International Journal of Engineering & Technology, 7 (3.27) (2018) 270-276

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Sybil Attack Detection Based on Authentication Process Using Digital Security Certificate Procedure for Data Transmission in MANET

P. Muthusamy[1*], T. Sheela[2]

[1]*Research Scholar, Department of Computer Science and Engineering, Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.*

[2]*Professor & Head, Department of Information Technology, Sri Sairam Engineering College, Chennai.*

Abstract

Mobile devices are becoming very popular due to the wide range of networking competence for the mobile device users. The security issues in MANET become the control towards the management of the multiple numbers of nodes in the MANET is distributed. To strategy for overcome the Sybil attack in MANET and improve the efficiency of the Sybil attack detection by enhancing the data confidentiality and reliability. The primary objective of this research work is to develop a scheme to detect and prevent the Sybil attack in the MANET and to provide a highly reliable data transmission approach. The proposed system ensures the availability, confidentiality, authenticity and reliability of the information using digital certificate chains and secret sharing schemes. To detect the sybil node during the route discovery process, the nodes authenticate each other by providing the digital security certificate (DSC). The digital security certificate proves the nodes and allows only authorized node to participate in the route to transmit the data packets from the source to destination. It will not ensure the confidential data transmission when the legitimate node exhibits the malicious behavior in certain circumstances. When any intermediate nodes learn about the data packet that is being transmitted, then the security in data transmission becomes a critical factor. The safety of the network can be enhanced by preventing the sybil attack in MANET by increasing the data confidentiality and reliability. Only certified and authenticated nodes can participate in the route to transfer the data packets between the nodes. To prevent the sybil attack, it is necessary to secure the data that is transmitted over the insecure communication routes.

Keywords: *Digital security certificate, route discovery, an authentication process, attack detection, sybil attack, MANET.*

1. Introduction

Mobile devices are becoming very popular due to the wide range of networking competence for the mobile device users. Presently there are varieties of applications available to be accessed on the mobile devices to fulfill the routine tasks. The group of mobile devices forms a network called the mobile ad hoc network (MANET). These are the infrastructure less network where the nodes can join or move out of the network‘s range at any time. A node can improve performance as a router to forward the data to the neighbor nodes.

An essential concern for basic functionality of a wireless network is the security in MANET. When all the security requirements have been met, accessibility of network services, confidentiality, and integrity of data can be achieved. Since MANET acquires open medium, rapidly changing topology, lack of central administration and no robust defense mechanism, they severely suffer from security attacks.

The other features like infrastructure less, wireless link use, multi-hop, node movement, amorphous, power limitations, memory, and computation power limitation and physical vulnerability of mobile devices seriously ruin the security factors of the MANET.

All the security services of Ad hoc networks can be enclosed altogether like other networks. The goal of these services is to protect information and resources from attacks and misbehavior of the nodes.

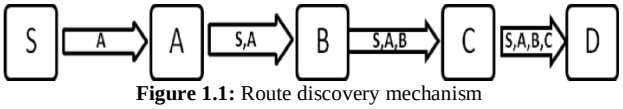

Figure 1.1: Route discovery mechanism

When the Source node S wants to start the data communication with destination D in the network, it checks its routing cache. When around is no route obtainable to the destination in the route cache or if the way has expired, it initiates the route discovery mechanism by broadcasting the route request message RREQ to the neighbor nodes. Figure 1.1 illustrates the path discovery mechanism of the DSR routing protocol. When the RREQ reaches the destination or any intermediate node that has anew route to the destination node then the route reply message RREP is generated. When the source node S receives the RREP, it updates its cache, and the data is routed through the discovered path.

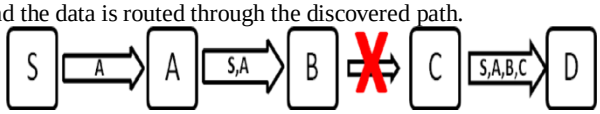

Figure 1.2: Data maintenance process

For example, in Figure 1.2, if Bis unable to deliver the packet to the next intermediate node C, then Breturns a ROUTE ERROR (RERR) to A, asserting that the connection from Bto Cis currently broken. Node Athen removes this broken link from its cache. The function of the upper layer protocols such as TCP is to retransmit

the original packet. For retransmitting the other packets to the same destination D, Source S checks in its route cache for another way to D. If S has another path to Din its route cache, it can retransmit the packet using the alternate route immediately.

