops all the packets going through it instead to forward them to its Descendant. This review paper can deal with the misbehavior called Blackhole Attack which is one of the Security Attacks and occurs in the Network Layer. Nodes interact with each other without any access point. It is a Dynamic network having the capabilities of real time network. Due to mobility of nodes network is easily affected by many types of attacks. In particular Blackhole attack the it can cause packet dropping and misrouting the information from source to destination. To reduce the impact of this attack, the new approach has been proposed i.e. New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to detect the Blackhole nodes and to verify the Data Authenticity, Data Confidentiality and Data Integrity. This proposed algorithm divided into two phases. The first phase is the Detection of Blackhole Attack achieved using Trust Active and Recommendation of the Nodes. In the second phase the New Proactive Secret Sharing Scheme is used to provide the data authenticity and data integrity. The simulation results shows that the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packet overhead and low end to end delay than the existing schemes.

Keywords:
MANET, Blackhole Attack, AOMDV, Proactive Secret Sharing Scheme, Public Key, Private Key.

1. INTRODUCTION
MANETs- Mobile Ad hoc networks are the 'self organizing and Dynamic network having the capabilities of real time network'.

It is a collection of wireless mobile connections or nodes that can communicate with each other without the centralized controller authority. Due to the characteristics of MANETs for instance wireless connection and dynamic network and distributed network Mobile Ad Hoc Network is exposed to many security attacks like Wormhole attack, Black hole attack, Gray hole attack, Flooding attack, jellyfish attack, Sybil attack etc.

Though, wireless networks are fully distributed and have the ability to work without the aid of any permanent infrastructure or access points. The mobile ad hoc network has some special features such as open and undependable wireless connection, dynamic network topology and limited bandwidth, battery lifetime and computation power of nodes. These features make the network adaptable or manageable [8].

In mobile ad hoc networks the cooperation between the nodes is necessary to transfer/ deliver packets to the destination node. The intermediary node that helps to send or receive packets can behave selfishly or mischievously to drop packets which are forwarding through it to its descendant. The packet dropper's main motive is to secure its resources like its less energy i.e. Selfish Behavior, or the launch of Denial of Service attack i.e. malicious behavior. This malicious behavior is known as Blackhole attack that can be launched by one single intermediate node known as single Blackhole attack and it can also be launched by the cooperation of several intermediary nodes known as cooperative Blackhole Attack.

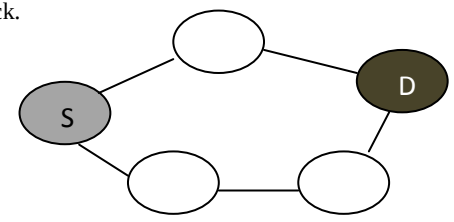


Fig-1 Mobile Ad Hoc Network

Source Node

Intermediate node

Destination Node

1.1 Characteristics of Mobile Ad hoc Networks:

The various characteristics are [19] :

1. Fully Distributed.
2. Wireless connection.
3. Dynamic network i.e. The nodes can join or leave the network anytime.
4. Flexible.
5. Heterogeneous Nodes.
6. No centralized controller Authority.
7. It must be vary with regular topology changes due to mobility of nodes.
8. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.

1.2 Security Issues in Ad hoc Network:

The various security issues in MANETs are [17].

- Lack of secure boundaries.
- Risks from compromised nodes inside the network.
- Lack of centralized management facility.
- Restricted Power Supply.
- Scalability.

1.3 Security Solutions to Ad hoc Network

The various security goals to evaluate if mobile ad hoc network is secure or not are as follows [18].

- Availability: Availability means the resources gain access to authorized parties at assumed times. Availability applies to both data and to services also. It makes sure that the durability of network service in spite of Denial of Service attack.

- Confidentiality: This makes sure that computer related resources are gain access only by authorized parties. Securing of information which is swapping through a MANET. It should be secured in opposition to any disclosure attack like Eavesdropping- unauthorized access to messages.

- Integrity: It means that the resources can be adjusted only be authorized parties or only in authorized way. Integrity makes sure that a message being transmitted is never corrupted.

- Authentication: Authentication is basically to sure that members in communication are authenticated and not impersonators. The assets of network should be gain access by the authenticated nodes.

- Authorization: It goal assigns different access rights to different types of users.

- Resilience to attacks: It needs to support network functionalities when a part of nodes is compromised or terminated.

