Digital Signature Authentication Scheme (DSAS) to detect Blackhole attack in MANETs

[1]Gouri Upadhyay, [2]Aditya Kumar, [3]Aradhana Sahu

[1]M.Tech. Scholar, [2]Assistant Professor, [3]Assistant Professor
[1]Computer Science & IT Department,
[1]Shri Shanakara Charya Engineering College, Bhilai, Chhattisgarh, India.

Abstract: This Mobile ad hoc networks (MANETs) are composed of independent and self organized nodes without the need of any infrastructure. Mobile ad hoc networks consist of mobile devices that are freely moving inside and outside in the network. These devices can operate as a host, a router or both at the same time. These nodes have the ability to organize themselves because of their self configurable capability; they can be organized immediately without the help of any infrastructure. Due to various features like open medium, dynamic topology, lack of defensive mechanism, makes MANET more susceptible to security problems and attacks. Ad hoc On-Demand Distance vector routing protocol (AODV) is one of the best and most popular routing protocols in MANET. This routing protocol is frequently affected by well known black hole attack in which it injects a forged route reply message that considers as it has a fresh enough route to destination node. In this research work a "Digital Signature Authentication Scheme (DSAS) to detect black hole attack in MANETs" is proposed using AODV routing protocol to implement black hole attack in NS-2 and measure its impact on the performance of AODV routing protocol by using different performance metrics like Packet Delivery Ratio, Average End-to-End Delay, Average Throughput, Normalized Routing Load, and Routing Overhead. The proposed work is implemented in NS-2 using AES symmetric cryptographic technique and digital signature schemes to secure AODV routing protocol of MANET from black hole attack. The proposed method DSAS_AODV is compared with existing Secure_AODV method and simulative results shows that DSAS_AODV is better than Secure_AODV 7.2% in terms of Packet Delivery Ratio, 10.257% in terms of End-to-End Delay, 9.79 % in terms of Throughput, 6.396% in terms of Normalized Routing Load and 3.047% in terms of Routing Overhead.

Index Terms **- Wireless Networks, MANET, AODV, black hole, AODV, Digital Signature, Hash Function, AES.**

I. INTRODUCTION

Wireless communication networks have become a very popular and rapidly growing part of the telecommunications industry. Today this is part of every organization and individual life. It's an easy and fast implementation and the dependencies of the fixed infrastructure are not the main reasons. In general, a Mobile Ad-hoc network is a group of wireless nodes in motion; establish dynamic connectivity between them without a pre-existing network or centralized administration using IEEE 802.11 technology. More logically, the less wireless network infrastructure is a technological solution for establishing communications in areas where infrastructure is not available or not accessible. A simple Wireless Ad-hoc network is shown in Figure 1.

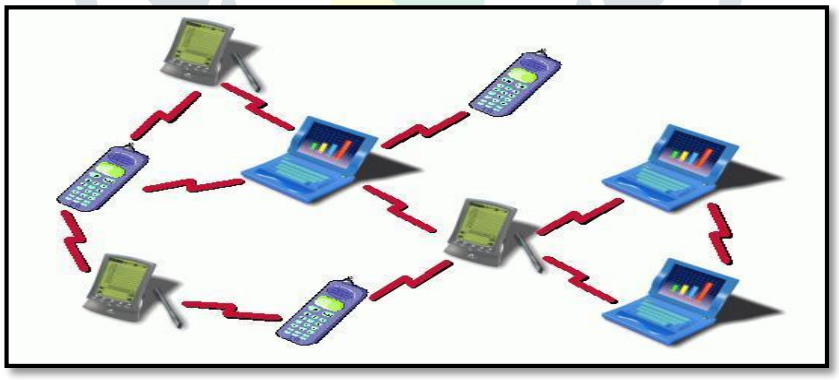

Figure 1: Wireless Ad Hoc Network [eexploria]

The involved nodes have the collaboration between them and can function as hosts and routers; they work together only in common agreement, without any knowledge of the network topology that surrounds them. Therefore, the network topology can be unpredictable and dynamic. Routing protocols, used in wired networks, cannot be used directly in the ad hoc mobile network. There are many reasons, such as bandwidth consumption, more than one route between two nodes, unidirectional connections between nodes and power supply are affected by the periodic updating of routing information and the slow convergence of routing protocol with respect to topology has changed dynamically. Therefore, efficient routing protocols are key components of successful communication in the mobile infrastructure minus the network.

A. Motivation

Wireless networking has gained a lot of attention in lot of years. The recent development in the field has led to focus learning on wireless networks. Integrity, confidentiality, and availability of data can be assured if all the security issues have been addressed. Thus, security in MANETs has been one of the major concerns for the normal functionality of the network. The lack of centralized monitoring system and easy to access open wireless channel make MANETs vulnerable to different types of attacks.

Blackhole attack, also known as packet drop attack has been one of the main threats to MANETs where the malicious node can attract and drop the packets in the network. When multiple attackers synchronize their efforts to harm the network, they cause intense damage to the network. Collaborative attacks are very complex, powerful and sophisticated. Thus dealing with these types of attacks is more challenging and interesting.

B. Research Problem

In recent years, wireless mobile ad hoc networks have gained a lot of importance in the field of wireless communications. Therefore, the need for securing these networks has been a huge challenge. This research paper mainly focuses on securing the MANETs against Blackhole attack. Much research has been done to secure the MANETs from Blackhole attacks, but only few of them have addressed the issue of Blackhole attacks effectively.

One of the simplest and possible solutions [4] to mitigate Blackhole attacks in MANETs is to disable intermediate nodes from replying to the RREQ packets, so, only the destination can reply to the RREQ packets. But, there are some disadvantages using this solution. First, the routing delay is greatly increased. Second, a malicious node can take further action such as fabricating a RREP packet on behalf of the destination node. The source node cannot determine if the reply message is really originated from the destination node or has been fabricated by the malicious node. When the data packet transmitted by the source node reaches the malicious node, it drops the packets instead of forwarding them to destination node creating a Blackhole. Such kind of attack may cause devastating impacts on a network and harm the network. Thus, in this thesis, a novel Digital Signature Authentication Scheme (DSAS) method is proposed to detect Blackhole attack while addressing the above mentioned concerns.

C. Black Hole Attack

Black hole attack is a type of denial of service where a black hole node can draw all packets sent by the source node by falsely maintaining a fresh route to the destination and then attract without forwarding them to the destination [5]. In an ad hoc network that uses the AODV routing protocol, a black hole node imagined to have new and enough routes to all destinations requested by all the nodes and attracts the network traffic. When a source node transmits the route request (RREQ) message for the destination, the black hole node instantly reacts with a route reply (RREP) message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a new and enough routes to the destination node. The source node assumes that the destination is at the back of the black hole node and then discards all the other RREP packets coming from other intermediate nodes. The source node then starts to send its data packets to the destination through the black hole node by trusting that these packets will deliver to the destination.

In figure 2, assume node B is a black hole node. When source node S broadcasts a RREQ packet to the entire neighbor node towards the destination node D, nodes A, B and C receive it. Node B, being a black hole node, this node immediately sends back a RREP packet with highest sequence number before any other node responds, even if any intermediate node sends RREP to the source node S without checking up its routing table for the requested route to the destination node D argue that it has fresh enough route to the destination. Node S receives the RREP from B further on the RREP from A and C. Hence, source node S updates its routing table for the new route to the particular destination node discards replies from node A and C even from an actual destination node D and assumes that the route through node B is the shortest and fresh path to reach the destination. Once a source node S saves a route, it starts to sends the data packets to the destination node D through this path. So, node B drops all the packets coming from source node S which produce black hole problem rather than forwarding them to the destination node D.

