Preserving against Sybil Attack in Mobile Ad Hoc Network Using SYDECT Algorithm

[1]Bindu Chaurasiya,[2]Mohit Shrivastav,[3]Devendra Kumar
[1]M.Tech. Scholar,[2]Assistant Professor,[3]M.Tech.
[1]CSE Department,
[1]School of Engg. & IT, MATS University, Gullu-Aarang Campus,Raipur (C.G.), India

***Abstract* - MANET is a kind of wireless network which is decentralized in nature and comprise of moving mobile nodes. Due to changing topology of such network it impose critical security protocol design against harmful attacks such as Sybil Attack. In a Sybil attack a malicious node can produce and manage a large number of logical identities on a single physical device. This gives the misapprehension to the network as if it were different rightful nodes. Sybil attacker node's additional identities are known as Sybil nodes. In this research work, a novel method is proposed to detect and eliminate Sybil attack; we named it as SYDECT algorithm. Proposed algorithm takes use of the Digital signature which ensures data authenticity and integrity, so no loss of information is ensured. A Sybil attack is detected and eliminated from the network dynamically and hence improves the network capabilities to perform well. The simulations and experiments would be carried out using Network simulator 2 taking varying number of nodes according to nodes velocity. Performance of network would be evaluated with respect to parameters like Average Throughput, Average Delay, Packet Delivery ratio (PDR) and Normalized Routing Load (NRL) under three MANET protocol namely DSR, AODV and AOMDV routing protocols. Further experiment is conducted to verify the efficiency of SYDECT algorithm based on parameters like Detection rate, True positive rate and false positive rate in MANET environment.**

***Index Terms* - MANET, Sybil Attack, Security**

I. INTRODUCTION

MANET is a kind of wireless network which is decentralized in nature and comprise of moving mobile nodes. Due to changing topology of such network it impose critical security protocol design against harmful attacks such as Sybil Attack. In a Sybil attack a malicious node can produce and manage a large number of logical identities on a single physical device. This gives the misapprehension to the network as if it were different rightful nodes. Sybil attacker node's additional identities are known as Sybil nodes.

A Sybil attacker node can harm to MANET in a number of ways. A Sybil attacker can dislocate location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on diverse locations or node-disjoint paths [4]. The Sybil attacker node impersonates multiple different identities at the same time as shown in figure 1. MANETs are mainly related to illegitimately gathering sensitive information about fake mobile nodes. Such kind of attack to ad hoc networks degrades the performance of the network and provides unsecured routing between sender and receiver mobile node.

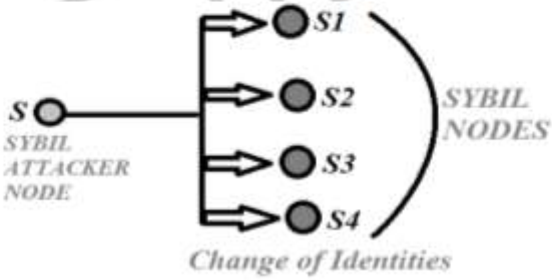


Figure 1: Sybil Attack

II. RELATED WORK

In 2004, J. P. Hubaux et al., [**1**] presented a method to minimize the drivers' hassle and inconvenience. Authors adopted a new intelligent secure privacy-preserving parking scheme through vehicular communications. Their idea employed parking lot RSUs to surveillance and contact between vehicles and the RSUs, will be processed through the road network. Once vehicles, equipped with wireless communication devices into the parking lot, the RSUs communicate with them. RSU needed to provide the drivers with real-time parking navigation service, secure intelligent antitheft protection, and friendly parking information distribution. Parking Lot Information Dissemination algorithm was used for conditional privacy preservation for drivers. Simulations are conducted to demonstrate their proposed model showed that reduced available parking space and subsequently saved fuel.

In 2005, Jinyuan Sun et al., **[2]** proposed ID-based cryptosystem framework to address the security problem in VANET. Their proposed method helps to achieve desired privacy by vehicles and required non repudiation by authorities. The fundamental security requirements including authentication, message integrity and confidentiality are satisfied. The result showed that the framework achieved good communication and provides authentication security in some extent.

In 2006, B. Xiao **[3]** introduced a method for the detection of Sybil attack using cryptography method. A good security mechanism has short delay for encryption, decryption and key exchange short delay is removed. By using this method has low delay for detection Sybil attack, because most operations are done by the Certification Authority.