- Freshness: It makes sure that the intruder node does not resend the foregoing captured packets.

1.4 Attack:

In Ad Hoc Network an attack is any try to damage, expose, alter, disable, sneak or gain unauthorized access to make unauthorized use of a resource [20].

Two types of attacks in MANET:

1) Passive attacks
2) Active attack

Passive Attacks: In Passive attack, the intruder listen to network in order to get data, what is going on in the network channel? It listens to the network in Order to know and understand how the nodes are interacting with each other, how they are placed in the network. Before the intruder launch an attack against the network, the intruder has enough data about the network that it can easily steal and introduce attack in the network. [15,16]

Active Attacks: In active attack the intruder unsettle the performance of the network, sneak significant information and attempt to harm the data during the exchange in the network [15,16].

Active attacks can be of two types. It can be internal or an external attack.

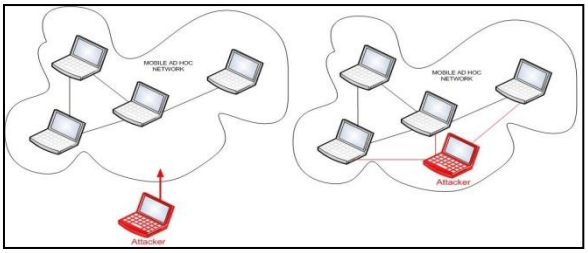


Fig-2 External and Internal attack in Mobile Ad Hoc Network [15]

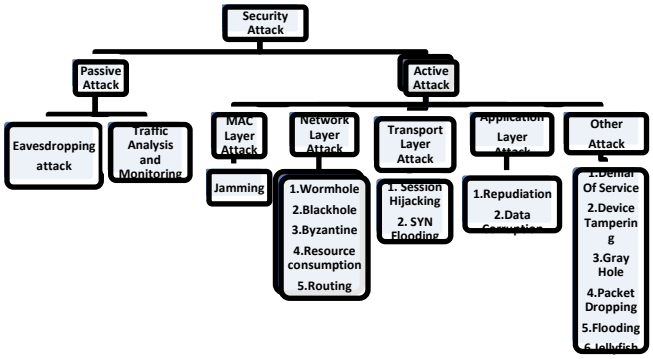


Fig-3 Various Types of Security Attacks in Ad hoc Networks

1.5 Various Detective and Preventive Security Measure tools such as:

Cryptographic Tools: Digital signature, Public Key Encryption.

Non-Cryptographic Tools: Intrusion Detection System.

These tools can enhance the security of the network. However, these techniques can take into account only the

subset of the threats, and the problem remains always open and the remedy is far from being obvious[8].

1.6 Objectives

The Proposed approach New Enhanced Proactive Secret Sharing Scheme checks the correct forwarding of the packets by the intermediary nodes. [14]

The main objective of this proposed approach is to:

1. Detection of Blackhole attack.
2. Secure Transmission of Data using New Enhanced Proactive Secret Sharing Scheme (NEPSSS).

2. LITERATURE REVIEW

So much work has been done by the researchers on detecting and Preventing the Blackhole attack with the help of various techniques such as cryptographic tools i.e. Digital Signature, Public Key Encryption and also the Non-Cryptography tools such as Intrusion Detection System has been used by the Researchers for enhancing the Security of the Network**.**

Mr. Golok Panda, Mr. Gouri Shankar Mishra & Mr. Ashok Kumar Sahoo et al. [1] proposed a approach which leads to prevent the inducer that carry black hole node in very fast. Nobody will listen to malicious node's Hello message packet. The various authors have given various proposals for detection and prevention of black hole attack in MANET but every proposal has some limitations and their respected solutions. It is clear that malicious node is the main security threat that affects the performance of the AODV routing protocol. Every parameter has shown tremendous improvement except avg. jitter and avg. end-to-end delay due to the overhead of key mechanism. It will be extended such that the value of these parameters can be enhanced.

Neelam Khemariya & Ajay Khuntetha et al. [2] proposed an efficient approach for the detection and removal of the Black hole attack in the Mobile Ad Hoc Networks (MANET) is described. The algorithm is implemented on AODV (Ad hoc on demand Distance Vector) Routing protocol. The algorithm can detects both the single Black hole attack and the Cooperative Black hole attack. The beauty of the algorithm described in this paper is that it not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

Firoz Ahmed, Seok Hoon Yoon and Hoon Oh et al.[3] proposed EVM method which can pin down multiple black hole nodes effectively by employing an encryption mechanism. The verification process is initiated conditionally and it verifies the sequence number that was not faked by any malicious node. It shows the simulation that the EVM not only reduces the control overhead but also effectively identifies the malicious node. In the future, it can extend this algorithm to solve a selective forwarding attack such as gray hole attack.