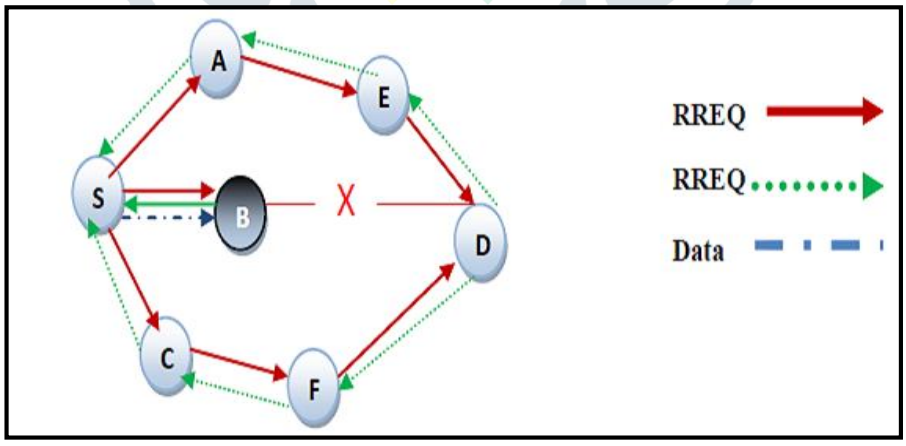

Figure 2: Illustration of Black Hole Attack

D. Research Objective

The aim of this research paper is to develop a secure routing protocol with a good performance based on AODV routing protocol. Secure is means the ability to protect the network from attacks. A novel Digital Signature Authentication Scheme (DSAS) method is proposed to secure the AODV routing protocol under Blackhole attack. Optimal performance is if the protocol has low end to end delay, high packet delivery rate, high throughput and low overhead. Main goals of this research work are:

1. Propose a novel Digital Signature Authentication Scheme (DSAS) method for AODV routing protocol to improve the security aspect.
2. To simulate the black hole attack using the AODV routing protocol.
3. Evaluate the proposed DSAS_AODV protocol with the Secure_AODV, Blackhole_AODV, Normal_AODV and Normal_DSR protocol in term of performance under Blackhole attack.

4. To analyze the performance of the network on factors like Packet Delivery Ratio, End-to-End Delay, Throughput, Normalized Routing Load and Routing Overhead.
5. Comparing the simulated results on various factors for the different scenarios.

II. LITERATURE SURVEY

In 2015, ***Nidhi Choudhary and Lokesh Tharani [1]***, demonstrated a timer-based sensing approach to identify the black hole node. In the network layer, they proposed a timer-based method to listen to the next action of the node. The results of the simulation with EXata-Cyber have shown that, in a dynamic network, it is possible to detect most of the malicious nodes and this result in a better package delivery relationship.

In 2015, ***Anjali Sardana ; Tushina Bedwal ; Akanksha Saini ; Radhika Tayal [2]***, given the analysis of the Black Hole ADOV performance by frequently changing the number of mobile nodes and also changing the nodes of the black hole. To analyze this, different performance metrics are used that include a medium end-to-end delay, packet loss and package delivery report and have seen that the effect on end-to-end delay is greater than packet loss.

In 2015, ***Pooja ; R. K. Chauhan [3]***, Three models of movement of the ONE simulator for mobility (shorter map-based movement model, random point movement model and group movement model) were analyzed and therefore the best model is selected as parameters of the simulation table. Here a probabilistic routing protocol is used based on suggestions to propose a scheme based on the local utility function to detect the nodes of the black hole. Then compare the performance of the network in the presence of a black hole and in the absence of a black hole with different performance metrics, such as packet drop, packet performance, and network overload. A simulator is used to simulate Black Hole attacks.

In 2016, ***Sushama Singh ; Atish Mishra ; Upendra Singh [4]***, An ad-hoc mobile network (MANET) is a wireless network such that nodes move dynamically in the network. In the network layer, many attacks, but only introduce the collaborative attack black hole, a group of black hole nodes easily employed against routing in mobile advertising networks called collaborative black hole attack. In this document, they introduced the trusted AODV routing protocol whose confidence value is calculated using the hyperbolic tangent function. The result showed an improvement in performance compared to the standard AODV protocol.

In 2016, ***Dhiraj Nitnaware ; Anita Thakur [5],*** This research attempts to develop a mitigation algorithm in order to avoid and prevent malicious attacks from real nodes. Attack black hole is one of the security threats that traffic to a node that does not exist on the network is redirected. The black hole node is presented in such a way by other nodes and the networks it knows the shortest path. Comprehensive research work is classified into three categories that are not attacking, attacking and preventive phase. Performance parameters collected for performance analysis and package delivery report against variable parameters such as the number of nodes, speed, pause time and the area to observe the impact of the attack of the black hole and the proposed mechanism different situations. He used a QualNet 5.2 simulator to simulate and evaluate the performance of the proposed solution. The complete experimental setup concludes that improving the mobile node increases network performance, but also increases the impact of the black hole. Subsequently, the improvement in the speed of the nodes degrades the impact of the black hole.

In 2016, ***Jay Thakker ; Jagruti Desai ; Lata Ragha [6]***, Recently a variety of routing protocols have been proposed for ad hoc wireless networks, but the AODV (On demand Distance Vector) protocol is popular because of its dynamic nature which is the exchange of routing information and the path search process starts only when it is required by a node to communicate with a destination node. The attack is launched in this protocol if an intermediate node behaves badly during the path search process and discards the packets that pass through it. This attack becomes more serious if the group of knots works in coordination to launch this attack. In this document, a mechanism to avoid a coordinated attack of this type called a black hole cooperative attack is proposed by calculating the trust value in each node using only the control packets that help reduce routing overhead.

In 2017, ***E.O. Ochola ; L.F. Mejaele ; M.M. Eloff ; J.A. van der Poll [7]***, MANETs are exposed to numerous security threats due to their characteristic features, which include the absence of a centralized control unit, open support, without infrastructure and dynamic topology. One of the most common attacks is the one known as the black hole attack, which is mainly aimed at MANET's reactive routing protocols, such as AODV and DSR. The MANET simulation scenarios based on AODV and DSR were performed using Network Simulator 2 (NS-2) and NS-3, introducing the black hole attack in each of the scenarios, to analyze the performance of the protocols. The different scenarios are generated by modifying the mobility (positions) of the nodes. The results also showed that performance decreases slightly when node mobility increases in the network. The increase in the speed of the nodes decreases both

the delivery speed of the packet and the end-to-end delay. The closer the node of the black hole approaches the source node that requires transmission, the worse the impact. An analysis focused on AODV indicates that, even with the introduction of relatively few black hole nodes in the network, there is still the possibility of generating significant interruptions in communication.

In 2017, ***Meghana Shinde ; D. C. Mehetre [8]***, This document focused more on routing that is secured and on the reliable model. Here they used the concept of active routing trust scheme to defend various types of attacks during data packet routing. These attacks mainly consist of a black hole attack, denial of service attack and selective forwarding attack. The system also protects data by hiding it during routing using the ECC algorithm, which provides security. The experimental results have shown that the proposed system improves safety, as well as extending the useful life of the network and low energy consumption and greater efficiency during the entire useful life of the network.

In 2017, ***M. V. S. S. Nagendranath ; Babu.A Ramesh ; V. Aneesha [9]***, MANET will not need any mounted infrastructure. The nodes in MANET will communicate with each alternative node if and as long as all the nodes measure within them. This distribution of nodes makes MANET vulnerable to various attacks, packet attacks or black hole attacks and replays are some of the possible attacks. It is very heavy to notice and exclude. To avoid packet loss attacks, the detection of misconduct and selfish nodes plays a necessary role in MANET. In this paper they compared all the techniques on how they notice the self-absorption link and the malignant node.

In 2018, ***Taranpreet Kaur; Rajeev Kumar [10]***, Denial of service is a known security problem in wireless sensor networks. Although the ZigBee protocol is designed based on safety and lower battery consumption, wireless sensor networks are still vulnerable to so many denial-of-service attacks, especially when nodes are deployed in an unsupervised environment. The attacker uses vulnerabilities to launch, many denial of service attacks on wireless sensor networks. In this document, several approaches to defend against denial of service attacks are described and an approach is proposed for the detection and defense of both the black hole attack and the wormhole attack. The proposed methodology is less complex and easier to implement, it also consumes less energy than the battery and, therefore, improves the useful life of the network.

In 2018, ***Ventrapragada Sree Pooja ; Todupunoori Rohit ; Nagulapally Manisha Reddy ; S Sudeshna [11]***, Safety is one of the most difficult problems in our daily activities. The ad-hoc mobile network (MANET) is a less open and wireless infrastructure medium. One of the main challenges here is the self-organizing and self-recovering network that causes dynamic topology, has no central infrastructure; It is also heavily influenced as data is transmitted. While the data is forwarded from the sending node to the receiving node, there may be a loss of packets during transmission, this is called "Blackhole attack". To overcome this, they proposed a solution method called "Dual Cryptography Technique with Secure Shell Protocol" that will help protect data with a double encryption and decryption algorithm with better results from existing approaches. When using our technique, security is safe to obtain confidentiality, availability and data integrity.

