International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Securing AODV for Defending Sybil Attack in MANET

Ankit Gupta[1], Deepak Sukheja[2], Amrita Tiwari[3]

[1]Oriental University, M.Tech (CN), Indore (M.P), India
[2]Oriental University, Department of Computer Science and Engineering, Indore (M.P), India
[3]Oriental University, Department of Computer Science and Engineering, Indore (M.P), India

Abstract: ***Security is of paramount concern in any ad-hoc network. In Mobile Ad-hoc networks (MANETs), mobility of the nodes poses a problem for providing security services. The ad-hoc network is more vulnerable to attacks, since it uses wireless communication link between the mobile nodes. Sybil Attack is a spoofing attack, where a malicious node illegitimately creates multiple fake identities (called the Sybil nodes) to impersonate as normal nodes. It is observed that most of the existing protocols fail to defend against Sybil attack. The existing static & dynamic routing protocols like ADOV, DSR, OLSR needs to be updated for providing better security against the issues. This work focus to improve the security issues in AODV routing protocol to detect and prevent Sybil attack.***

Keywords: MANET, AODV, Sybil Attack, Node

1. Introduction

In recent years, in the field of wireless communication and networking considerable advancements have been experienced. MANETs have become very popular. Ad hoc is derived from Latin, meaning “for this purpose” meaning temporary. “Mobile Ad hoc Networks” as the name reflects is a temporary deployed mobile wireless network. MANET is a multi-hop, temporary, self-organizing system made up of a group of portable electronic equipment with wireless transmitter and Receiver. This collection of mobile nodes may operate in isolation, or may have gateways to interface with a fixed network. An ad-hoc network uses no centralized administration.This work aims towards designing and implementing an efficient security solution for mobile ad hoc networks against Sybil attacks. The proposed secure routing protocol is based on AODV. The objective of this work is to provide higher security against these attacks with minimum overhead and acceptable delay. It is also desirable to evaluate the performance of modified routing protocol on the basis of different performance metrics through the simulation results and compare the results of modified protocol and existing protocol under these attacks. This simulation work is done by using network simulator-2.

2. Related Study

In the paper [1], author proposed neighbor discover distance algorithm used to detect the Sybil attracters. In MANET each and every nodes consists of a neighbors data address. The neighbor’s data address transfer to destination without any packet loss. Near duplication detection algorithm is more security and efficient data transmission on their network.

Proposed NDD algorithm is a RSA algorithm based node verification and authentication method.NDD algorithm based to find detection and prevention Sybil attack and secure and avoid the attacking system on the network.

In the paper [2], author proposed cross-layer scheme for detecting large-scale colluding Sybil attack. In this proposed technique used RSU road side units for position verification, distance verification and for location verification. The RSUs listen passively to all beacons sent from all vehicles in its communication range. If an RSU suspects that there is a Sybil attack, it verifies the suspected vehicle’s location as follows. The RSU composes a challenge packet at the MAC layer and directs the physical layer to send it to the vehicle’s claimed location. This can be done by beam forming which is a physical layer technique that can concentrate the radio transmission at a small area. It used speed and position location to verify identity mobility and false rate and detection rate probability as metrics.

In the paper [3], author proposed mitigating zero-day Sybil vulnerability in privacy-preserving vehicular peer-to-peer networks an efficient local Sybil resistance scheme, called LSR, to locally detect Sybil attack. Especially, in the proposed LSR scheme, if a vehicle never signs an event more than once, the signatures it signed cannot be linked, and its privacy can be well protected. However, if a vehicle signs two or more signatures on the same event, any vehicle can easily link these signatures and thus detect a Sybil attack locally. Moreover, with two-layer/multi-layer reporting, a Sybil attack can be quickly reported to a trusted authority (TA) for tracking the Sybil attacker's real identity and making global revocation.

Detailed security analysis demonstrates that the Proposed LSR scheme can enhance the security of a privacy-preserving VPNET, such as locally detecting Sybil attack, preventing a Sybil attacker's future attacks before its being revoked by TA, et al. In addition, performance evaluation via extensive simulations also confirms the high effectiveness of the proposed LSR scheme.