Nirali Modi & Vinit Kumar Gupta et al. [4] proposed algorithm that used the trust value which is used to identify the malicious node, after identifying the malicious node it will be removed from the neighboring table and we select the another path. This proposed algorithm can offer a secure way transmission between any nodes in network topology. Researcher propose modification to the AODV protocol and justify the solution with implementation and simulation using NS-2.33. This simulation analysis shows the significant improvement in end-to-end delay, throughput, and packet delivery ratio of AODV in presence of Black hole attack.

Nabarun Chatterjeea, Jyotsna Kumar Mandalb et al. [5] proposed a technique to avoid Blackhole attack in AODV routing protocol using Triangular Encryption Method in NS2 Simulator. Triangular Encryption has been chosen because of its low computation overhead.It compares the Proposed technique with existing blackhole detection technique which reveals that the proposed technique obtains better results.The limitation of the proposed work was that it only Avoid the Blackhole behaviour but could not detect and eliminate Blackhole nodes.The implementaion becomes very slow as the number of nodes increases.The number of packet sent is much more than the original AODV protocol and thus it increases network load.

Amol Bhosle, Yogadhar Pandey et al.[6] proposed a method to provide the data security of such network using node authentication and digital signature. In this paper some previous methods for identifying malicious node are discussed, there was no such method to authenticate the new node before it joins the network. This new protocol design provides the integrity, confidentiality, non repudiation and authentication with the help of AES, and digital signature. The node authentication achieved by the IP address of the nodes. Digital signature formed with the help of RSA and hash function MD-5. This security mechanism called SMDNA (Securing MANET Data using Node Authentication) improves the performance of the routing protocol AODV.

Rashmi, Ameeta Seehra et al.[7] present a clustering approach in Ad-hoc On-demand Distance Vector (AODV) routing protocol for the detection and prevention of black-hole attack in MANETs. In this approach every member of the cluster will ping once to the cluster head, to detect the peculiar difference between the number of data packets received and forwarded by the node. If anomalousness is perceived, all the nodes will obscure the malicious nodes from the network. The simulation results show that clustering approach is responsible for full delivery of packets even in presence of multiple black-hole nodes. Also the detection rate and throughput are improved by four times and 1.5 times.

Abderrahmane Baadache, Ali Belmehdi et al.[8] deals with this misbehavior called black hole attack, and proposed an authenticated end-to-end acknowledgment based approach in order to check the correct forwarding of packets by intermediate nodes. This proposed approach detects the black hole conducted in simple or cooperative manner and also detects the modification and the replay of messages attacks. Through simulation using OPNET simulator, it shows the detection efficiency and evaluate the performance of the proposed approach in both proactive and reactive routing based networks in terms of end-to-end delay and network load. Also, it compare the approach with existing approaches that is with 2-hop ACK and the watchdog approaches in terms of detection ratio, delivery ratio and additional overhead.

T. Prasanna Venkatesan, P. Rajakumar, A. Pitchaikkannu et al.[9] In this paper, it is briefly explained on existing intrusion detection techniques in the context of MANETs. Since Intrusion prevention alone is not sufficient to achieve security in a network, it is presented a way to manage MANET security, by enhancing the existing secure protocols adding the component of Malicious nodes, not only in determining the route for sending packets, but also avoiding attempts of Denial of Service from Malicious Nodes. The accuracy of IDS can suffer from the high false positive or low false negative rates. If the majority of the mobile nodes are compromised then the intrusion detection becomes fail. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, which may be addressed in future.

Payal N. Raj and Prashant B. Swadas et al. [10] proposed an approach DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of blackhole by notifying other nodes in the network of the incident. The simulation results in ns2 (ver-2.33) prroves that our protocol not only prevents Blackhole attack but on the other hand improves the overall performance of (normal) AODV in presence of black hole attack.