In 2018, ***Taku Noguchi ; Mayuko Hayakawa [12],*** A black hole attack is one of MANET's known security threats. A black hole is a security attack in which a malicious node absorbs all data packets by sending false routing information and deletes them without forwarding them. To defend against a black hole attack, in this document they proposed a new method to prevent black hole attacks based on thresholds that use different RREPs. To study the performance of the proposed method, they compared it with existing methods. The results of the simulation showed that the proposed method overcomes the existing methods in terms of package delivery speed, performance and routing overload.

In 2018, ***Gibson Chengetanai [13]***, this research has found a solution to reduce collaborative attacks of the black hole in wireless networks. The simulations were performed with the Network Simulator version 2.35 (NS2.35) simulation tool for the proposed AODV routing protocol and the results were presented and compared with other routing protocols. The results of the simulation showed that the proposed solution works in terms of package delivery ratio and average end-to-end delay in relation to other routing protocols.

In 2018, ***Giuseppe Primiero ; Agostino Martorana ; Jacopo Tagliabue [14]***, From a security point of view, VANETs (ad hoc vehicular networks) are vulnerable to attack by malicious users, due to the decentralized and open nature of the wireless system. For many of these types of attacks, detection is not feasible, which hinders the production of security. In this document, they provide an algorithmic definition and a simulation of a protocol based on trust and mitigation to contain a Black Hole style attack on a VANET. We experimentally show their optimal working conditions: total connectivity, followed by a random network; connection to external

networks; Early implementation of the protocol and classification of the message. We compare the results with those of the existing protocols and future work will focus on repeated transmission, forwarding of opportunistic messages and tests on real data.

In 2018, ***Vasiliy Krundyshev ; Maxim Kalinin ; Peter Zegzhda [15],*** In this article, information security issues have been addressed in VANET transport networks, a sub-type of mobile ad hoc (MANET) in which moving vehicles are considered hosts for wireless communications networks. They proposed a new approach to provide security for VANET and other types of relative transport networks using algorithms of artificial intelligence swarms. The article describes the algorithm itself, its features and its main advantages. The article presents the results of experimental studies that confirm the effectiveness of the swarm algorithm developed to protect against two common and difficult-to-detect routing attacks: black hole and wormhole.

In 2018, ***Victor Oluwatobiloba Adeniji ; Khulumani Sibanda [16]***, This article presents an assessment of the effect of black hole attack with other influential factors in the WMN. In this study, the NS-3 simulator with AODV was used as a routing protocol. The results show that the package delivery ratio and the WMN performance under attack decreases considerably compared to the WMN without attacks. On average, 47.41% of the transmitted data packets were removed in the presence of a black hole attack.

In year 2018, ***Shoukat Ali ; Muazzam A Khan ; Jawad Ahmad ; Asad W. Malik ; Anis ur Rehman [17],*** The IoT is now extended to IoET (Internet of Everything) to cover all existing electronic devices, such as networks of body sensors, VANETs, smart grid stations, smart phones, PDAs, autonomous cars, smart refrigerators and roasters capable of communicating and share information using existing network technologies. The sensor nodes in WSN have a very limited transmission range, as well as limited processing speed, memory capacity and low battery. Despite a wide range of applications that use WSN, its limited resource nature has led to a series of serious security attacks, for example, Selective attack, Jamming attack, Sinkhole attack, Wormhole attack, Sybil attack, Hello Flood attacks, Gray Hole and the most dangerous Blackhole attacks. Attackers can easily exploit these vulnerabilities to compromise the WSN network.

In 2018, ***Jose Grimaldo ; Ramon Martí [18]***, In this article, they analyzed the impact on the performance of black hole attacks on VANET in a real scenario. This is done by combining a realistic urban traffic scenario in Panama City with four main routing protocols (AODV, OLSR, DSR and DSDV) that function regularly and under attack from the black hole, and that rely on ns-3 and SUMO (Simulation urban mobility) simulation tools. Finally, the simulations show that the use of realistic scenarios produces more precise results closer to reality.

In 2018, ***Gibson CHENGETANAI [19],*** this research has come up with a solution to reduce collaborative attacks of black holes in wireless networks. The simulations were performed with the Network Simulator version 2.35 (NS2.35) simulation tool for the proposed AODV routing protocol and the results were presented and compared with other routing protocols. The results of the simulation showed that the proposed solution works in terms of package delivery ratio and average end-to-end delay in relation to other routing protocols.

III. Research Methodology

In this section the proposed system Digital Signature Authentication Scheme (DSAS) is been discussed. This chapter explains the working of DSAS method and implementation done on network simulator 2.

A. DSAS method

Mobile ad-hoc network is wireless network that contains a collection of different nodes communicate with each other without having to set up any infrastructure. But the security of such network is a major issue. So to achieve secure communication in these types of network some requirements must be fulfilled:-

- Between mobile nodes, a security association must be existed in the network; these security associations ensure non repudiation and authentication of trusted nodes.
- Between the nodes in the network, sensitive information must be exchanged confidentially.
- Integrity of the information exchanged within the network has to be maintained so that corrupted messages are detected and blocked.

In this research, there is symmetric cryptographic algorithms used to preserve integrity and confidentiality of information exchanged between mobile nodes and digital signature and hash function to ensure the authentication and integrity of trusted nodes in AODV routing protocol to prevent the effects of Blackhole attack in MANET. Symmetric cryptographic algorithm enables us to store the data in a condensed or compressed encryption form which results in a small size file that means, it improves the performance of MANET. Also it provides faster encryption/decryption Algorithm. Due to these advantages Advanced Encryption Standard (AES) is used, which is one of the favourite and currently used types of symmetric cipher algorithm, to perform data encryption and decryption.

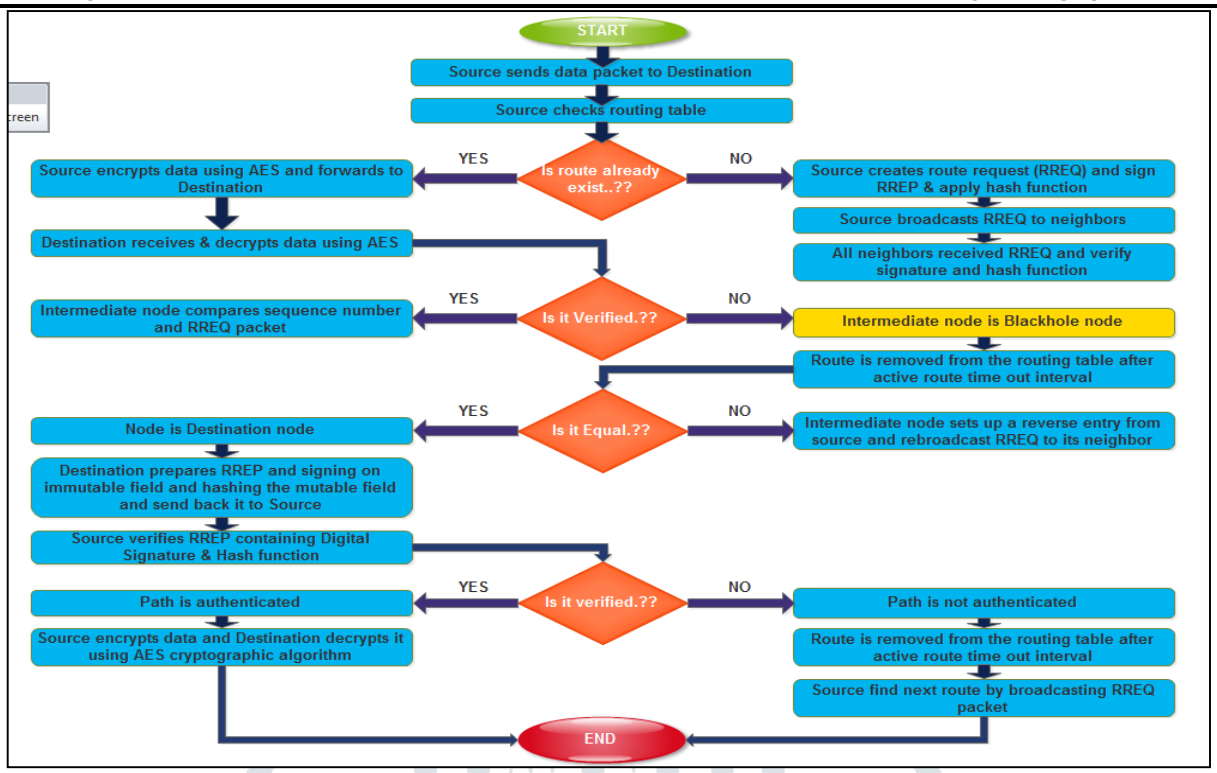

Figure 3: DSAS Methodology flowchart

This is an enhancement of AODV routing protocol to fulfill security feature such as integrity and authentication. DSAS_AODV provides an end-to-end authentication and hop-to-hop verification of the routing messages. The protocol assumes that a node has certified public keys of other nodes in the network and a certified private key for itself. DSAS_AODV uses asymmetric cryptography to authenticate all non-mutable fields of routing messages and a hash algorithm to authenticate the hop count (the only mutable) field. The protocol suggests appending an extension message that includes a hash value of the hop count and a digital signature of the packet using the private key of the sender. A node can verify a signature of a sender using the sender's public key to ensure the identity of the sender and verify hash value of the hop count using the hash function that is included in the packet to ensure the integrity of the packet. A node fails to verify hash value or digital signature discards the received routing packet.