In 2007, Maxim Raya et al., **[4]** proposed Misbehavior Detection System (MDS) protocol and Voting Evaluators (VE) protocol for the identification and local control of misbehaving or faulty nodes. The vulnerability is eliminated by identifying faulty or misbehaving nodes and distributes revocation information in VANET. The Misbehavior Detection System (MDS) protocol detects the fault nodes and activate a Local Eviction of Attackers by Voting Evaluators (LEAVE) to revoke the attacker from the network. The result showed that the proposed scheme is practical, efficient, and effective in isolating misbehaving and faulty nodes.

In 2008, Jesus Tellez Isaac et al., **[5]** proposed Kiosk Centric Model payment protocol to secure vehicle-to-road side communication in vehicular Ad hoc Network. This method is used for authentication while communication is not directed between the nodes. The payment process is enabled for both credit-card and debit-card transactions. The result showed that the scheme achieved more security for online payment.

In 2009, Mohamed Salah Bouassida et al**., [6]** proposed a Sybil detection approach based on the received signal strength variations, according to their localizations, which allows a node to verify the authenticity of the other communication nodes. In addition, VANET that allows two nodes to determine the Sybil and malicious ones, an estimate of the degree of ability to distinguish between metric. This contribution fits the geometric analysis, simulations and validated by actual measurements. Assessment of their ability to differentiate their geographic localizations verification VANET: This approach is the interaction between the ends of two complementary technologies to verify the authenticity of a node in an allowable.

In 2010, Jinyuan Sun et al**., [7]** proposed a privacy preserving technique for VANETs security to preserve desired privacy by vehicles. Fundamental security requirements including authentication, non repudiation, and message integrity are analyzed in the method. To avoid the use of certificates the ID-based cryptography (IBC) algorithm uses the public key entity which is derived from its public identity information such as name, email address in PKI

In 2011, Sushmita Ruj et al., **[8]** introduced the concept of data-centric Misbehavior Detection Schemes (MDS) to detect false alert messages and misbehaving nodes by observing their actions after sending out the alert messages. In the data-centric MDS, each node decide whether received information is correct or false. Based on the consistency of recent by arrived alert messages vehicle positions are estimated. So, voting or majority decisions are not needed for making MDS resilient to identify Sybil attacks. Once misbehavior is detected, it does not revoke all the secret ID of misbehaving nodes. Instead of imposing fines on misbehaving nodes (administered by the certification authority) discourage them to act selfishly. The results showed that the scheme reduced the computation and communication costs involved in revoking all the secret ID of misbehaving nodes.

In 2012, Ramakrishna M **[9]** described about the Distance jobs Routing (DBR) protocol described. This protocol is used to create real-time traffic information via a link to the vehicles. Connection diagram depicts the distance between neighboring vehicles. Location-based routing algorithm significantly when compared to flood-based routing protocol, which reduces the probability of packet and reduces network traffic. The proposed protocol error GP Even if the information is being obtained by using the S-velocity digital map data loads neighbors. As a result, the vehicle's speed and direction change, thus reducing network overhead, without a hello message periodically broadcast protocol that avoids the reducing the network overhead.

In 2013, V. Geetha Devi et al**.,[10]** a Threshold El Gamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion by the malicious vehicles. The packet loss tolerance is used to analyze the performance of the model. This method provide security with low overhead in emergency Braking notification and does not increase overhead for Decentralized floating car Data driving security promotion. The result showed that the scheme effectively compromise and reduce the collusion in VANET.

In 2014, Muhammad Al-Mutaz et al., **[11]** described a novel protocol for Sybil detection in vehicular networks, which are cyber-physical systems, The protocol showed similar performance for Normal Dispersion Efficiency Attack model, while the Minimum Efficiency Attack model may remain undetected at high Sybil percentages. Cryptographic primitives for Sybil detection algorithm is used for the purpose of effective, practical, efficient, and simple. Additionally, they have presented some advanced attack methods where the attacker knows the detection scheme and has a priori road information.