Djamel Djenouri1, Nadjib Badache2 et al.[11] propose a novel monitoring approach that overcomes some watchdog's shortcomings, and improves the efficiency in detection. To overcome false detections due to nodes mobility and channel conditions we propose a Bayesian technique for the judgment, allowing node redemption before judgment. Finally, we suggest a social-based approach for the detection approval and isolation of guilty nodes. We analyze our solution and asses its performance by simulation. The results illustrate a large improvement of our monitoring solution in detection vs. the watchdog, and an efficiency through our judgment and isolation techniques as well.

Djamel Djenouri *, Nadjib Badache et al.[12] this paper deals with the misbehavior nodes in mobile ad hoc networks (MANETs) that drop packets supposed to be relayed, whose objective may be either saving their resources or launching a DoS attack. It proposed a new solution to monitor, detect, and safely isolate such misbehaving nodes, structured around five modules: (i) The monitor, responsible for controlling the forwarding of packets, (ii) the detector, which is in charge of detecting the misbehaving of monitored nodes, (iii) the isolator, basically responsible for isolating misbehaving nodes detected by the detector, (iv) the investigator, which investigates accusations before testifying when the node has not enough experience with the accused, and (v) finally the witness module that responds to witness requests of the isolator. These modules are based on new approaches, aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead.

Satyendra Tiwari, Anurag Jain and Gajendra Singh Chowhan et al. [13] proposed a modified ack-based scheme for decision ambiguity for requested node on the basis of finite state machine. Finite state machine is a automata of theory of computation here we used deterministic finite automate for the decision making of node and improved node authentication and minimize packet dropping in adhoc network.

K.SELVAVINAYAKI ,DR. E. KARTHIKEYAN et al.[14] To reduce the effect of blackhole attack,a New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to detect the black hole nodes and to ensure the data confidentiality, data integrity andauthenticity has been proposed. 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.

3. BLACKHOLE ATTACK

3.1 Single Blackhole Attack

Black hole attack is the one of the security attacks that is occur in the network layer. In this attack one mischievous node conduct the Blackhole attack. In this attack mischievous node uses the routing protocol to promote or to shows itself as having the shortest path to the destination node to which node it wants to interrupt. When the information is actually start transmitting it grasps all the packets that were originally meant for the destination node and then the mischievous node drops the transmitted packets without forwarding them.[8,14]

3.1.1 Blackhole Attack in AODV

The AODV is the Ad hoc On Demand Distance vector routing protocol is a Reactive Routing Protocol which is used to find the path between source nodes to destination node when desired. It uses Request Message such as Route Request (RREQ) and Route Reply (RREP) for establishing a path from source to the destination.

In AODV the source node broadcast a route request message having information as: Destination Address, Destination Sequence number and Hop Count. Neighbors of the source node update their routing tables accordingly and broadcast RREQ. This Process Continues until RREQ reaches the exact Destination node. Once the RREQ reaches to the destination node it again re-organizes the reverse route to send back the Route Reply (RREP) message to the source node. It must be noted that the Source node can receive several RREPs from different nodes. However, it selects the one with highest sequence number from the intended destination. If RREPs containing greatest sequence number for the same destination are reported by more than one node, then the path with lowest hop count will be selected [21].

In AODV based Blackhole attack when the malicious node receives the RREQ, it takes note of the destination address, and prepares a RREP, in which the destination address is set to the spoofed destination address, the sequence number is set to a highest value and the hop count set to a lowest value. The Blackhole node sends RREP to the nearest intermediate node belonging to the actual active route. RREP received by the intermediate node will be relayed through the Reverse path towards the source node. The source node updates its routing table according to the received RREP and uses the new route

to send data. When intercepted, data will be dropped and the node act as Blackhole node.

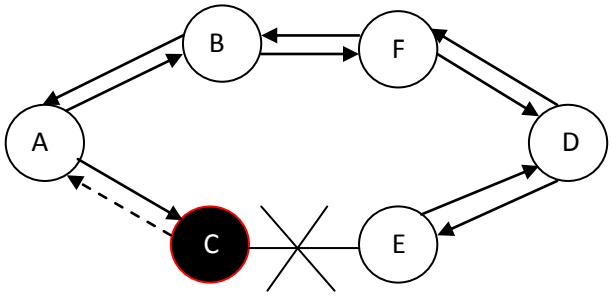


Fig-4 Single Blackhole Attack Problem

The Fig-4 shows how black hole problem occur, here node "A" wish to send data packets to node "D" and initialized the path discovery process. So if node "C" is a mischievous node then it will request that it has effective route to the desired destination as soon as it receives RREQ packets. It will then send the reply to node "A" before any other node. In this way node "A" will believe that this is the effective route and thus effective route discovery is complete. Node "A" will not pay attention to all other replies and will start sending data packets to node "C". In this way all the data packet will be destroy or absorbed by mischievous node [15].