In the paper [4], author proposed security mechanisms for sensor network. They consider Sybil attack as crucial problem and deploy malicious node by converting legal node into Sybil node having various replica IDs. Sybil node leads to data leakage lead to compromise data integrity violation. In the proposed solution, malicious node can be checked by validating neighbour verification. Neighbour node exchange information with each other and try to highlight the node communicating misleading information. To detect and prevent Sybil attack they use Random Password Comparison [RPC] method. Which proposed that facilitates deployment and control of the position of node thereby preventing the Sybil attack. The RPC method is dynamic and accurate in detecting the Sybil.

In the paper [5], author used RSSI based technique to detect Sybil node in network, each node identified in network with energy level, radio signal strength and ID's. This value associate with routing table and each node identified with this values. If similarity between parameters is observed than node is consider as malicious Sybil node.

In the paper [6], author approach protects routing from Sybil attack. A node with highest id selected as super node or cluster head. All traffic should be transit through super node (snode).this node maintain topology table and routing table of network. Each route lookup request sends to snode and snode replay with route path.

In the paper [7], author proposed key distribution approach in followed in this approach. It create secure communication channel between nodes. Random key set is assigned to nodes and common key used to establish channel for communication. A set of key k assigned form key pool p and node can only communicate if they exchange shared key.

In the paper [8], author proposed method introduced trusted centralized authority in network. The authority is used to assign identity and credentials in network and one to one mapping between node and its identity. Assigned .credential use by trusted authority are cryptograph keys, digital certificate, computed checksum or hash value to verify and validate node identity.

Certificate Authority - peer to peer network a central authority used to assign, trusted credentials to node in network such as digital certificate or validation certificate. It is similar as SSL certification assignment by CA and cryptography solution using public key infrastructure for authentication and validity of node. a trusted node have public key of all nodes in network and send public key encrypted message for verification of nodes when node received message it decrypted it and send reply back message encrypted with private key to trusted node or trusted system approach, in this approach used a single (p2p) or group (distributed network) of administrative node in network to monitor, analysis, detection of abnormal communication pattern .if the detect threat they block node and remove from routing table of nodes in network. This approach is similar to Intrusion detection system (IDS).

In the paper [9], author proposed special type adhoc network sensor network node are located at fixed location. In sensor network a topology map is created and stored in each node. When some node failed sensor node look for other route. If node found in more than one route so it may be a Sybil node. This approach is truly based upon assumption and it is very costly in resource consumption.

3. Sybil Attack

Sybil attack is kind of attack in which malicious node carries fake identities of existing or non-existing legitimate node to control a part of network. A Sybil attack may apply due to poor authentication on network layer .it is an attack which creates repudiation of large fake identities a single physical node to gain disproportional large influence .this attack aims to degrade network services or availability of resources when co-operation is required. The Sybil attack occurs in network when it runs without central authority.

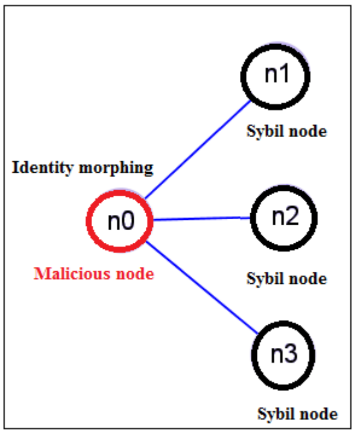

Figure 3.1: Sybil attack

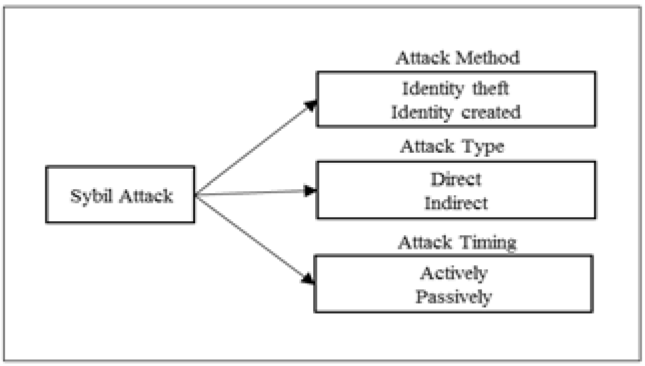

Figure 3.2: Sybil Attack Taxonomy

Sybil attack is an approach in which a malicious node illegitimately fakes multiple identities by compromised node or clamming same from external source Sybil attack is also capable of disturbing routing mechanism in MANET multipath routing and secure routing may affected by this attack. In multipath routing fake identities may be the part of one or various routes in different position. To compromise communication and degrade network performance.