III. PROPOSED SCHEME

To detect Sybil attack using digital certified signature is the key idea to work on SYDECT Method. In SYDECT Method, we need to detect the Sybil attack during the packet transmission between sender and destination node. The main operation of this method is started with assigning digitally certified certificate to all nodes of the mobile ad-hoc network. All nodes are able to send the messages with their NODE ID, digital certificate and its location identity. Whenever a sender node request to send data to destination, it establish its digital signature key, node ID and its location as status and send it to destination node. If the digital signature is verified then message will be encrypted and decrypted with appropriate hash function and message authentication & data integration is applied. It allows secure transmission between sender node and receiver node. Since SYDECT method is applied during runtime of packet transmission so minimal delay is achieved. If the digital signature is not verified occurrence of malicious activity is been detected. At this stage, the node status at which malicious activity detected is checked out with NODE ID, its location and Digital certificate. If it reflects more than one node IDs with same digital certificate, then other IDs digital certificate will not be verified and Hence Sybil attack detected. The SYDECT algorithm is shown below in figure 2.

```
INPUT: SYDECT Method
Output: Digital signature certified MANET network
STEP1.  Initiate all MANETs Node.
STEP2.  Sender node sends hello request with node ID and its location to all nodes.
STEP3.  Source node send request message to receiver node.
STEP4.  Starting with SYDECT method before sender node and receiver node.
        >>> initialize digital signature key establishment phase.
        >>> initialize privacy preserving phase using route discovery.
STEP5.  Destination sends RREP message with signed Digital Signature.
STEP6.  Is Digital Signature Verified?
STEP7.  If yes; then
        >>> Do encryption and decryption of certificates assigned to nodes with different Node IDs.
        >>> Data integration and authentication phase will be initialized.
        >>>Expand the communication between sender and destination node.
        >>> Exit. Go to step 9.
STEP8.  If no; then
        >>> Occurrence of malicious activity has been detected.
        >>>Send the node status at which it takes place to other node of the network.
        >>>If it reflects more than one node IDs with same digital certificate, then other IDs digital certificate
        will not be verified and Hence Sybil attack detected.
        >>> Exit. Go to step 9.
STEP9.  EXIT
```

Figure 2: SYDECT Algorithm

IV. SYBIL ATTACK IMPLEMENTATION AND DETECTION

To conduct experiment, the very popular simulation tool NS-2 is used. The main reason to select this tool is that it has pre-installed setup of many routing protocols. Here we consider DSR, AODV and AOMDV routing protocols for performance analysis. Also it has flexibility to expand and adopt the code written in c++ language. First of all we have implemented the Sybil attacker to show up multiple identities and modified the appropriate routing protocols. Figure 3 shows the snapshot of output NAM window when Sybil attacker is not involved in communication between sender and receiver node, it does not drop packets.