A Sybil attack is an attack caused at the network layer, where malicious node promotes itself as it is consuming the optimal way to the terminus by sending the false routing information. The intermediate nodes will keep transmitting the packets through the route announced by the malicious node. The malicious node will not forward rather it will drop all the packets. Sybil attacks are categorized as single Sybil attack and cooperative Sybil attacks. Commonly the MANETs are most vulnerable to the single 20 Sybil attack. In a singleSybil attack, there is only one malicious node within a network range.

In a cooperativeSybil attack, there are multiple Sybil nodes within the specified network range. To establish a route the sybil node advertises itself as the router having the routes to the destination. The legitimate node initiates the route discovery process by forwarding RREQ packet through the sybil node. The sybil node can spitefully drop the RREQ and alter the destination identification. Once the RREQ packets are intercepted the sybil node can fabricate the RREP packet to advertise itself that it contains the shortest path to the destination. Now the routes are established through the malicious node.

The legitimate node sends the data packet to the sybil node. The sybil node will initiate the powerful attack there by dropping all the packets within the node. The digital security certificate chain is a security certificate which is self-organized and Public Key Infrastructure (PKI) legitimate by a chain of nodes deprived of the use of animportant third party.A certificate is a required between a node, its community key, and the security parameters.A set of refuge certificates that form a cable is used to represent authentication.

To achieve the maximum level of node participation every node in the network has same roles and responsibilities. All the participating nodes authenticate its neighbors by creating and issuing certificates for the neighbors and preserve the set of certificates it has issued. The certificates are issued based on the security parameters of the node. Certificates issued by the node to other nodes and records received by the nodes from the other nodes are stored in the local repository.

The methodologies to improve the security factors are analyzed on the dynamic topology. It is formulated that digital security certificate scheme offers a better safety in forwarding the data without allowing the intruder to hack it. The Secret sharing scheme 29 enables the node to transfer the data without allowing the thief to learn any information about the data that is being shared.

2. Literature Survey

The Sybil Attack Detection Using Vehicular ad hoc network (VANET) Vehicular ad hoc network (VANET) is a type of mobile ad hoc network (MANET) employing wireless communication for vehicle to vehicle communication the vehicular network [1], a Message is broadcasted by more than one vehicle and receiver decides what to do base on the number of incoming messages..

The Sybil Attack Detection for Mobile ad hoc networks (MANETs) require a unique, distinct, and persistent identity per node is order for Their security protocols to be viable, Sybil attacks pose a serious threat to such networks [2]. A Sybil attacker can either create more than one identity on a single physical device is order to launch a coordinated attack on the network or can switch identities is order to weaken the detection process, there by promoting lack of accountability network.

The Sybil attacks can cause damage are both Networking layer and Application layer. The Networking layer, the cooperation among virtual nodes leads to the possibility of using more channel resource than other benign nodes [3]. The Sybil nodes are expected to be detected by using this approach because they are at the same position where the malicious node generates them.

Sybil attack where is a node masquerade as several different nodes, called Sybil nodes disrupting the proper functioning of the network [4]. A Sybil attacker can create more than one identity on a single physical device is order to launch a coordinated attack on the network or can switch identities is order to weaken the detection process, thus promoting lack of accountability in the network. Sybil attacks can distort routing protocols in adhoc networks, especially the multicast routing mechanism.

The Sybil attack using attack prevention algorithm and also introduced the Priority Batch Verification Algorithm to provide an immediate response to the emergency vehicles. When an receives multiple requests from different vehicles at a same time, time delay can occur to process by these Sybil nodes To detect the Sybil attack, two timestamps which are obtained from the last two passed by the vehicle must be enclosed with the traffic message sent to legitimate vehicles [5].

Sybil attack is a network attack a node acquires multiple fake identities .A node or a device takes many identities that may not necessarily be lawful. Sybil attack, which means that a malicious node can claim multiple fake identities proving to be harmful to a number of ad hoc network applications [6]. Sybil nodes can also be used to launch Denial of Service attacks that can harm the operations of network, leaving other legitimate nodes out of service by affecting data dissemination protocols.

The Sybil attack and detect Sybil users, while protecting user's privacy as well the prevent Sybil attack, need to find a way to prevent users from creating multiple pseudo-identities at a given time period. Sybil users past privacy still need to be protected [7]. And normal users are able to detect Sybil users using the information provided by the revocation Sybil user.

The Sybil attack intrusion detection technology and analyzed the characteristics of Sybil attack. Then an improved ratios-based technique to identify Sybil nodes with very high accuracy [8], even when they perform power control. Sybil attack synthetically according to the received signal strength even when they perform power control the technique to identify Sybil nodes with very high accuracy, even when they perform power control.