4. Proposed Technique

This research work proposes an efficient technique to detect and prevent Sybil attack without the need for special hardware or strict location or synchronization requirements. The proposed technique makes use of variance in routing information between neighbours to detect Sybil attack. The detection technique uses an approach based on identity verification formally known as ID verification. The Sybil affected routes are distinguished from legitimate routes by analysing ID value of all neighbours. Basic idea of the technique is to discover alternative routes to the destination. These alternative routes will be dissimilar in length. The idea behind this approach is illustrated below.

4.1 Deployment of Sybil Attack in MANET

The objective of this phase is to create malicious environment of Sybil node to observe the impact of Sybil attack in

MANET. Here, a Sybil node is deploy at time of network deployment. Afterwards, it starts participating into network activity and attempt to collect IDs of neighbour nodes. Sybil attack may be deploying into two ways either through fresh identity or through existing identity. work uses the existing node identity to create multiple ID replicas. In this ways, Sybil node collect neighbour node IDs in routing table. When source broadcast RREQ packet to discover route from source to detonation, it uses fake IDs to misguide source about shortest route towards destination. Thus source register Sybil node into routing table and start communication through malicious node.

4.2 Implementation of Sybil Node Detection

This phase comprises the detection technique of malicious node using intrusion detection system. AODV protocol has been modified and monitoring methods are deploying to listen and validate fake node id. As per traditional process source will broadcast the RREQ packet to discover shortest route towards destination and register Sybil node into routing table. But in case of detection, it will rebroadcast packet to multiple routes and attempt to collect information of all neighbour nodes. Because Sybil node always uses multiple id for communication, it will have multiple id for same neighbour. Source will compare the id details with stored path and if it found different it consider it as malicious node. In simple words, detection system collect neighbour node information hop count and compare this result with existing routing table. if it found any entry in existing table missing from recently collected neighbour node information, it consider that node as malicious node and forward this detail to SAODV.

4.3 Development of SAODV to prevent Sybil nodes

This phase is to detect and prevent Sybil attacks in AODV routing protocol which has been done in the proposed technique based on identity verification approach. The basic idea behind the proposed technique is to integrate Intrusion detection scheme and SAODV algorithm to detect and prevent Sybil attack. Here, detection approach detect malicious node by cross examine identity verification and forward malicious node ID to SAODV. This process deletes malicious node entry from source routing table and blacklists the malicious node at source node. Next time, when source attempt to forward packet towards destination, it verify node information from blacklist and bypass the malicious route.

```
BEGIN:
Setting Parameters -
Set Channel – Wireless
Set Link – Mac/802_11
Set Traffic Pattern – CBR
Set Transport Agent – UDP
Set Nodes - 100, 300, 500
Set Duration – 500 Sec
Sybil Node Deployment -
Broadcast RREQ to all neighbours
Receive Acknowledgement
Update Routing table with multiple fabricated IDs
Mechanism to detect Sybil node Intrusion -
Broadcast RREQ to All Neighbours, Wait for Reply Acknowledgement
If pdr is < threshold value, check for intrusion;
If (Rtable ID = = Received ID)
rtable.hopcount == rep.hopcount;
Validate TTL Value;
Source REP ACK == True && TTL== Fixed;
Revert RREP & ACK;
Else
Set ACK==False;
Forward malicious node id to SADOV; BroadcastRREQ;
Secure AODV to prevent genuine node from malicious Sybil node -
If (Intermediate node == malicious node)
ACK == False
Bypass malicious route, Delete malicious node entry at source note routing table
Search alternate path
Else
Forward packet to next node;
END
```