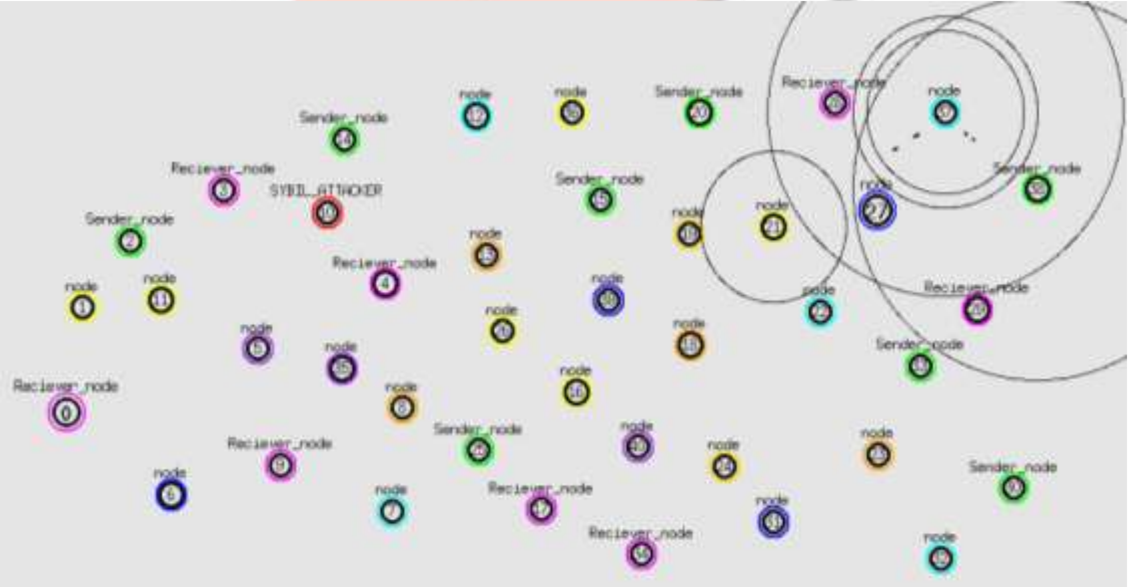


Figure 3: Sybil Attacker not involved in communication, no packet drop

Figure 4 shows the output NAM window when Sybil attacker is involved in communication between sender and receiver node, here packet drop is seen due to the reason that attacker node impersonating Fake IDs , and sender node doesn't find the real receiver node. Every time when the Sybil attacker involves during communication it drops packets. It results higher packet loss rate and degrade the performance of the network.

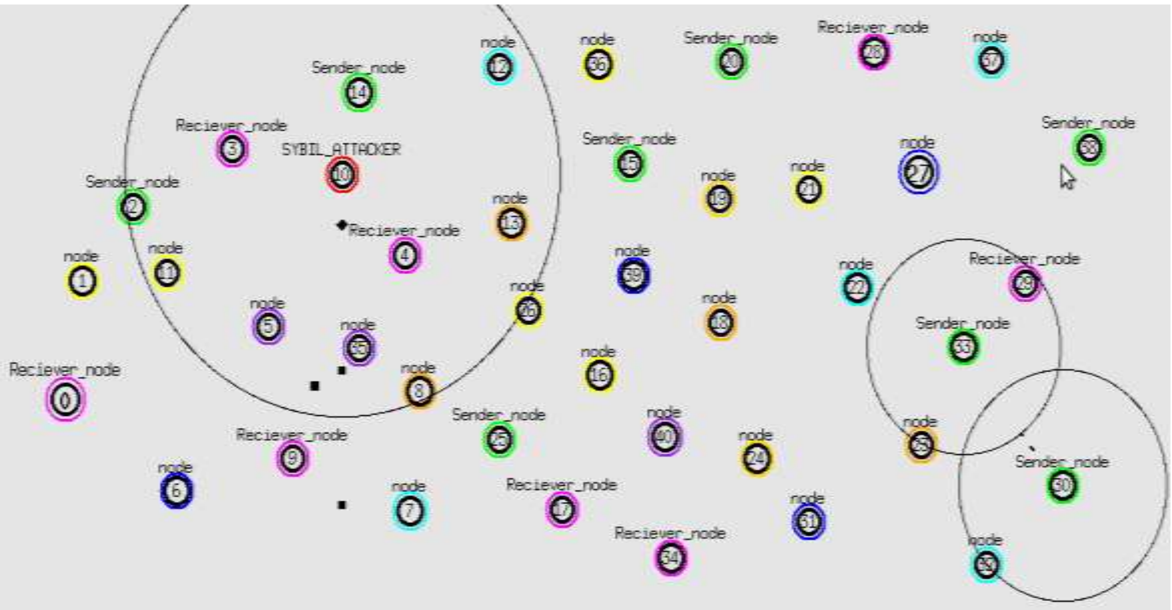
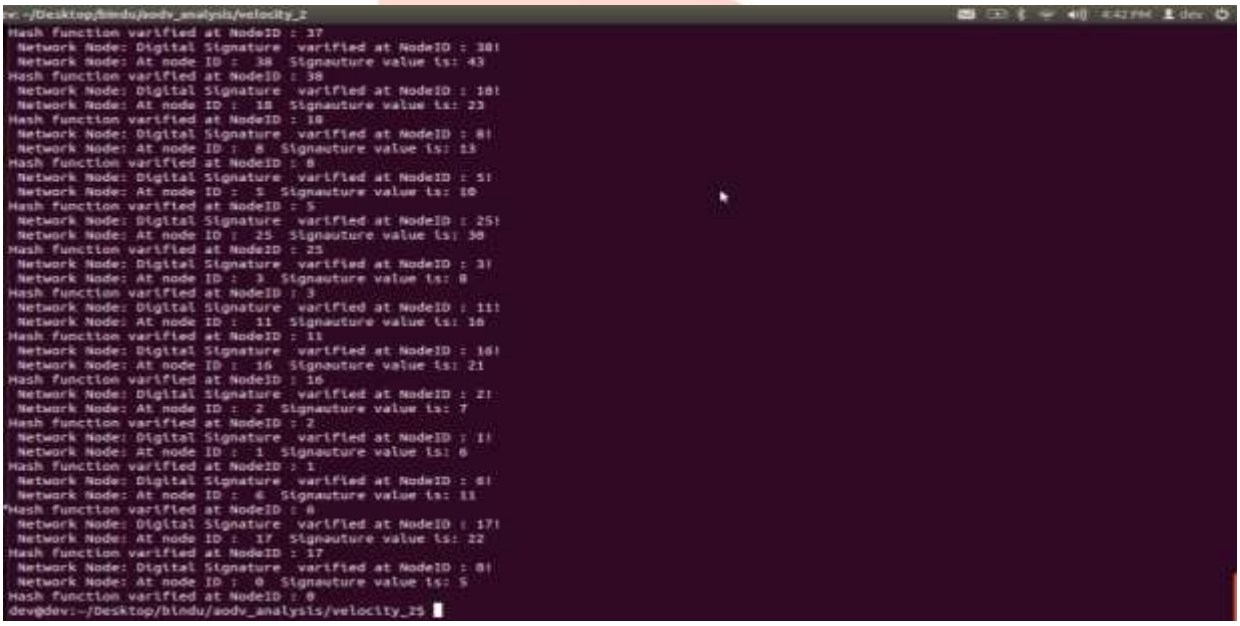