As the protocol design is based on AODV, it uses the same route discovery and route maintenance procedure. A source node sends a RREQ to a destination includes a hashed value of the hop count and a signature of the RREQ by its private key. An intermediate node that receives a RREQ has to verify the hash value of hop count and the digital signature. If it succeeded in verifying both of them, it stores a reverse route entry to the source in its routing table, increments the hop count value in RREQ packet, generates a new hash value and rebroadcasts the RREQ again to its neighbor. The destination that succeeded in verifications has to reply by sending RREP that includes a hashed value of the hop count and a signature of the RREP by its private key. Similarly, the source and intermediate nodes have to verify both the hash of the hop count and the signature of the RREP before adding the forward route to their routing tables. This procedure ensures that both the source and the destination can identify its communication partner and avoid impersonation attacks. The working methodology of DSAS method is shown in figure 3.

The above scenario implies that it is impossible for intermediate nodes to reply to RREQs even if they have a route to the destination because the RREP message must be signed by the destination's private key which is known only to the destination. To imitate AODV that permits to other nodes that have a fresh route to the destination to send a RREP, SAODV suggests a delegation feature that allows intermediate nodes to reply to RREQ messages. This delegation is based on a double signature in which a node sends a RREQ message can include a second signature that is computed on a fictitious RREP message towards itself. Intermediate nodes stores this second signature in their routing table to be used if later a node asks for a route to the owner of the double signature. Then, the intermediate node generates the RREP message includes the double signature and signs this message with its own private key.

B. Digital Signature

It is used to authenticate the identity of the sender of the message. It also guarantees that the original contents of the message have not been altered. If the public key of the source node is known, any node can be verified the digital signature. This makes digital signature is scalable to large numbers of receiver nodes. In order to protect the integrity of the immutable data in RREQ and RREP messages, Digital signature algorithm is used. When a node receives a RREQ, it first verifies the signature before creating or updating a reverse route. Only if the signature is verified, it stores the route. Otherwise, RREQ is rebroadcasted. When a RREQ is received by the destination itself, it will reply with a RREP only if the AODV's requirements are satisfied. This RREP will be sent to the source node along with digital signature. When RREP, it first verifies the signature before creating or updating a route. Only if the signature is verified, it stores the route which is received by the node the signature of the RREP. This procedure is shown in figure 3.

C. Hash Function

A Cryptography hash function is considered as a function because it takes an input message and produces an output. It takes a message of arbitrary length that can be transformed in to a string of bits and computes from it a fixed -length or short number. The

Cryptographic hash value, such that any intentional or unintentional modification to the data with very high possibility will modify the hash value. The data that has to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digests.

In hash function the hash of a message y, represented as h (y) has the following properties:

- For any message y, it is relatively easy to compute h (y). This means that in order to be practical it can't take a lot of processing time to compute the hash.
- Given h(y), there is no way to find an y that hashes to h(y) in a way that is substantially easier than going through all possible values of y and computing h(y) for each one.
- Even though it is clear that many different values of y will be transformed to the same value h (y) because there are many more possible values of y, it is computationally infeasible to find two values that hash to the same thing.

***Step 1**: Source node wishes to send data packets to the destination*
***Step 2:** Then source checks its routing table if it has a current route to the destination*
If (route is already existed) {
Source node encrypts the data using AES then forwards to destination using the path
Destination node receives and decrypts the data using AES
} else {
***Step 3:** Source creates route request (RREQ) and signs on immutable fields of this RREQ (IP address and sequence number) and apply hash function on mutable field of RREQ (i.e. hop count)*
***Step 4:** Then source broadcasts RREQ to neighbor nodes*
***Step 5**: All neighbor nodes relieved RREQ verify the signature and hash functions*
If (not verified) {
Intermediate node is Blackhole node.
This route is removed from the routing table after active route timeout interval
} else {
***Step 6:** Intermediate node compares the destination sequence number in its routing table and RREQ packet*
If (not equal){
Intermediate node sets up a reverse entry for the source node. Then after intermediate node rebroadcasts the RREQ to its neighbor
} else {
The node is destination node. The destination node prepares RREP and signing on immutable fields and hashing the mutable fields of it then sends back these packets to the source using reverse entry
}
}
***Step 7:** The source node then verifies RREP containing digital signature and hash function on it*
If (verified) {
The path is authenticated and forward path entry is established
The source encrypt the data using AES cryptographic algorithm and sends it to the destination using the forward path.
Destination node receives and decrypts the data using AES cryptographic algorithm
}
Else {
The path is not authenticated and node is Blackhole node
The route entry is deleted after active route time out interval and route is not longer valid and cannot be used again
Source finds the next route by broadcasting RREQ
}

Figure 4: DSAS Algorithm

Hash chain algorithms can be used to improve the effectiveness of public key algorithms. The best known public key algorithms are sufficiently processor intensive that it is desirable to compute a message digest of the message and sign that, rather than to sign the message directly. Because the message digest algorithms are much less processor intensive, and the message digest is much shorter than the message. In proposed solution hash chain algorithm is used to authenticate the hop count field i.e. the only mutable fields of RREQ and RREP control messages, in such a way that allows every node that receives the message (either an intermediate node or the final destination node) to verify that the hop count has not been decremented by an attacker. Hash function avoids unauthorized modification of hop count by attacker nodes during the travel throughout the network. In our approach the middle node is allowed to response a route request packets (RREQ) and route reply packets (RREP) whenever the node has a fresh enough route to the destination nodes. The pseudo code for DSAS algorithm is shown in figure 4.

IV. Simulation of Blackhole attack in NS-2

The simulation is done using Network Simulator version 2.35 in the work done the black hole behaviour in wireless ad hoc network that uses AODV protocol is implemented. All the routing protocols in NS are installed in the directory. The changes are done in the source file named as aodv.cc and aodv.h. The simulated work shows the functioning of AODV protocol when works normally the implementation is done for 50 nodes. The flooding is also performed on the protocol. A comparative study at different parameters like delay, routing overhead, packet delivery ratio, throughput, routing overhead is done when the AODV protocol function in a normal behaviour and when the black hole node is introduced. The Blackhole generates a fake RREP for each RREQ it receives to incorporate itself in all routes, therefore all packets are sent to a point where they are not forwarded anywhere which is a form of a DoS attack. Later, when a source node uses this malicious node to forward data, it drops the received data. Figure 6 shows the definition of Blackhole attacker node in NAM and figure 5 shows the declaration of attacker in c++ file of AODV.