4. PROPOSED APPROACH

New Enhanced Proactive Secret Sharing Scheme (NEPSSS) 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. NEPSSS 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 [14].

As per the NEPSSS scheme RREQ packet and RREP packets are modified to hold additional information which is discussed Below [14].

4.1.Detection of Black hole attack

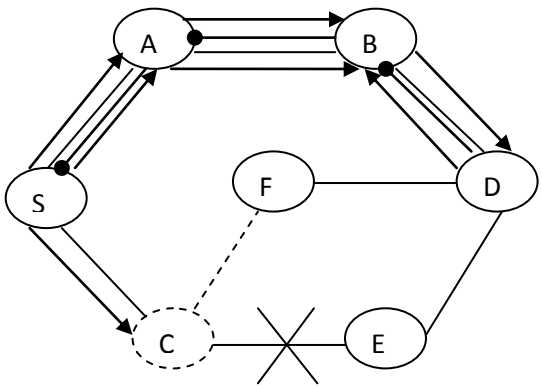
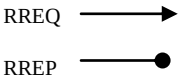


Fig-5 Blackhole Attack [14]



As in Figure 5, Suppose Source S wants to disseminate with Destination node D. Here A and B are the intermediate nodes. Source broadcasts the Route 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 t_1.But after a sometime, node B may transit or move to another zone which is out of radio range of node A ,due to the mobility of nodes in MANET. At time t_2, node B happens to be back in node A's radio range again. The trust value should declined/decayed during this time gap.

Let ${}_AT_B(t_1)$ be the trust value of node A to node B at time t_1 and ${}_AT_B(t_2)$ be the decayed value of the same at time t_2. Then trust active is defined as follows,

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

Node A receives RREQ. It search for 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[PvA[Aid], PbD[Sid], Did ,${}^MR_N$ } where Pv A is the private key of A. Where Node proposal ${}^MR_N$ is also used to identify the malicious behaviour.

Evaluating the recommendation is given by ${}^MR_N$ which is node M's evaluation to node N by collecting recommendations.

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

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 6, 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