Figure 4: Sybil Attacker involved in communication, packet drops seen

After successful implementation of Sybil attack in MANET environment, we need to implement SYDECT algorithm. Our proposed algorithm verify each node before communication between sender and receiver node , hence there is less chance for sybil attacker to misguide the sender node. Although sybil attacker impersonate fake identities but after verification of ID of node from receiver side , sender node selects alternative path to complete the communication and sybil attacker node eliminated dynamically from the network. Figure 5 shows the output snapshot of terminal showing implemented SYDECT algorithm.



```
ev: ~/Desktop/bindu/aodv_analysis/velocity_2
Hash function varified at NodeID : 37
 Network Node: Digital Signature  varified at NodeID : 38!
 Network Node: At node ID :  38  Signauture value is: 43
Hash function varified at NodeID : 38
 Network Node: Digital Signature  varified at NodeID : 18!
 Network Node: At node ID :  18  Signauture value is: 23
Hash function varified at NodeID : 18
 Network Node: Digital Signature  varified at NodeID : 8!
 Network Node: At node ID :  8  Signauture value is: 13
Hash function varified at NodeID : 8
 Network Node: Digital Signature  varified at NodeID : 5!
 Network Node: At node ID :  5  Signauture value is: 10
Hash function varified at NodeID : 5
 Network Node: Digital Signature  varified at NodeID : 25!
 Network Node: At node ID :  25  Signauture value is: 30
Hash function varified at NodeID : 25
 Network Node: Digital Signature  varified at NodeID : 3!
 Network Node: At node ID :  3  Signauture value is: 8
Hash function varified at NodeID : 3
 Network Node: Digital Signature  varified at NodeID : 11!
 Network Node: At node ID :  11  Signauture value is: 16
Hash function varified at NodeID : 11
 Network Node: Digital Signature  varified at NodeID : 16!
 Network Node: At node ID :  16  Signauture value is: 21
Hash function varified at NodeID : 16
 Network Node: Digital Signature  varified at NodeID : 2!
 Network Node: At node ID :  2  Signauture value is: 7
Hash function varified at NodeID : 2
 Network Node: Digital Signature  varified at NodeID : 1!
 Network Node: At node ID :  1  Signauture value is: 6
Hash function varified at NodeID : 1
 Network Node: Digital Signature  varified at NodeID : 6!
 Network Node: At node ID :  6  Signauture value is: 11
Hash function varified at NodeID : 6
 Network Node: Digital Signature  varified at NodeID : 17!
 Network Node: At node ID :  17  Signauture value is: 22
Hash function varified at NodeID : 17
 Network Node: Digital Signature  varified at NodeID : 0!
 Network Node: At node ID :  0  Signauture value is: 5
Hash function varified at NodeID : 0
dev@dev:~/Desktop/bindu/aodv_analysis/velocity_25 
```

Figure 5: SYDECT algorithm Terminal output snapshot

V. Experiment Results

In this research paper the network performance is measured by four parameters: throughput, packet delivery ratio, average delay and normalized routing load. Further the analysis of proposed scheme is tested to know its efficiency based on parameters detection rate, true positive rate and false positive rate. We have simulated a network of 40 nodes with varying nodes velocity 2m/s,4m/s,6m/s,8m/s,10m/s,12m/s,14m/s and 16m/s deployed randomly within a 1000 meter × 1000 meter area. Each node has a radio propagation range of 250 meters and simulation run time is 60 seconds. We used the IEEE 802.11p as the MAC layer protocol, Constant Bit Rate (CBR) node traffic and used the random waypoint model for node mobility.