The Privacy-Preserving Detection of Sybil Attacks Attackers have more computational power and canalter their transmission signal strength. Attackers can use more than one certified pseudonymto send the same message [9]. Attackers can collude to launch a Sybil attack. Sybil attack is peer-to-peernetworks, this attack affect distributed networks

Network attacker disturbs the accuracy count by increasing its trust and decreasing others or takes off the identity of few mobile nodes MANET. Mobile Ad hoc Networks (MANETs) are vulnerable to different kinds of attacks like Sybil attack [10]. To present practical evaluation of efficient method for detecting lightweight Sybil Attack and without using any additional resources such as trusted third party and Received Signal Strength to detect Sybil attacker.

Sybil Attacks is Opportunistic Networks These networks have fragile structures and the topology of the network is changed frequently, so it is impossible to have a Trust Third Party as a certificate authority [11]. There are many different attacks against these networks and one of them is Sybil Attack. A new trust connection structure for Sybil attacks detection in OppNet.

Sybil attack a reputation system is destroyed by falsifying identities in peer to peer networks. Communication between the users of networks only requires the users to be part of the same network [12]. The Sybil attack was described in different networks like social networks, sensor networks, and peer to peer networks. Social Networks, Sybil nodes can be identified the Sybil attack including radio resource testing, key validation for random key redistribution, position verification and registration.

Sybil Attack Detection Technique Sybil attack is an attack which uses many identities at a time or one identity at a time. The identities Used by Sybil attackers are either created by it or uses

someone else's identity [13]. Sybil attackers distribute secret data is other networks and it reduces the secrecy of network. Sybil attackers cause immeasurable loss to a network.

The Sybil Attack Prevention and Detection Vehicular Ad hoc Network Each vehicle participates the Sybil node detection. All nodes are communication range of sender, receive the beacon packets will form a group of neighboring nodes the process of group formation is same as described [14]. Whenever a Sybil attacker creates a fake identity, all the identity will have same physical properties and same neighbor set.

Attack Detection in Vehicular Network based on Received Signal Strength Sybil attack is particularly easy to perform in wireless network due to the broadcast nature of the wireless medium [15]. If normal vehicles cannot recognize the Sybil attack vicinity, they might make a wrong decision based on the false information advertised by an attacker node Sybil attack.

Attack Detection Scheme for Wireless Sensor Network Sybil attack was first introduced in a peer-to-peer network environment by Sybil node tries to forge multiple identities, which will destroy distributed storage system redundancy mechanism [16]. The Sybil attack also exists to the wireless sensor networks, and establish a shared key authentication between nodes by the base station to defend against Sybil attacks.

A Sybil attacker could disturb the generation of routes when a multipath or geographic routing algorithm is used, by appearing to several places are generated routes affect the results of data aggregation by contributing to the process of aggregation several time evade detection while behaving maliciously by spreading the actions he executes over the forged identities and prevent the network [17].

The Sybil attacks are Military Wireless Sensor networks (MWSNs). The identification of Sybil attacker is based on two types of authentication techniques. The first is based on the use of tags embedded Soldiers to authenticate them and get certificates [18]. The second is based on the use of those certificates by soldiers to authenticate them to their neighbors. The solution prevents Sybil attacks by identifying soldiers that are using two valid certificates at the same time the only entities that are able to detect the Sybil attack.

Detection Mechanism for Social Networks Sybil attack is a centralized approach for detecting Sybil node [19]. The centralized approach there is a central authority is used to detect the Sybil node Sybil community detection algorithm is used to detect Sybil community surrounding it after detecting one Sybil node. The Sybil community detection algorithm takes the social graph and a known Sybil node is Sybil attack.

Sybil attack detection framework has two components first, evidence collection second evidence validation. Every node to collect the network collects the evidences by observing the activities of neighboring nodes [20]. These evidences are validated by running sequential hypothesis test to decide whether neighboring node is a benign node or Sybil node Lightweight Sybil Attack Detection Framework.

3. Materials and Methods

MANET provides a possibility of creating a network in situations where setting the infrastructure would be impossible or prohibitively expensive. The dynamic changing nature of network topology creates any node in MANET to join and move out of the network at any instant. The controller towards the organization of the nodes in the MANET is distributed, and this feature does not give declaration towards the security characteristics of the network. There are many routing attacks caused due to lack of security. In general, attacks are the threats against the physical, MAC and network layer which are the most critical layers that function for the routing mechanisms of MANETs. The network layer is affected by the Sybil attack, where the sybil node either does not forward the packets or edits the messages by adding or changing the parameters in the routing messages. Most of the direction-finding protocols do not discourse the issues of theSybil routing attack. This results in a strategy requirement to overcome the Sybil attacks in MANET. The solution is proposed to detect and prevent the Sybil attack using three phases there is Route Discovery Process, Authentication Process, and Sybil attack Node Detection Process.