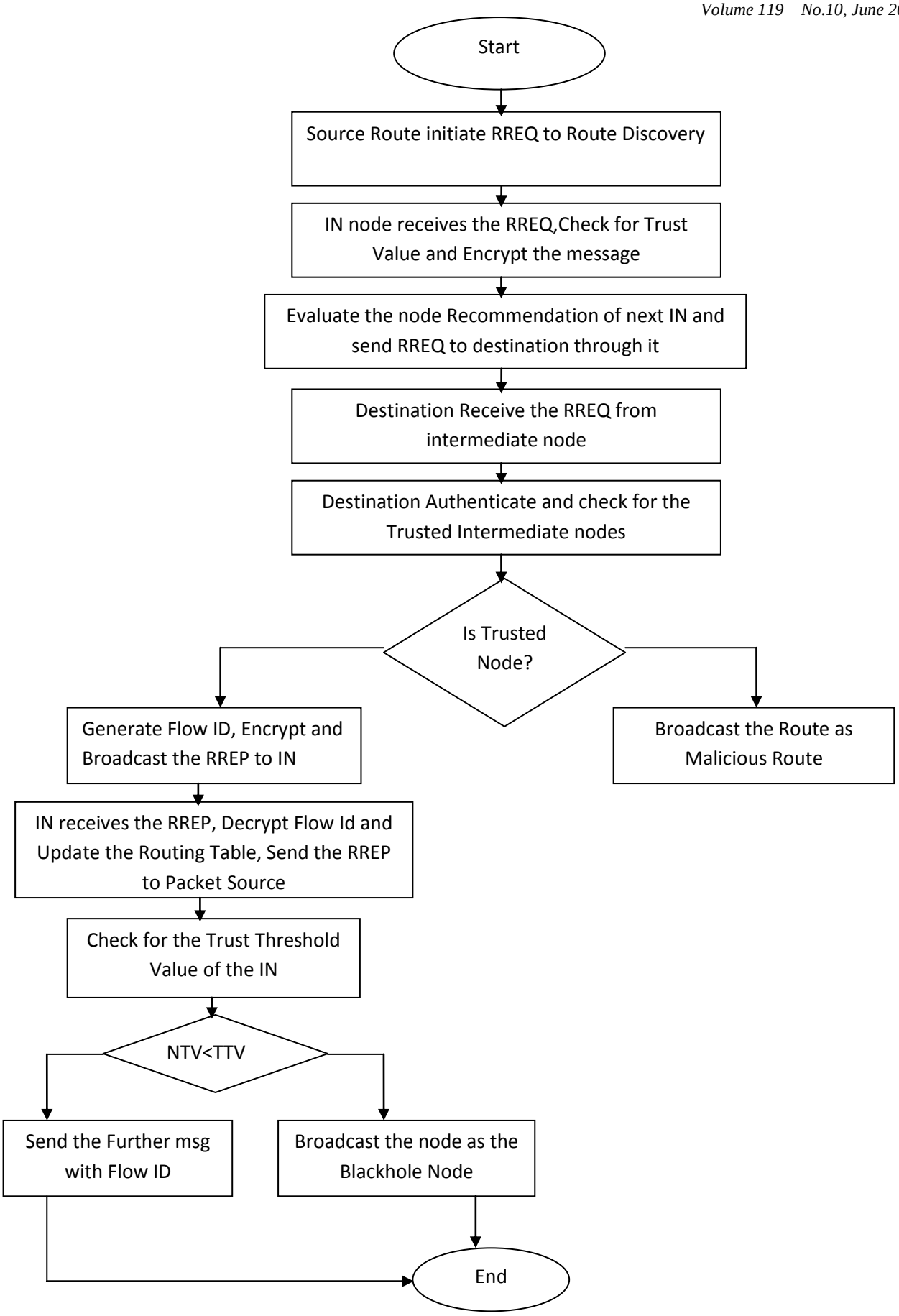


Fig -6 Blackhole Detection Process [14]

its routing 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[14].

4.2 Enhanced Proactive Secret Sharing Scheme 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 period to comprise the secret. The sub shares from secret can be created and old shares are unreasonable [14].

This feature unable the compromisers to expose the secret. To assure the authenticity of the information transferred The New Enhanced proactive secret sharing scheme has been Proposed [14].

Various stages of Enhanced proactive secret sharing scheme are as Follows:

A. Secret share generation.

B. Initiation of the Sharing process.

C. Verify and authenticate the digital signature.

4.2.1. 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_{1,2,3,….n}) which randomly generates Sk's sub shares like (Si1, Si2, ….. Sin) for (t.n) sharing. All subshares Skp (p_{1,2,3,….n}) is distributed to node p through the secure or protected link. When node j gets the sub shares {S1k, S2k, ….. Snk}. It calculate a new share from these sub shares and its old share with an equation.

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

4.2.2 Initiation Of The Sharing Process

Source Node A transit 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.

4.2.3 Verify and Authenticate the Digital Signature

The digital signature gets 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:

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

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

The integer value is calculated as

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

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 $\tilde{u}1$.

Determine $y = \tilde{u}1 \bmod N$ (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 the Signature will be 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 recreated. If Sk holds shares (m1, n1) and Sp hold shares (m2, n2), then the share holder node recreate 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.

5. PERFORMANCE ANALYSIS

In this work Network Simulator (NS2.34) tool is used to simulate the 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[14]. The simulation settings and parameters are summarized in Table- 1.

Table-1 Simulation Setting and Parameters [14]

No. Of Nodes	100
Area Size	1200 x1200
MAC	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Packet Rate	5 pkt/sec
Protocol	AOMDV

5.1 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 (PDR): The ratio of the data packets delivered to the destinations to those generated by the CBR i.e. constant bit rate sources. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher the PDR better the result. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness. To improve the performance of the network system the PDR must be high as feasible [22].

$$PDR = \frac{Total\ number\ of\ packets\ received}{Total\ number\ of\ packets\ sends}$$

Throughput: It is the average rate of Successful transmitted data packets in bytes per second within runtime. It is denoted by Tp.

$$Tp = \frac{No.\ of\ bytes\ received * 8}{Simulation\ time * 1000}\ kbps$$

6. CONCLUSION AND FUTURE WORK

Mobile Ad hoc Networks consist of mobile nodes without any centralized Controller Authority. Here the node may be affected by several kind of attacks. It may cause the packet dropping, delaying, modifying and misrouting the information to another destination. In the proposed work, it has been focused on detection of the black hole attacks. This attack deteriorate the performance of the mobile ad hoc networks. So that, a new approach has been proposed i.e. 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 future work, the energy consumption model can also be 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. Further, I am going to precede my research as Trust Based Detection and Elimination of Blackhole Attack in MANETs for my Dissertation work.