We have adopted two methods; one is RSS based detection and proposed digital signature based detection SYDECT method. Both detection methods are applied to DSR, AODV and AOMDV routing protocols. Following figure 6 shows the throughput graph for each routing protocol. It could be easily seen that our proposed SYDECT method works well than the RSS detection method for every protocol. We have found the higher throughput rate for AODV routing protocol and lesser throughput rate for DSR protocol.

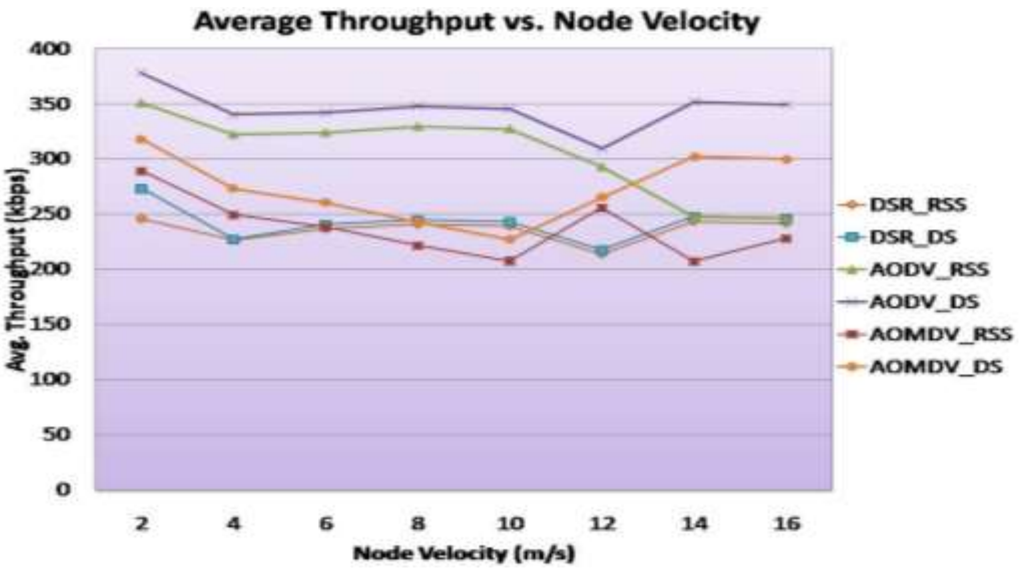


Figure 6: Average Throughput

Following figure 7 shows the packet delivery ratio graph for each routing protocol. It could be easily seen that all routing protocol give better outputs with little difference among them, but it is concluded that protocol utilizing SYDECT approach gives better result than RSS method.