3.1. Route Discovery Process

Once a source node S wants to find a path to a terminus node D, it checks in the routing table whether the way to the terminus node D is already obtainable. If there is no other route to the destination, then the node S broadcasts an RREQ packet to the neighboring nodes. When an RREQ packet attains at a middle node, RREQ is scanned, and if the destination address of the RREQ is same as the address of the intermediate node, then the intermediate node will send the RREP otherwise it rebroadcasts the RREQ.

Algorithm

```
begin
initialize source, destination.
assigns– source, i- intermediate node, d-destination, α-
small step value
compute the interruption time for all the node in the
network
dt = (α · old_dt) + ((1 − α) · new_dt)
route discover(data packet)
begin
if (s) then lookup route table (dest_id)
{
if(route_not_found) then add route entry(destination_id)
{
dest_seq_no= undefined;
seq _ no= seq _no +2;
}
endif
}
else
{
bcast_id = bcast_id +1;
transmission_rreq(source_id:seq_no:0,00.endpoint_id:d
est_id,dest_seq_no:
dest_seq_no,advertised hop count:0)
}
endif
if (i is not( d)) then  {rebroadcast rreq}
else
{
d return rrep
d unicasts rrep
forward the rrep
}
endif
if (rrep reaches s) then
{
if (rrep time < the delay time )then
ignore rrep
}
else
{
the route is established between s and d
}
endif
store the alternate routes
end;
```

The destination node that receives the RREQ wills unicast the RREP packet to the source. Any malicious node may reply fast to

the request from the source by claiming to have the shortest path to the destination. Once the RREP is received, the source node checks whether the RREP has arrived within the delay time. If the RREP has arrived too earlier than the delay time, then the source node assumes that node as the malicious node and simply ignores the concerned RREP. If the RREP from the nodes is valid, then all the nodes on the routes enter into the authentication phase. All the separate routes are stored in the changing table. Thestored routes in the routing table are sorted based on the shortest communication cost. The route with the shortest communication cost is established as the selected route.

3.2. Authentication Process

To prevent the Sybil nodes from dropping the packets, the selected route is not used for the data transmission immediately. After the route discovery process, the nodes arrive into the authentication phase for being authenticated by the neighboring nodes in the path. All the nodes in the selected route try to validate its neighbors by issuing the digital security certificates. To generate the digital security certificate, secured public key of the node should be created. The nodes request the IP address of its neighbor, and it generates the obtained public key by applying the hash function.

$$HMACpK(M) = h((K + spad) \| h((K + epad) \| M)) \quad (3.1)$$

Where HMACpk(M) is the hash function of the message M and the message is the IP address of the node. h( ) is the underlying hash function, spad and epad are the starting and ending padding sequence. K is the underground key. HMAC delivers the secured public key which cannot be attacked by the intruders

The digital security certificate is a self-organized PKI certification where the public key is authenticated by the chain of nodes. A node in the network can requestproblem certificate to each other node within the radio statement range of each other. Every node in the network would be able to authenticate the other nodes in the network, by generating and issuing the certificates to the neighbors. The node also maintains the certificates received from the other neighbors. The certificates are delivered based on security trust value. The nodes make a periodical request for the certificates from the neighbors. The digital certificates are validated based on the public key which is one of its components. The digital certificate contains the following components.

[IP- ADDRESS, PK, TV, ET] KEY OF THE ISSUE NODE (3.2)

For example, the certificate issued by source S to an intermediate node I is given in the following form.

$$DSC(S \rightarrow I) = [IP, keyI, TV, ET] \text{ key } S \quad (3.3)$$

PK is the public key of the destination node. TV is the Trust Value of the node then ET is the Expiration Time of the certificate. Before generating a certificate the issuer node checks whether the TV value is feasible. If it is feasible, the public key is generated, and the certificate is delivered to the receiving node, and a copy of the similar is deposited in the routing table of the issuer. TV is designed based on the time taken to procedure the RREQ packet and the position of the node. The malicious node which obtains the RREQ will proximately process the RREQ by distribution the RREP straight without confirming the route table for the obtainability of the node‘s routing information. When the source node receives the RREP too earlier than the expected time, it suspects the RREP initiator to be the sybil node, and it ignores the route with the sybil node and selects the alternate route. The certificates exchanged periodically between the neighboring intermediate nodes are as follows.

$$DSC(S \rightarrow A)DSC(A \rightarrow B)DSC(B \rightarrow D) \quad (3.4)$$

Here A and B are the intermediate nodes, S and D are the sources and destination nodes respectively. The source waits for the authentic reply from the end node. The target node sends the authenticated message appended with the digital security certificate that is issued by the neighboring node in the network. The legitimate RREP packet from the endnode would be in the given form.