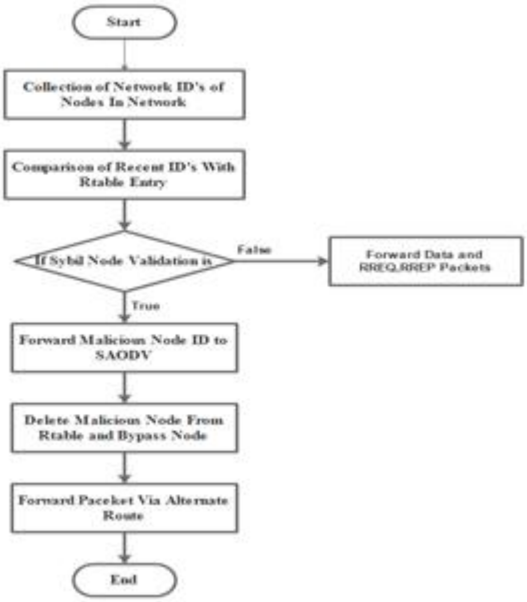
Start
Collection of Network ID's of Nodes In Network
Comparison of Recent ID's With Rtable Entry
If Sybil Node Validation is
False
Forward Data and RREQ,RREP Packets
True
Forward Malicious Node ID to SAODV
Delete Malicious Node From Rtable and Bypass Node
Forward Pacekt Via Alternate Route
End

Figure 4.1: Flow Chart of Proposed Algorithm

4.2 Implementation Steps

The work starts with studying the theoretical and practical concept of the AODV routing protocol.

1. AODV routing protocol is then implemented in ns2 on different scenarios have 100 nodes, 300 nodes and 500 nodes in network.
2. Performance evaluation of AODV protocol under different scenarios is done on basis of Throughput, Packet Delivery Ratio and Packet Drop Ratio.
3. Theoretical aspects of security issues and their impacts on ado network are studied.
4. Simulation of network AODV routing protocol with Sybil Attack is done to analyse the impact of malicious node on performance metrics.
5. Analyse the impact Sybil Attack on various performance metrics for AODV.
6. Implement the proposed detection technique in AODV for detection of Sybil Attack.
7. Analyse the performance metrics for modified AODV using detection technique to detect Sybil attack.
8. Implement the proposed Secure-AODV technique in AODV for prevention of Sybil Attack.

9. Analyse the performance metrics for modified SAODV using to prevent Sybil attack.
10. Compare the performance parameters for AODV under Sybil Attack, IDS AODV and SAODV for 100 nodes, 300 nodes and 500 nodes Scenario

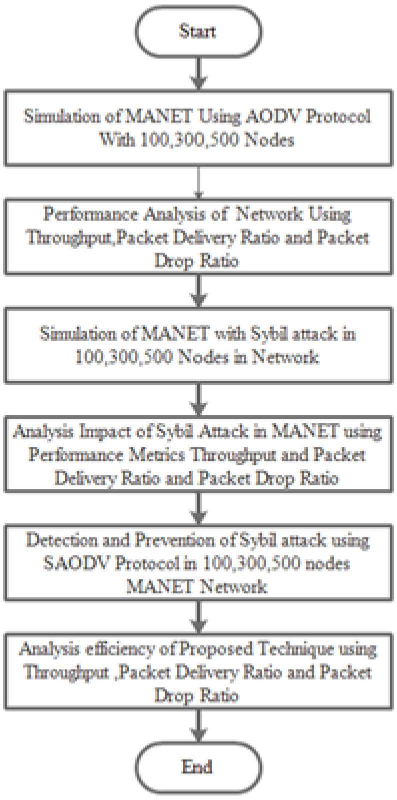
Start
Simulation of MANET Using AODV Protocol With 100,300,500 Nodes
Performance Analysis of Network Using Throughput,Packet Delivery Ratio and Packet Drop Ratio
Simulation of MANET with Sybil attack in 100,300,500 Nodes in Network
Analysis Impact of Sybil Attack in MANET using Performance Metrics Throughput and Packet Delivery Ratio and Packet Drop Ratio
Detection and Prevention of Sybil attack using SAODV Protocol in 100,300,500 nodes MANET Network
Analysis efficiency of Proposed Technique using Throughput ,Packet Delivery Ratio and Packet Drop Ratio
End