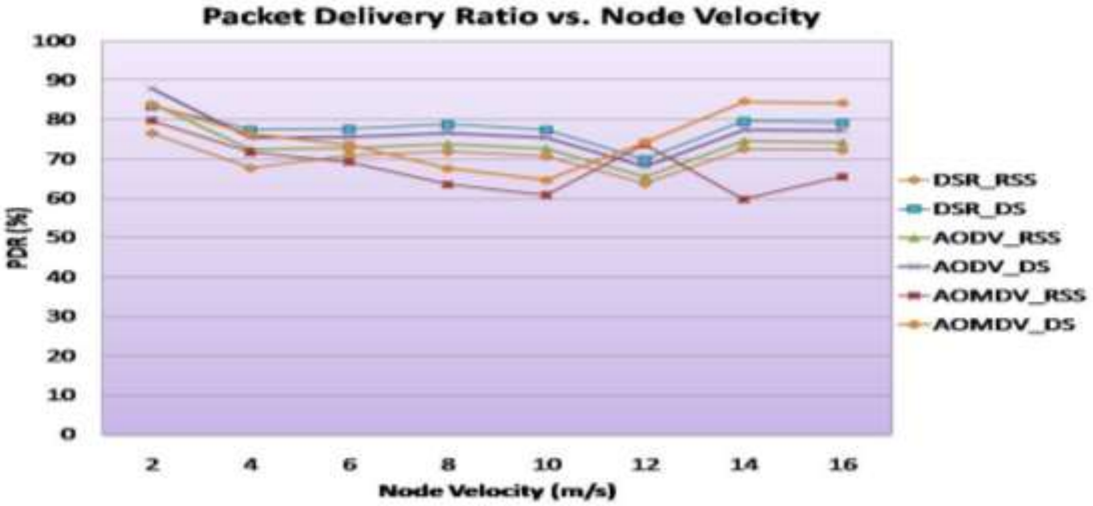


Figure 7: Packet Delivery Ratio

Following figure 8 shows the average delay graph for each routing protocol. It could be easily seen that all routing protocol give better zigzag outputs with little difference among them except in case of AOMDV protocol. AOMDV protocol gives higher delay than other two protocols. But under SYDECT method the same AOMDV protocol shows lesser delay compared to RSS method.

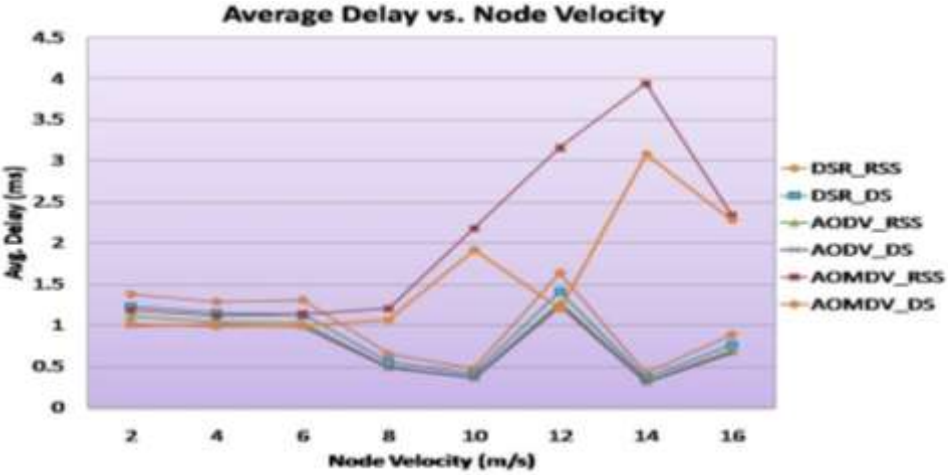


Figure 8: Average Delay

Following figure 9 shows the Normalized routing load graph for each routing protocol. It could be easily seen that all routing protocol give increasing routing load due to reason that all protocols need to update their forwarding hops in their routing table whenever they are having communication which finds difficulty in increasing node velocity. Routing protocols using SYDECT approach gives better result than RSS method.

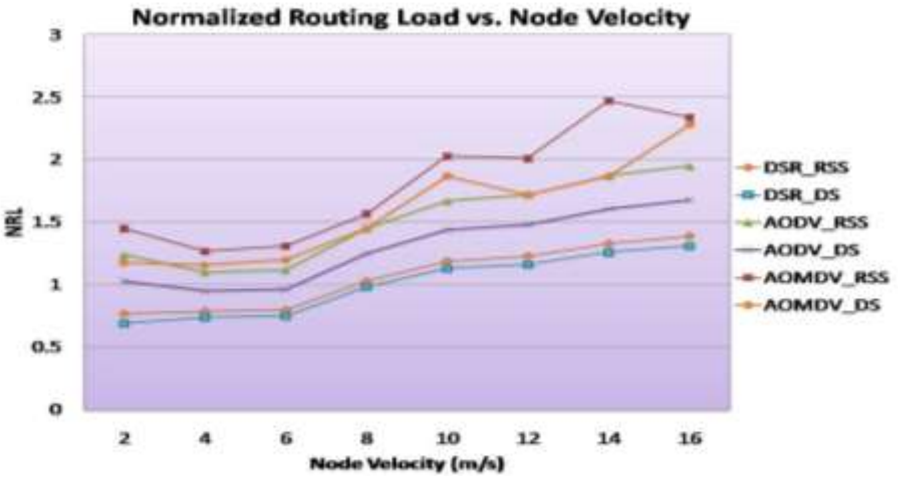


Figure 9: Normalized Routing Load

Following figure 10 shows the detection rate graph for each routing protocol. From the graph it could be easily conclude that SYDECT approach shows 100 percent detection rate. The reason is that it checks the nodes digital signature before proceeding to communicate with other nodes and Sybil attacker node detected at earlier stage.