[Source ID, NextHopID, FinalDest ID,DSC] (3.5)

The RREP packet since D would be [D, B, S, DSC ($B \rightarrow D$)].When this packet reaches the node B, it checks its routing cache to verify whether DSC ($B \rightarrow D$) is available. It checks whether D is the sybil node by verifying the list of certificates issued by B. If D is the promiscuous node, then it forwards the RREP packet to A by appending its certificate. The procedure is continued by all the intermediate nodes on the route until the RREP reaches the source node. B forwards the RREP to the intermediate node to A. Finally, RREP that reaches S from A will be in the form as follows.

$$[D, B, A, S, DSC(B \rightarrow D), DSC(A \rightarrow B), DSC(S \rightarrow A)] \quad (3.6)$$

When the RREP reaches S, it checks the whole certificate group. If there are no issues in the certificate, node S trusts that the route is secured and starts sending the packets through the route and the trust value of the intermediate nodes on the route is incremented. If any issues are found then the trust value of the node is decremented, and the route is announced as the malicious route. The following Algorithm 3.2 explains the node authentication process of SAOMDV protocol scheme.

Algorithm

BEGIN
Nodes forming the route certify each other
{
Request ID and security parameters of Intermediate nodes
Generate public key of Intermediate nodes based on ID
Issue Certificates encrypted with public key
Store Certificates in route cache 8. Exchange Certificates with neighbor nodes
}
D sends certified RREP appended with Digital Security Certificate from Intermediate nodes. Assign TV = 1
For I = N to 1
{
IF is Available(DSC(D)) in I THEN
{
IF(I DSC(D)) = DSC(D) THEN
Attach their certificates and advancing the certified RREP
ELSE
Revoke the DSC from the Node
}
RREP reaches S
S verifies certificate chain of the route unicasted by D.
IF is VALID(Certificate Chain) THEN send the Data Packets through the Route.
TV = TV+1
Else
2Broadcast the route as a maliciousroute to all the other nodes in the network.
2Stop forwarding data packets.
Select the alternative route from Route Cache.
END;

Once the route is recognized between the source and the destination, the nodes starting the path enter into a verification phase. The source node requirements the individuality of the next hop node and generates a public key based on its status. The time is taken to procedure the RREQ packet and the position of the node are the ideal limitations to control the security level of the node on Sybil attack. The security parameters of the next hop node are requested, and safety certificates are distributed if the issuer is committed about the security parameters. The malicious

node which receives the RREQ replies by sending the RREP immediately without any time delay. In this case, the source node sets thesmallest time delay to obtain the RREP. If it receives the RREP in advance, then the source suspects the RREP initiator to be Sybil node and initiates the sybil node detection and removal process.

3.3. Sybil Attack Node Detection Process

Node Detection Process If any of the digital security certificates is found to be mismatching, which means that if two different nodes hold the digital security certificate with the same public key or two different digital security certificates is assigned to the same node, then the corresponding node is assumed to be a sybil node. The route including the sybil node is ignored. The alternate route is selected from the routing table. The source ignores the alternative paths if it includes the malicious node which is traced in a previous way.
The Algorithm 3.3 explains the alternate path selection approach in the Sybil node detection and removal process for the secured data transmission in MANET.
The 59 source node implements this algorithm to select the alternate route when the route chosen for the transmission is attacked by the malicious nodes.
To prevent a legitimate node turning malicious over a period, the node's behavior would be recorded, and if the behavior of the node is found to be unsatisfactory, then the certificate would not be renewed after its expiry time.
Therefore the node is isolated from further participation in the network activities. Since the security levels of participating nodes are updated based on their faithful participation in the network, any sybil node among the source and destination can be very well remote from the network as these nodes would not be able to provide the certificates to be appended to the RREP message.