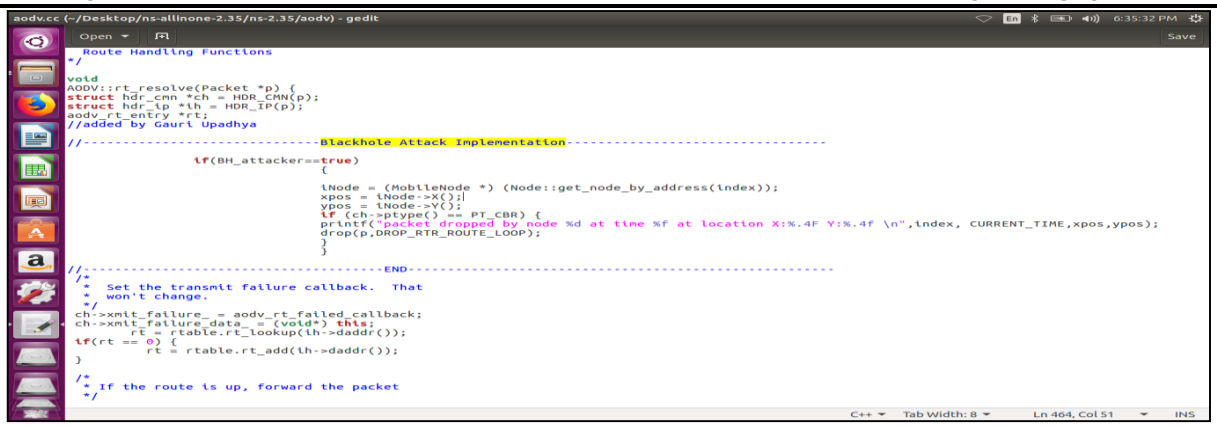

Figure 5: Blackhole node declaration in C++ file

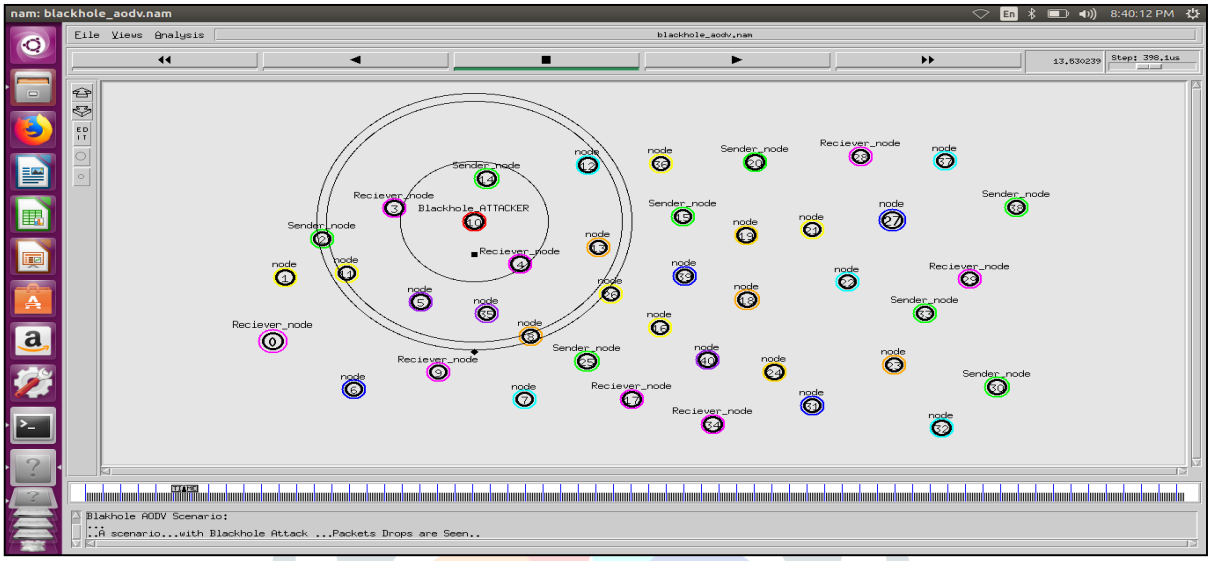

Figure 6: Blackhole drops packets, seen in NAM

A. Implementation of DSAS method in NS-2

Although NS-2 has many protocol implementations, it does not have an implementation for DSAS_AODV protocol. DSAS_AODV module is implemented by modifying the original AODV source code to include the security features such as hashing the hop count value of both RREQ and RREP packets and provide digital signature of these packets and RERR as well. These additional fields are appended to the RREQ, RREP and RERR packets of AODV protocol as a message extension. The size of the additional fields for RREQ, RREP, and RERR packets are 448 bytes, 448 bytes, and 404 bytes, respectively. RREQ and RREP include signature (64 bytes), top hash (16 bytes), hash (16 bytes) certificate (339 bytes) and other header information (13 bytes). RERR includes the signature (64 bytes) certificate (339 bytes) and other header information (1 byte). Secure Hash Algorithm 1 (SHA-1) is used for generating and verifying the hash values of the hop count.

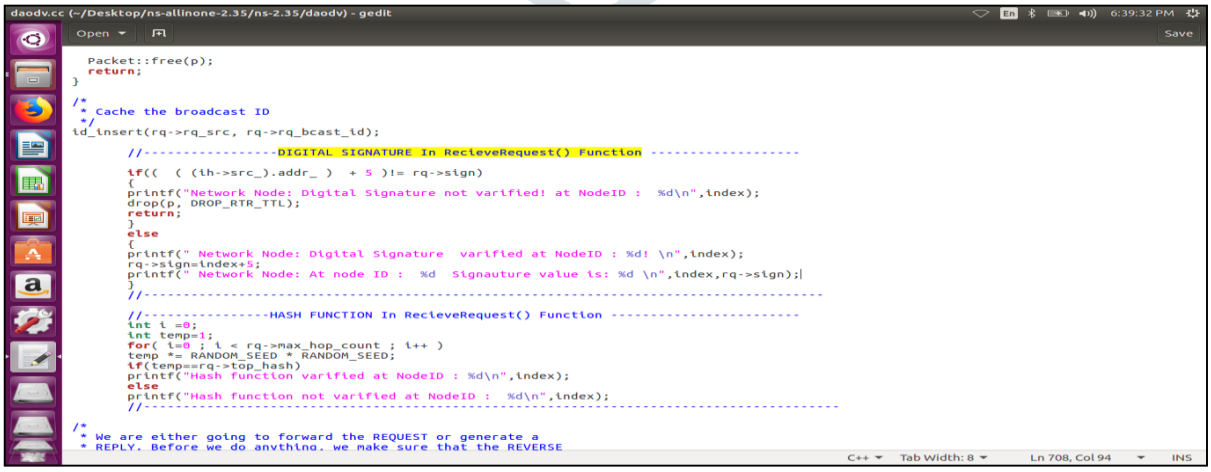

Figure 7: DSAS declaration in receive_request () function

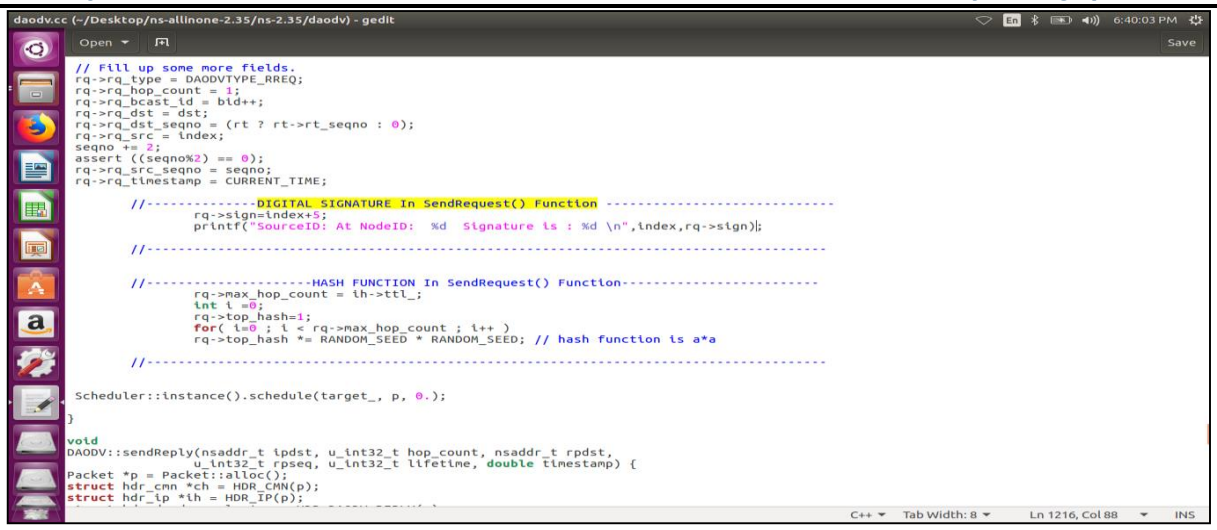

Figure 8: DSAS declaration in send_request () function

Form figure 7 to figure 8, some snapshots of implementation of DSAS method is shown. Here modification in header files and c++ libraries of AODV protocols has been modified accordingly. There are lot of files and folder in ns-all-in-one-2.35 packages which is been needed to be modified. To implement DSAS method, digital signature and hash function are included in the sending & receiving function of AODV protocols, so that node could securely send and receive data packets using this cryptographic feature and enhance the security of the protocol. This would strengthen the protocol to defend against Blackhole routing attack.