7. ACKNOWLEDGMENT

This review work carried out is the part of my dissertation M.Tech (CSE) 4th semester of my course whereby I have been accompanied and supported by many people. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

Firstly, I would like to thank God. The Almighty, for having made everything possible by giving me strength and courage to do this work.

I express my sincere gratitude to my guide Dr. Tanupreet Singh, Head of Department of Electronics and Communication Engineering, ACET Amritsar for his stimulating Guidance and Continuous encouragement right from the beginning of the work. I am extremely thankful to him for devoting his valuable time and imparting knowledge to me.

Lastly, I am thankful to my parents and friends for their moral support in every sphere. Their vital push infused sense of insurgency in me, I am thankful to them for their assistance and cooperation.

8. REFERENCES

[1] Mr. Golok Panda, Mr. Gouri Shankar Mishra & Mr. Ashok Kumar Sahoo, "Prevention of Black hole Attack in AODV protocols for Mobile Ad Hoc Network by Key Authentication." IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.3, June 2012

[2] Neelam Khemariya & Ajay Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs" International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[3] Firoz Ahmed, Seok Hoon Yoon and Hoon Oh, "An Efficient Black Hole Detection Method using an Encrypted Verification Message in Mobile Ad Hoc Networks" International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[4] Nirali Modi & Vinit Kumar Gupta, "Prevention Of Black hole Attack using AODV Routing Protocol in MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3254 – 3258.

[5] Nabarun Chatterjee, Jyotsna Kumar Mandal, "Detection of Blackhole Behaviour using Triangular Encryption in NS2" 1*st* International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA- 2013) Procedia Technology 10 (2013) 524 – 529, Available online at Sciencedirect.com.

[6] Amol Bhosle, Yogadhar Pandey, "Review of authentication and digital signature methods in Mobile ad hoc network" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

[7] Rashmi, Ameeta Seehra, "A Novel Approach for Preventing Black-Hole Attack in MANETs"" International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014.

[8] Abderrahmane Baadache ⇑, Ali Belmehdi, "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks", available online 20 August 2014 available at ScienceDirect.

[9] T. Prasanna Venkatesan, P. Rajakumar, A. Pitchaikkannu, "An Effective Intrusion Detection System for MANETs" International Journal of Computer Applications® (IJCA) (0975 – 8887) International Conference on Advances in Computer Engineering & Applications (ICACEA-2014) at IMSEC,GZB.

[10] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET" IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[11] Djamel Djenouri, Nadjib Badache, "Struggling Against Selfishness and Black Hole Attacks in MANETs", wireless communication Mobile computing. (WCMC) 8 (6) (2008)689-704.

[12] Djamel Djenouri , Nadjib Badache, "On eliminating packet droppers in MANET: A modular solution" Ad Hoc Networks 7 (2009) 1243–1258, Available online at www.sciencedirect.com.

[13] Satyendra Tiwari, Anurag Jain and Gajendra Singh Chowhan, "Migrating Packet Dropping in Adhoc Network Based on Modified ACKbased Scheme Using FSA" International Journal on Emerging Technologies **2**(2): 102-105(2011).

[14] 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;

[15] IRSHAD ULLAH & SHOAIB UR REHMAN, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Electrical Engineering, and Thesis no: MEE 10:62 June, 2010

[16] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[17] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Network- A Survey", Department of Computer Science and Electrical Engineering , University of Maryland, Baltimore County Available: http://www.csee.umbc.edu/~wenjia1/699_report.pdf

[18] Aarti, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering,volume-3, Issue 5, May 2013, pp. 252-257.

[19] MANET (Mobile ad hoc network)- Characteristics and Features. http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/

[20] http://www.slideshare.net/sunitasahu101/attacks-in manet#btnNext Last Visited- 22, May, 2014

[21] C. Perkins, E.B. Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC: 3561 (Experimental), IETF, July, 2003.

[22] Vidyapathi, Sundar, Harshita, Komal, "Securing MANET From BlackHole And WormHole Attacks", International Journal of Engineering and Technology" Vol. 5, No 3, Jun-Jul, 2013.