Algorithm

BEGIN
Let S is anestablished of S-1 Alternate paths
Let p1,p2,p3,……p(s-1) be the alternative routes that are stored in two-dimensional array S.
Let N=set of paths that are node- separatethen free from malicious links.
Initialize N= 0.
Let Pm be the path through the malicious node.
For k=1 to S-1 do
{
Select Pk from S and Check whether it includes the malicious link.
If (Pk ∩ Pm =0)
then add Pk to N
}
If N=0 then
Goto Route Discover(data _packet)
Else
Route particular = Pk // Pk is the shortest path through no malicious link.
END

Computes the multiple loop free paths during the route discovery process and all the disjoint routes are stored in the routing table. With the obtainability of the multiple paths, the protocol changes from one route to the next conceivable best route when the other route fails. The new route discovery process is initiated only when all the paths to a particular destination fails. The loop-free link disjoint paths and multipath routing are very efficient in reducing the routing overheads and supporting in better load balance. A switch to the another route will avoid the node congestion. This factor reduces the expenses to perform a new route discovery at each time when a route in use breaks.

4. Result and Discussion

The proposed scheme to detect and prevent the Sybil attack in MANET are simulated using NS2.34 simulator. This work assumes the network model to be asynchronous, where there is no reliability for the delivery of the message to the proper destination. The four types of mobile nodes defined in the network are source node(S), destination node (D), intermediate nodes (I, A, B, C) and the malicious node (M).
The source node S generates the traffic and sends it to the destination node D.

Table 4.1: Simulation Settings and Parameters

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

One or more in-between nodes are associatedwith each other to form a route between the source node and the destination node, and it is used to forward the traffic from S to D. At the destination node, the traffic sent by the node of origin is received and the packet distribution ratio is measured at this node.

Table 4.2: Evaluation of PDR by Varying the Number of Nodes

No of nodes	*RANDOM HASHING*	*DSC*
20	75.7498	93.2562
40	73.6424	90.2872
60	71.2120	85.4948
80	70.8115	87.1355
100	69.8105	81.5650

Table 4.2 illustrates the analysis of evaluation of the PDR results by changing the number of nodes.

Table 4.3: Performance Evaluation of Attack detection by Altering Speed

Techniques	Speed variation at Nodes(m/s)	PDR (%)	NLT (pkts)	Throughput (%)
RANDOM HASHING	20	75.7490	0.0038	0.0000
	40	73.6420	0.0051	0.0000
	60	71.2120	0.0063	0.0000
	80	70.8110	0.0077	0.0000
	100	69.8100	0.0087	0.0000
DSC	20	82.2560	0.0031	53.3000
	40	79.2870	0.0038	49.9300
	60	77.4940	0.0053	42.6500
	80	75.1350	0.0067	37.7600
	100	73.5650	0.0075	11.5000

Table 4.3 shows the comparative analysis of the performance evaluation of attack detection, based on the above-mentioned parameters by varying the speed.

4.1. Metrics for Performance Evaluation

The results of the simulation are evaluated based on the various metrics like Packet delivery ratio, Average throughput, an Average end to end delay time and Network lifetime.
Packet Delivery Ratio (PDR) is the ratio of the packets received to the packets sent effectively. This metric specifies both the loss ratio of the routing protocol and the effort necessary to collect the data. In an ideal scenario, the rate should be equal to 1. If the rate falls significantly below a perfect ratio, then it could be a suggestion of some faults in the protocol enterprise. However, if the ratio is developed than the ideal ratio, then it is an indication that the destination node receives a data packet more than once. It is not desirable because the reception of the same packets

consumes the network‘s important resources. The relative number of replacements received by the destination node is also important to take an appropriate action to reduce the redundancy.

PDR=(no of packets delivered/ no of packets transmission)*100

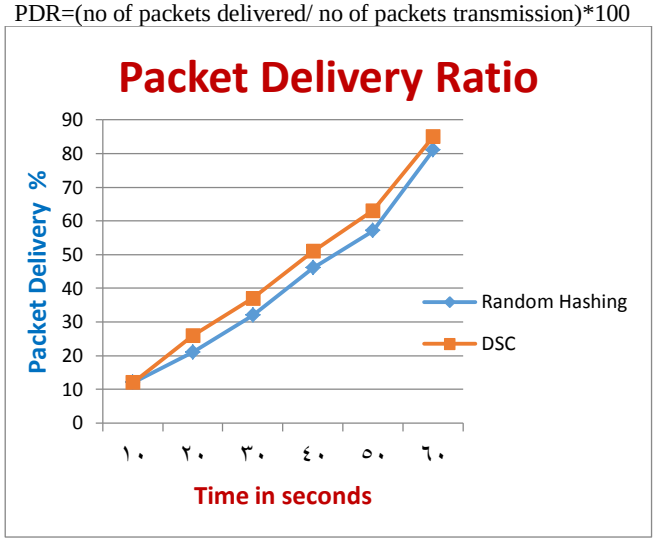

Figure 4.1: Performance of delivery ratio

Average Throughput is the average rate of successful data delivery measured at the destination node (bytes) divided by the simulation duration time (sec).It processes the elapsed time between the time that the source node started sending an RREQ and the time the destination node receives the last data packet.[21]