Figure 4.2: Flow Chart of Implementation

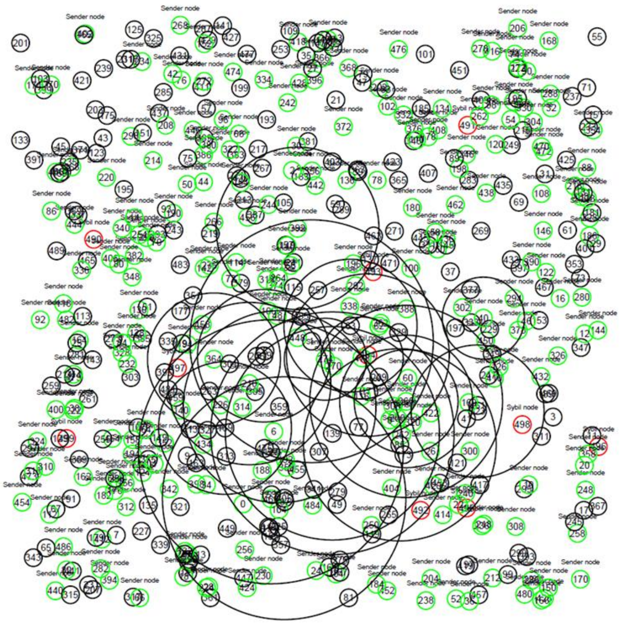

Figure 4.3: Simulation Scenario with 500 nodes in MANET

5. Result Observation

The simulation of the work completed in three scenarios. The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all nodes in each scenario are normal and no malicious node is present in the scenario. The standard AODV routing algorithm is used at routing protocol on network layer. The scenarios are differentiated as per normal scenario, scenario with Sybil nodes and scenario with proposed technique. Impact of performance variation is observed in 100 nodes, 300 nodes and 500 nodes.

Scenario 1: It describes the normal situation of mobile ad-hoc networks with normal AODV routing protocols.
Scenario 2: It described impact of Sybil Attack and impact of Sybil attack on performance of ad-hoc networks.
Scenario 3: it implements the proposed technique to detect and prevent Sybil attack in mobile ad-hoc networks.

Figure 5.1 & 5.2 demonstrates the evaluated performance of normal AODV, AODV with Sybil attack and modified AODV with improved performance. The network performance metric is throughput and packet delivery ratio.

Throughput = Total received packets / Total simulation time …Equation (1)

Packet Delivery Ratio = (packets received/packets sent) ...Equation (2)

Throughput Graph

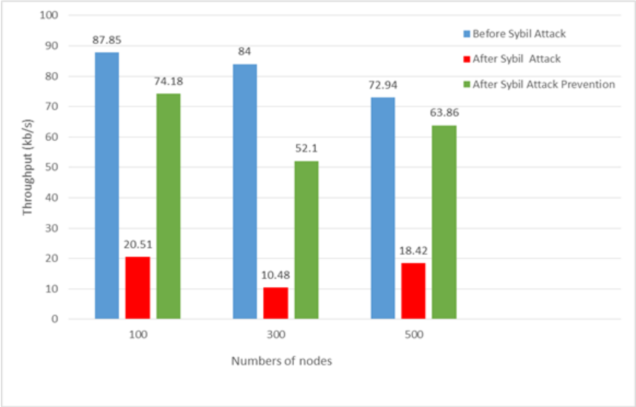

Figure 5.1: Comparison of Throughput in 100, 300, 500 Node Network with Different Scenario