B. Performance Metrics

Efficient routing protocols can provide significant benefits to wireless ad hoc networks in terms of both performance and reliability. Routing protocols are evaluated using different performance metrics. They symbolize different characteristics of the overall network performance to achieve the required quality of service (QoS) and describe a number of quantitative metrics that can be used for evaluating the performance of ad hoc networks routing protocols. In this report, five metrics are used for evaluating and comparative study of their effect on overall network performance. The metrics proposed are packet delivery ratio, packet end-to-end delay, routing overhead, and network throughput.

(i).Packet Delivery Ratio

Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a CBR traffic source and the number of packets received by a CBR traffic sink. It can be obtained from the total number of data packets arrived at destinations divided by the total data packets sent from source nodes. It deals the loss rate as seen by transfer protocols and as such, it characterizes both the accuracy and efficiency of ad hoc routing protocols. It represents the highest throughput that the network can achieve. The performance is better when the packet delivery ratio is nearer to one.

$$Packet\ Delay\ Ratio = (\sum Number\ of\ packets\ receive / \sum Number\ of\ packets\ send)*100$$

(ii). Packet End-to-End Delay

The packet end-to-end delay is the average time that packets take to pass through the network. This is the time from the creation of the packet by the sender up to their reception at the destination's application layer and is expressed in seconds. The average end-to-end delay can be obtained by computing the mean of end-to-end delay of all successfully delivered messages. Therefore, end–to-end delay partially depends on the packet delivery ratio. As the space between source and destination increases, the possibility of packet drop increases. Hence it includes all the delays caused by buffering during route discovery latency, queuing at the boundary queue, retransmission on delays at MAC, and propagation and transfer times.It is calculated as the total delay duration of all successfully transmitted data packets from source node to destination node. It is measured in seconds or milliseconds. The higher the end-to-end delay metric is, the higher the delay in routing packets and consequently the lower the efficiency of the protocol. It is given by following equation:

$$Delay\ Time\ (t) = N\ ((L)/R)$$

Where, N is total number of senders sending packets, L is length of packets and R is transmission rate.

(iii). Routing Overhead

Mobile ad-hoc networks are designed to be scalable. As the network grows, various routing protocols perform in a different way and the amount of routing traffic increases. Routing Overhead is an important measure of the scalability of protocol, and thus the network. It is defined as the total number of packets transmitted over the network, articulated in bits per second or packets per second. This is the ratio between the total control packets generated to the total data packets during the simulation time. Some sources of routing overhead are network congestion and route error packets. It is the total number of routing packets sent divided by the total number of data packets received. This accounts for the overhead of the routing protocols. The number of total routing packets includes the number of route request packets (RREQ), route reply packets (RREP), route error packets (RERR), acknowledgement packets, hello packets etc., mathematically it is calculated as:

$$Routing\ Overhead = (No.\ of\ (RREQ + RREP + RERR + forward)\ Packets) / (No.\ of\ Nodes)$$

The higher the routing overhead metric is the higher the overhead of routing protocol and consequently lower the efficiency of the protocol.

(iv). Throughput

Throughput is one of the basic parameter which is considered for performance evaluation of the network. It is the average number of successfully delivered data packets on a network. In other words throughput describes as the total number of received packets at the destination out of total transmitted packets. Throughput is calculated in bytes/sec or a data packet per second, mathematically throughput is calculated as:

*Throughput (bytes/sec) = (Total no. of received packets at destination * packet size) / Total Simulation Time*

The higher the Throughput metric is, the higher the value of received routing packets and the higher the efficiency of the protocol. So, the value of throughput should be high as much as possible.

(v). Normalized Routing Load

It is defined as the total number of packets transmitted over the network, articulated in bits per second or packets per second. This is the ratio between the total control packets generated to the total data packets during the simulation time. Some sources of routing overhead are network congestion and route error packets. The number of total routing packets includes the number of route request packets (RREQ), route reply packets (RREP) and forwarded packets mathematically it is calculated as:

Routing Overhead= (No. of (RREQ + RREP + forward) Packets) / (No. of Nodes)

The higher the NRL metric is the higher the overhead of routing protocol and consequently lower the efficiency of the protocol.

V. Results & Discussion

For simulation and result analysis, it must require setting of simulation parameters and mobility models. The summarized simulation parameter is depicted in table 1.

Table 1: Simulation Parameters

parameter	value
Simulator	NS-2 (ns-all-in-one-2.35)
Routing protocol	AODV, DSR, Secure AODV, DSAS AODV, Blackhole AODV
Simulation time	150 seconds
Number of nodes	50
Traffic model	Constant Bit Rate (CBR)
Packet size	512 Bytes
Nodes velocities	2 m/s, 5 m/s, 10 m/s, 15 m/s, 20 m/s, 25 m/s, 30 m/s
Simulation Area	1000 * 1000 meter square
Number of Blackhole node	1
Mobility model	Random Way Point
Mac layer protocol	IEEE 802.11

In this research Random Waypoint Model is used, where mobile node is allowed to move at random in any direction .Constant Bit Rate (CBR) traffic with a transmission rate of 4 packets per second is used. Nodes in experimental scenario select any arbitrary destination in the 1000 X 1000 M2area and moves with the speed of 2 m/s, 5 m/s, 10 m/s, 15 m/s, 20 m/s, 25 m/s and30 m/s . 50 nodes are used in scenarios with change in pause times and 1 number of Blackhole node with simulation times of 100 seconds to compare the performance of the protocols for low as well as high density environment and for low mobility of the nodes to high mobility.

This section discusses the graphs of Normal_AODV, Normal_DSR, Secure_AODV, DSAS_AODV and Blackhole_AODV protocols based on various parameters like packet delivery ratio, end to end delay, throughput, normalized routing load and routing overhead.

A. Packet delivery ratio graph

Following figure 9 shows the packet delivery ratio (PDR) graph obtained for all the protocols considered in this research. PDR is decreasing continuously for all protocols because the velocity of nodes is increasing varied from 2 m/s to 30 m/s and indicates DOS/DDOS attacks cause the packet exchange during the communication process fail & decrease the network perfomance. The highest PDR value is obtained for normal behavior of protocols i.e. for Normal_AODV and Normal_DSR protocols and the lowest value of

PDR is obtained for Blackhole_AODV protocol since attacker node drops the packets. The following figure clearly shows that the proposed DSAS_AODV is improved by 7.2 % than the Secure_AODV protocol.

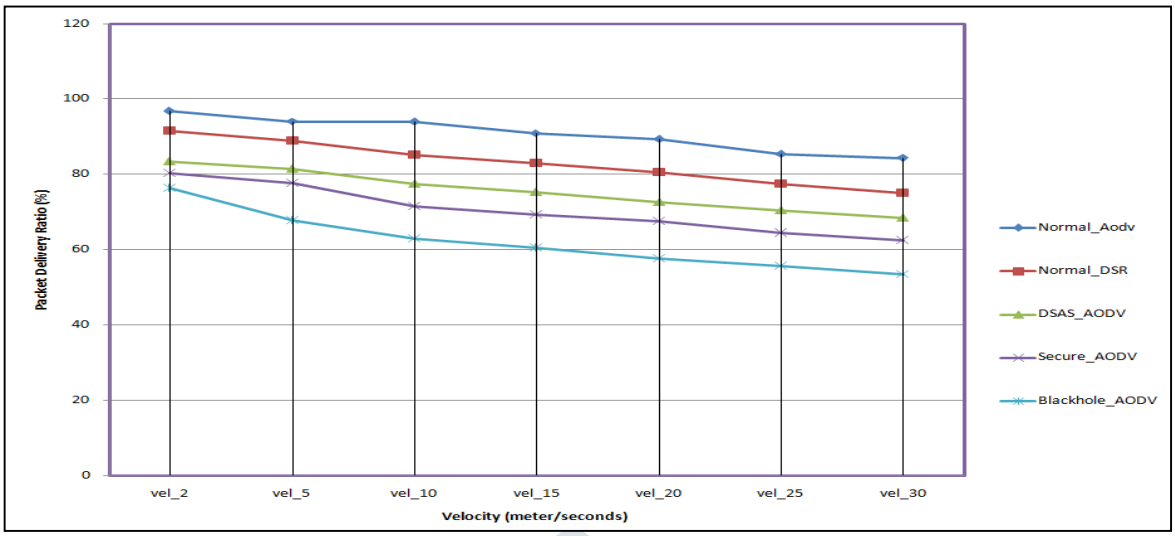

Figure 9: Packet Delivery Ratio

B. End to end delay graph

Following figure 10 shows the end to end delay (E2E) graph obtained for all the protocols considered in this research. Simulation result shows that the average end to end delay of the protocol without security mechanism is much higher and the trend of average delay increases when the number of node is increased. The highest E2E value is obtained for Blackhole_AODV protocol since attacker node drops the packets and the lowest value of E2E is obtained for DSAS_AODV protocol and Secure_AODV protocol, this shows that both protocols are able to defend against Blackhole attack successfully and minimize the effect of Blackhole attack in MANET. The following figure clearly shows that the proposed DSAS_AODV is improved by 10.257 % than the Secure_AODV protocol.