Average ThroughPut= (Total Amount of Data Received at Destination/ Time(sec s))*100

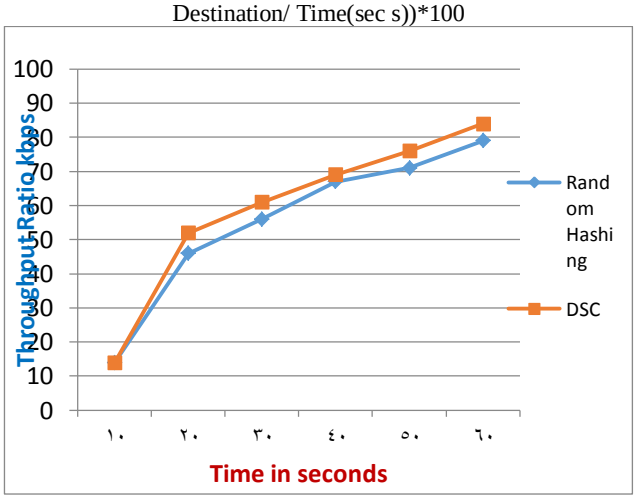

Figure 4.2: Performance of throughput ratio

Network Life Time (NLT) is the time of the first node rectifying due to the energy of battery power charge during the imitation with anexact routing procedure. The network lifetime decreases as the offered traffic load increases.

NLT = (process Time- Node Failure Time/Time)

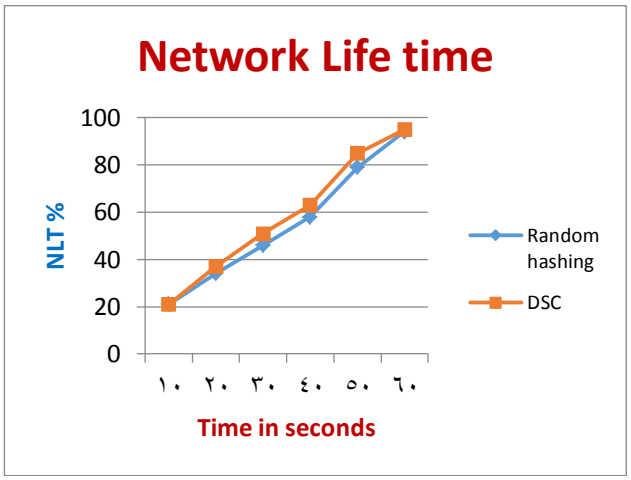

Figure 4.3: Performance of network life time

Table 4.4: Performance Evaluation of attack detection by varying Node Mobility

Protocol	No of Nodes	PDR (%)	Throughput (kb/s)	NLT (secs)
RANDOM HASHING	10	65.7400	1893.7400	345.2000
	30	63.6400	1841.0600	233.7000
	50	61.2100	1780.3000	127.2000
	70	60.8100	1770.2900	97.3000
	90	59.7800	1745.2600	70.2000
DSC	10	87.2560	1993.7400	352.8000
	30	84.2800	1941.0600	241.7000
	50	81.1300	1880.3000	132.8000
	70	79.4900	1870.2900	107.4000
	90	75.5600	1820.2600	107.4000

Table 4.4 illustrates the performance assessment results of Sybil attack detection by varying the node mobility. When the mobility of the nodes increases the throughput decreases because most of the packet will get dropped. In the case of proposed scheme, most of the missing packets are retransmitted again over multiple reliable routes from source or intermediate node to the destination.[22]

5. Conclusion

The most common security threat experienced by the MANET is the Sybil attack. The sybil node severely affects the performance of the network layer and results in denial of service. The attack detection experiences severe unwanted impact on the performance due to the Sybilattack. To avoid the adverse 75 effect of the sybil attack nodes on the network, The simulation results prove that our proposed scheme provides efficient packet delivery ratio. Also, it will detect the Sybil node during the route discovery process and ensures that any sybil node cannot be a participating node in the route to transmit the data packets from the source to destination. During the data transmission, any legitimate node can tend to behave maliciously.

References

[1] Alimohammadi M & Pouyan AA, “Sybil attack detection using a low cost short group signature in VANET”, *IEEE 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, (2015), pp.23-28.