Packet Delivery Ratio Graph

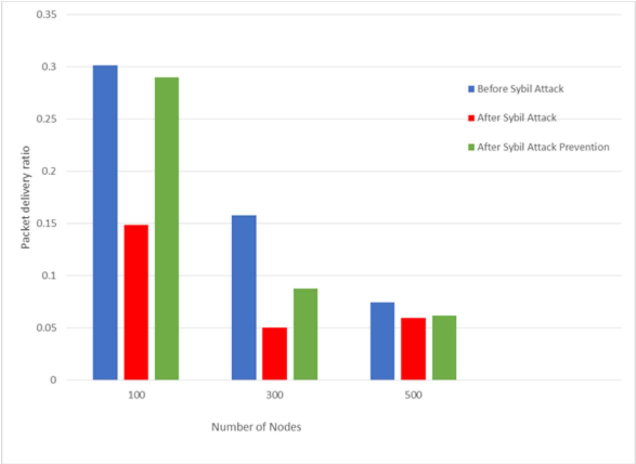

Figure 5.2: Comparison of PDR in 100, 300, 500 Node Network with Different Scenario

Description - Result show in graph describe that before Sybil attack throughput and packet delivery ratio is high and after

Sybil attack, it decrease and after prevention values are restored with some difference due to routing path change and routing packet delivery .In 300, 500 nodes network throughput in 500 nodes network have high throughput after prevention of Sybil attack because of new routing path and low routing overhead.

6. Conclusions

This work proposed SAODV based technique to detect and prevent Sybil attack. To evaluate the performance of proposed techniques, simulation of Sybil attack has been performed. Neighbor node id based Sybil attack deployment has been used. The performance of this approach improves nodes. According to simulation results the proposed techniques show superior performance as Packet delivery ratio and throughput increases. In the analyzed scenario, it is found that the modified Secure AODV has superior performance than AODV. Modified Secure AODV is suitable to detect and prevent Sybil attack. It improves the PDR under attack conditions, with acceptable decrease in throughput due to routing path change and new route.

References

[1] R. Bhuvaneswari, N. Balamalathy, S. Premalatha “An Improved Performance, Discovery and Interruption of Sybil Attack in MANET”, Middle-East Journal of Scientific Research ISSN: 1990-9233 Vol. 23 No. 7, Page No. 1346-1352, Year 2015.

[2] K. Rabieh, M. Mahmoud, T. Guo, M. Younis "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs", Conference: IEEE International Conference on Communications (ICC), London, UK, Pages 1-11 Year 2015.

[3] Lin, Xiaodong “LSR: Mitigating Zero-Day Sybil Vulnerability in Privacy-Preserving Vehicular Peer-to-Peer Networks” IEEE Journal on Selected Areas in Communications, Volume:31, Issue: 9 Page(s):237 – 246 ISSN :0733-8716 September 2013

[4] R. Amuthavalli, DR. R. S. Bhuvaneswaran “Detection And Prevention Of Sybil Attack In Wireless Network Employing Random Password Comparison Method” Journal of Theoretical and Applied Information Technology ISSN: 1992-86 Vol. 67 No.1 Page 236-246 Year 2014

[5] J. Newsome, E. Shi, D. Song, and A. Perrig “The Sybil attack in networks analysis & defences”, the 3rd International Symposium On Information Processing In Sensor Networks Pages 259-268 ISBN:1-58113-846-6 Year 2004

[6] Priyanka Sharma, Dr. Kamal Sharma, Surjeet Dalal “Preventing Sybil Attack In MANET Using Super Node Using Approach” International Journal of Recent Research Aspects, ISSN: 2349-7688, Vol. 1, Issue 2 pp. 25-30Sept. 2014

[7] Chunling Cheng “An Approach Based on Chain Key Predistribution against Sybil Attack in Wireless Sensor Network” International Journal of Distributed Sensor Networks Vol. 2013 (2013), Article ID 839320, Page(s) 1-8 July 2013

[8] Yue Liu “A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities” IEEE Transactions on Mobile Computing ISSN 1536-1233 Issue 99 Feb 2015

[9] Debapriyay Mukhopadhyay, Indranil Saha “Location Verification Based Defense Against Sybil Attack In Sensor Networks” 8th International Conference on Distributed Computing and Networking Pages 509-521 2006 Online ISBN 978-3-540-68140-3

[10] John R. Douceur “The Sybil Attack “International workshop on Peer-To-Peer Systems” Pages 251-260 ISBN:3-540-44179-4Year 2002