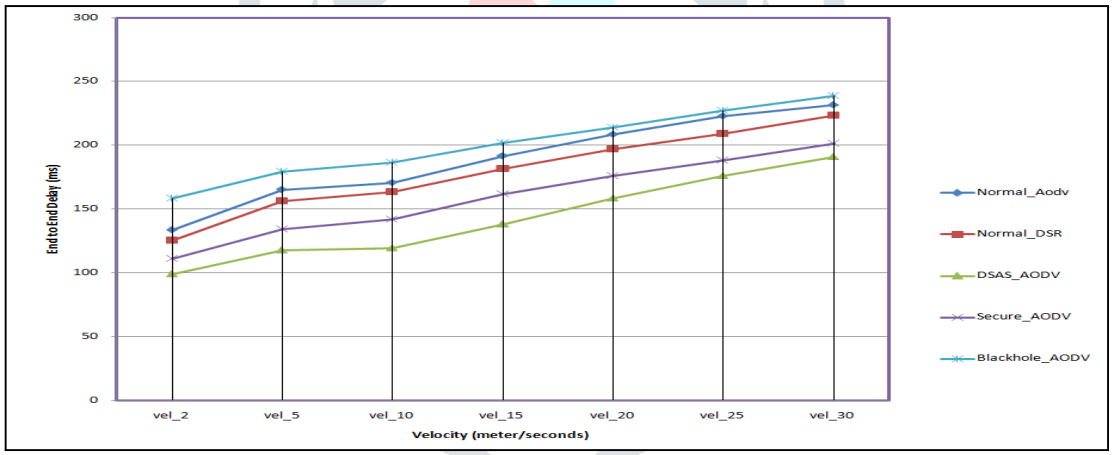

Figure 10: End to End Delay

C. Throughput graph

Following figure 11 shows the throughput graph obtained for all the protocols considered in this research. Throughput is decreasing continuously for all protocols because the velocity of nodes is increasing varied from 2 m/s to 30 m/s. The highest throughput value is obtained for normal behavior of protocols i.e. for Normal_AODV and Normal_DSR protocols and the lowest value of PDR is obtained for Blackhole_AODV protocol since attacker node drops the packets. The following figure clearly shows that the proposed DSAS_AODV is improved by 9.79 % than the Secure_AODV protocol.

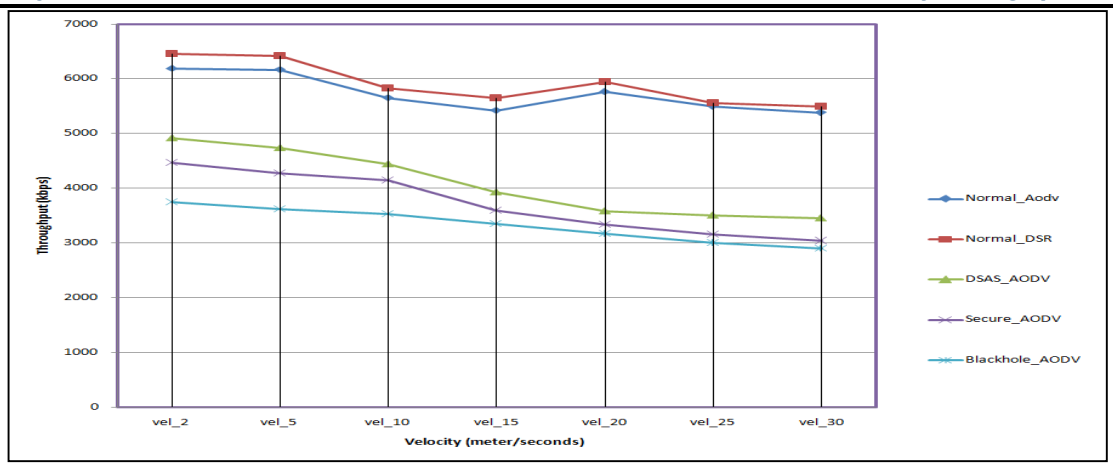

Figure 11: Throughput

D. Normalized routing load graph

Following figure 12 shows the normalized routing load (NRL) graph obtained for all the protocols considered in this research. NRL is increasing continuously for all protocols because the velocity of nodes is increasing varied from 2 m/s to 30 m/s. The highest NRL value is obtained for Blackhole_AODV protocol since attacker node drops the packets and the lowest value of PDR is obtained for DSAS_AODV protocol and Secure_AODV protocol, this shows that both protocols are able to defend against Blackhole attack successfully and minimize the effect of Blackhole attack in MANET. The following figure clearly shows that the proposed DSAS_AODV is improved by 6.396 % than the Secure_AODV protocol.

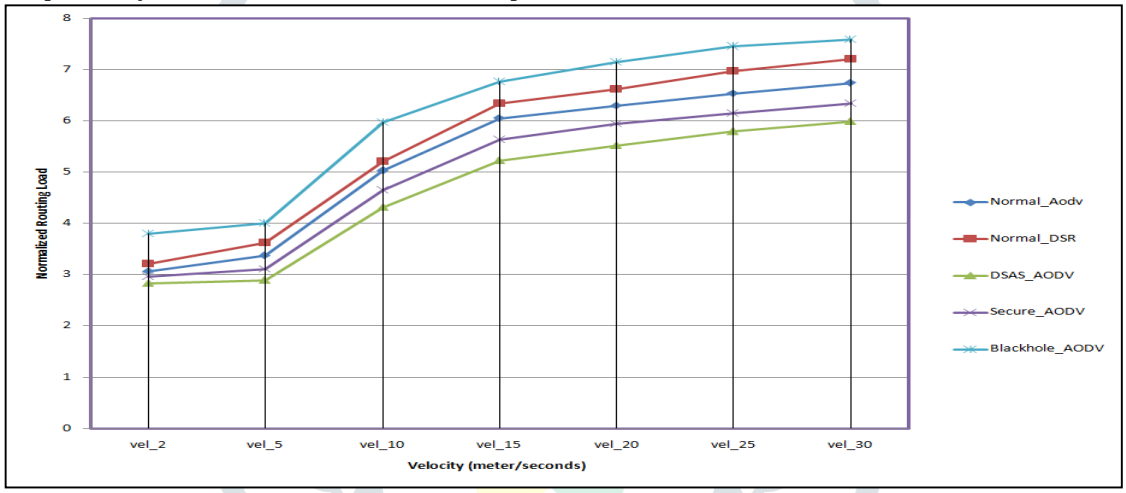

Figure 12: Normalized Routing Load

E. Routing overhead graph

Following figure 13 shows the routing overhead (RO) graph obtained for all the protocols considered in this research. RO is increasing continuously for all protocols because the velocity of nodes is increasing varied from 2 m/s to 30 m/s. The highest NRL value is obtained for Blackhole_AODV protocol since attacker node drops the packets and the lowest value of PDR is obtained for DSAS_AODV protocol and Secure_AODV protocol, this shows that both protocols are able to defend against Blackhole attack successfully and minimize the effect of Blackhole attack in MANET. The routing overhead of all routing protocols increase as the number of nodes velocity increases and proposed algorithm has better perforce compared to other routing protocols as a result of continuous detection of Blackhole nodes. The following figure clearly shows that the proposed DSAS_AODV is improved by 3.047 % than the Secure_AODV protocol.