[2] Bhumkar R & Pete DJ, “Reduction of error rate in Sybil attack detection for MANET”, *IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, (2015), pp.1-6.

[3] Gu P, Khatoun R, Begriche Y & Serhrouchni A, “Vehicle driving pattern based sybil attack detection”, *High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science*

and Systems (HPCC/SmartCity/DSS), IEEE 18th International Conference on, (2016), pp.1282-1288.

[4] John R, Cherian JP & Kizhakkethottam JJ, "A survey of techniques to prevent sybil attacks", *IEEE International Conference on Soft-Computing and Networks Security (ICSNS)*, (2015), pp.1-6.

[5] Kumar PV & Maheshwari M, "Prevention of Sybil attack and priority batch verification in VANETs", *IEEE International Conference on Information Communication and Embedded Systems (ICICES)*, (2014), pp.1-5.

[6] Lakhanpal R & Sharma S, "Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique", *IEEE International Conference on Computation of Power, Energy Information and Communication (ICCPEIC)*, (2016), pp.283-287.

[7] Li P & Lu R, "A sybil attack detection scheme for privacy-preserving mobile social networks", *IEEE 10th International Conference on Information, Communications and Signal Processing (ICICS)*, (2015), pp. 1-5.

[8] Liu R & Wang Y, "A new sybil attack detection for wireless body sensor network", *IEEE Tenth International Conference on Computational Intelligence and Security (CIS)*, (2014), pp.367-370.

[9] Mekliche K & Moussaoui S, "L-P2DSA: Location-based privacy-preserving detection of Sybil attacks", *IEEE 11th International Symposium on Programming and Systems (ISPS)*, (2013), pp.187-192.

[10] Mulla M and Sambare, S, "Efficient analysis of lightweight Sybil attack detection scheme in Mobile Ad hoc Networks", *IEEE International Conference on Pervasive Computing (ICPC)*, (2015), pp.1-6.

[11] Rashidibajgan S, "A trust structure for detection of sybil attacks in opportunistic networks", *IEEE 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, (2016), pp.347-351.

[12] Samuel SJ & Dhivya B, "An efficient technique to detect and prevent Sybil attacks in social network applications", *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, (2015), 1-3.

[13] Sharma H & Garg R, "Enhanced lightweight sybil attack detection technique", *IEEE 5th International Conference on the Next Generation Information Technology Summit (Confluence)*, (2014), pp.476-481.

[14] Sharma AK, Saroj SK, Chauhan SK & Saini SK, "Sybil attack prevention and detection in vehicular ad hoc network", *IEEE International Conference on Computing, Communication and Automation (ICCCA)*, (2016), pp.594-599.

[15] Shrestha R, Djuraev S & Nam SY, "Sybil attack detection in vehicular network based on received signal strength", *IEEE International Conference on Connected Vehicles and Expo (ICCVE)*, (2014), pp.745-746.

[16] Tian B, Yao Y, Shi L, Shao S, Liu Z & Xu C, "A novel Sybil attack detection scheme for wireless sensor network", *IEEE 5th IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT)*, (2013), pp.294-297.

[17] Triki B, Rekhis S, Chammem M & Boudriga, N, "A privacy preserving solution for the protection against sybil attacks in vehicular ad hoc networks", *IEEE 6th Joint IFIP Conference on Wireless and Mobile Networking (WMNC)*,(2013), pp.1-8.

[18] Triki B, Rekhis S & Boudriga N, "An RFID based system for the detection of Sybil attack in military wireless sensor networks", IEEE *World Congress on Computer Applications and Information Systems (WCCAIS)*, (2014), pp.1-2.

[19] Valarmathi ML, Meenakowshalya A & Bharathi A, "Robust Sybil attack detection mechanism for Social Networks-a survey", *IEEE 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, (2016), pp.1-5.

[20] Vamsi PR & Kant K, "A lightweight sybil attack detection framework for wireless sensor networks", *IEEE Seventh International conference on Contemporary computing (IC3)*, (2014), pp.387-393.

[21] G, Abikhanova, A Ahmetbekova, E Bayat, A Donbaeva, G Burkitbay (2018). International motifs and plots in the Kazakh epics in China (on the materials of the Kazakh epics in China), Opción, Año 33, No. 85. 20-43.

[22] A Mukanbetkaliyev, S Amandykova, Y Zhambayev, Z Duskaziyeva, A Alimbetova (2018). The aspects of legal regulation on staffing of procuratorial authorities of the Russian Federation and the Republic of Kazakhstan Opción, Año 33. 187-216.