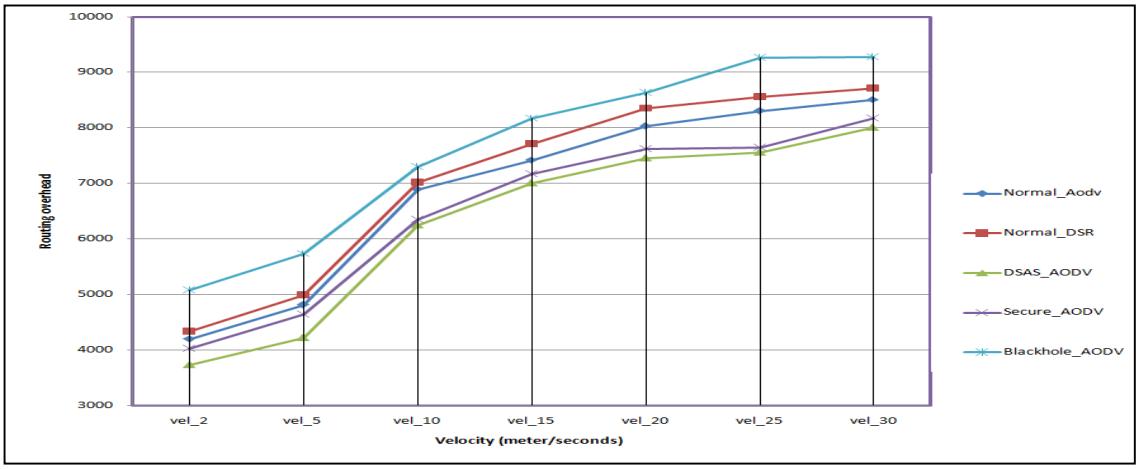

Figure 13: Routing Overhead

IV. CONCLUSION & FUTURE WORK

In this research, the effect of the Blackhole attack is analyzed in AODV routing protocol of MANET and proposed a solution for preventing the effects of this attack in an AODV routing protocol. For this purpose Blackhole AODV is implemented that can behaved as Blackhole nodes and its solution that can be used to prevent and minimized its effect in MANET. Afterwards, various scenarios has been implemented and simulated the Blackhole attack in NS-2, and it is seen the number of packets dropped and routing overhead of AODV routing protocol are increased but throughput and packet delivery ratio of this protocol are decreased in all scenarios. That means its performance is decreased as Blackhole Node drops packets in Mobile Ad hoc Network. Commonly Blackhole node or Blackhole attack affects the overall network performance and connectivity of AODV routing of MANET. Finally, to prevent the effect of Blackhole attack, a solution is implemented by using AES Cryptography Algorithm and Digital Signature and named it as Digital Signature Authentication Scheme (DSAS) method. As it can be observed from the simulation results, the proposed solution effectively prevents the effects of Blackhole attack in AODV routing protocols of MANET.

The simulative results showed that DSAS method is successfully improvised the existing Secure AODV protocol. DSAS AODV shows 7.2 % improvement in terms of packet delivery ratio, 10.257 % improvement in terms of average end to end delay, 9.79 % improvement in terms of throughput, 6.396 % improvement in terms of normalized routing load and 3.047 % improvement in terms of routing overhead compared to existing Secure AODV protocol. Following table 2 shows the percentage of improvement of DSAS AODV.

Table 2: percentage improvement of DSAS method

Parameter	Secure AODV	DSAS AODV	% improvement
Packet Delivery Ratio	493.7343	529.3239	**7.2 %**
End to End Delay	1115.149	1000.7666	**10.257 %**
Throughput	26034.94	28584.47	**9.79 %**
Normalized Routing Load	34.8091	32.5827	**6.396 %**
Routing Load	45640	44249	**3.047 %**

This section highlights areas for potential future research, based on the contributions of this thesis. Many research ideas can be derived from our research work such as: Introducing similar algorithms that can resist other attacks on MANETs using the DSAS method. Proposed method can be used as an underlying concept to design algorithms that can resist the other dangerous attacks such as wormhole attack. Examining this new algorithm in larger networks to confirm the success of their design and to discover and address their advantages and disadvantages in these networks. This is can be a key to enhance the DSAS algorithm to achieve success in discovering and excluding only genuine malicious nodes.

REFERENCES

[1] Nidhi Choudhary ; Lokesh Tharani, “Preventing Black Hole Attack in AODV using timer-based detection mechanism”, International Conference on Signal Processing and Communication Engineering Systems, Electronic ISBN: 978-1-4799-6109-2, IEEE, 2015.

[2] Anjali Sardana ; Tushina Bedwal ; Akanksha Saini ; Radhika Tayal, “Black hole attack's effect mobile ad-hoc networks (MANET)”, International Conference on Advances in Computer Engineering and Applications, Electronic ISBN: 978-1-4673-6911-4, IEEE, 2015.

[3] Pooja ; R. K. Chauhan, “An assessment based approach to detect black hole attack in MANET”, International Conference on Computing, Communication & Automation, Electronic ISBN: 978-1-4799-8890-7, IEEE, 2015.

[4] Sushama Singh ; Atish Mishra ; Upendra Singh, “Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm”, Symposium on Colossal Data Analysis and Networking (CDAN), Electronic ISBN: 978-1-5090-0669-4, IEEE, 2016.

[5] Dhiraj Nitnaware ; Anita Thakur, “Black hole attack detection and prevention strategy in DYMO for MANET”, 23rd International Conference on Signal Processing and Integrated Networks (SPIN), Electronic ISBN: 978-1-4673-9197-9, IEEE, 2016.

[6] Jay Thakker ; Jagruti Desai ; Lata Ragha, “Avoidance of co-operative black hole attack in AODV in MANET”, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Electronic ISBN: 978-1-4673-9338-6, IEEE, 2016.

[7] E.O. Ochola ; L.F. Mejaele ; M.M. Eloff ; J.A. van der Poll, “Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack”, SAIEE Africa Research Journal (Volume: 108 , Issue: 2 , June 2017), Page(s): 80 – 92, Print ISSN: 1991-1696, IEEE, 2017.

[8] Meghana Shinde ; D. C. Mehetre, “Black Hole and Selective Forwarding Attack Detection and Prevention in WSN”, International Conference on Computing, Communication, Control and Automation (ICCUBEA), Electronic ISBN: 978-1-5386-4008-1, IEEE, 2017.

[9] M. V. S. S. Nagendranath ; Babu.A Ramesh ; V. Aneesha,” Detection of Packet Dropping and Replay Attacks in MANET”, International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Electronic ISBN: 978-1-5386-3243-7, IEEE, 2017.

[10] Taranpreet Kaur ; Rajeev Kumar, "Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol", IEEE International Conference on Smart Energy Grid Engineering (SEGE), Electronic ISBN: 978-1-5386-6410-0, IEEE, 2018.
[11] Ventrapragada Sree Pooja ; Todupunoori Rohit ; Nagulapally Manisha Reddy ; S Sudeshna," Mobile Ad-hoc Networks Security Aspects in Black Hole Attack", 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Electronic ISBN: 978-1-5386-0965-1, IEEE, 2018.
[12] Taku Noguchi ; Mayuko Hayakawa, "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks", : 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Electronic ISSN: 2324-9013, IEEE, 2018.
[13] Gibson Chengetanai, "Minimising Black Hole Attacks to Enhance Security in Wireless Mobile Ad Hoc Networks", 2018 IST-Africa Week Conference (IST-Africa), Electronic ISSN: 2576-8581, IEEE, 2018.
[14] Giuseppe Primiero ; Agostino Martorana ; Jacopo Tagliabue, "Simulation of a Trust and Reputation Based Mitigation Protocol for a Black Hole Style Attack on VANETs", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Electronic ISBN: 978-1-5386-5445-3, IEEE, 2018.
[15] Vasiliy Krundyshev ; Maxim Kalinin ; Peter Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks", IEEE Industrial Cyber-Physical Systems (ICPS), Electronic ISBN: 978-1-5386-6531-2, IEEE, 2018.
[16] Victor Oluwatobiloba Adeniji ; Khulumani Sibanda, "Analysis of the effect of malicious packet drop attack on packet transmission in wireless mesh networks", Conference on Information Communications Technology and Society (ICTAS), Electronic ISBN: 978-1-5386-1001-5, IEEE 2018.
[17] Shoukat Ali ; Muazzam A Khan ; Jawad Ahmad ; Asad W. Malik ; Anis ur Rehman, "Detection and prevention of Black Hole Attacks in IOT & WSN", Third International Conference on Fog and Mobile Edge Computing (FMEC), Electronic ISBN: 978-1-5386-5896-3, IEEE, 2018.
[18] Jose Grimaldo ; Ramon Martí, "Performance comparison of routing protocols in VANETs under black hole attack in Panama City", International Conference on Electronics, Communications and Computers (CONIELECOMP), Electronic ISSN: 2474-9044, IEEE, 2018.
[19] Gibson CHENGETANAI, "Minimising Black Hole Attacks to Enhance Security in Wireless Mobile Ad Hoc Networks", IST-Africa 2018 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, ISBN: 978-1-905824-60-1, IEEE, 2018.