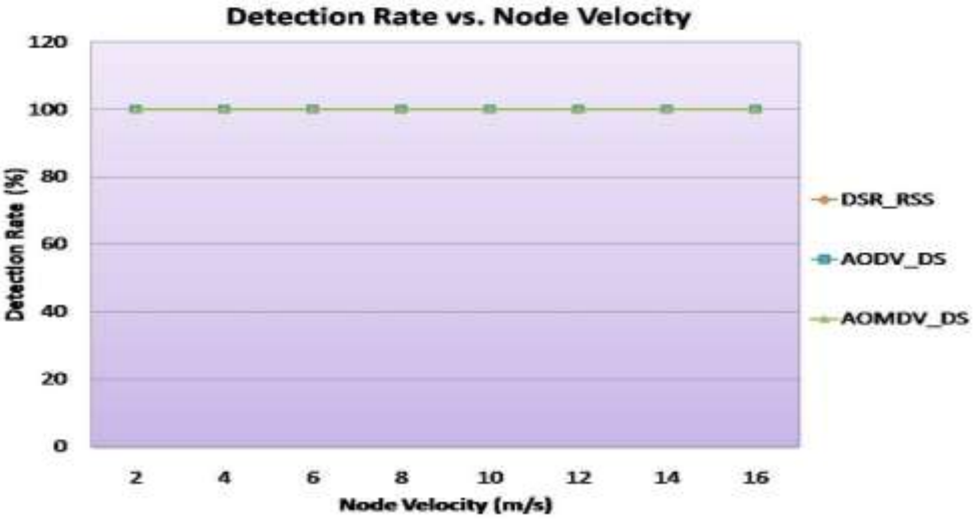


Figure 10: Detection Rate

Following figure 11 shows the True positive rate (TPR) graph for each routing protocol. TPR is probability of the right detection of sybil attacker node among many other node which have been identified as attacker one. From the graph it could be easily conclude that AOMDV protocol has higher TPR rate than other two protocols, it means our proposed SYDECT method works better in this protocol in respect of detection approach.

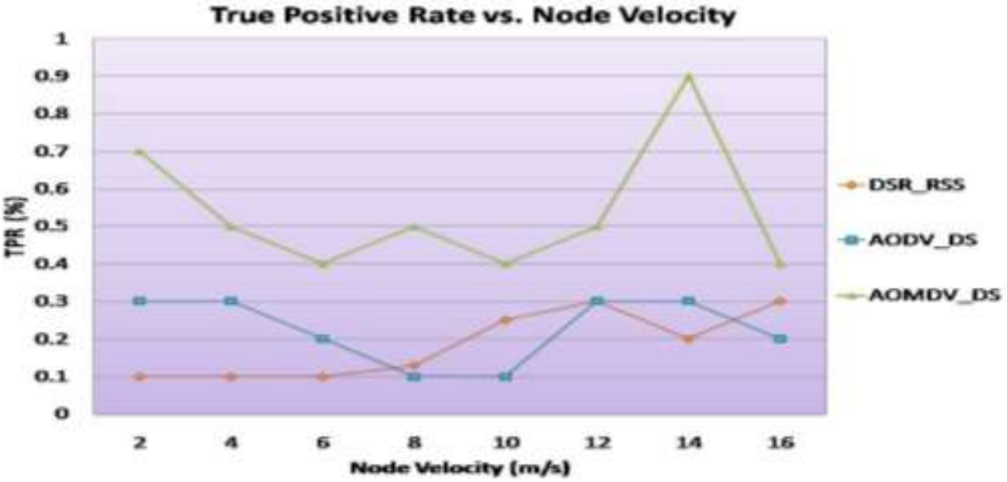


Figure 11: True Positive Rate

Following figure 12 shows the False positive rate (FPR) graph for each routing protocol. FPR is probability of the false detection of Sybil attacker node among many other node which have been identified as attacker one. From the graph it could be easily conclude that AOMDV protocol has lower FPR rate than other two protocols, it means our proposed SYDECT method works better in this protocol in respect of detection approach.

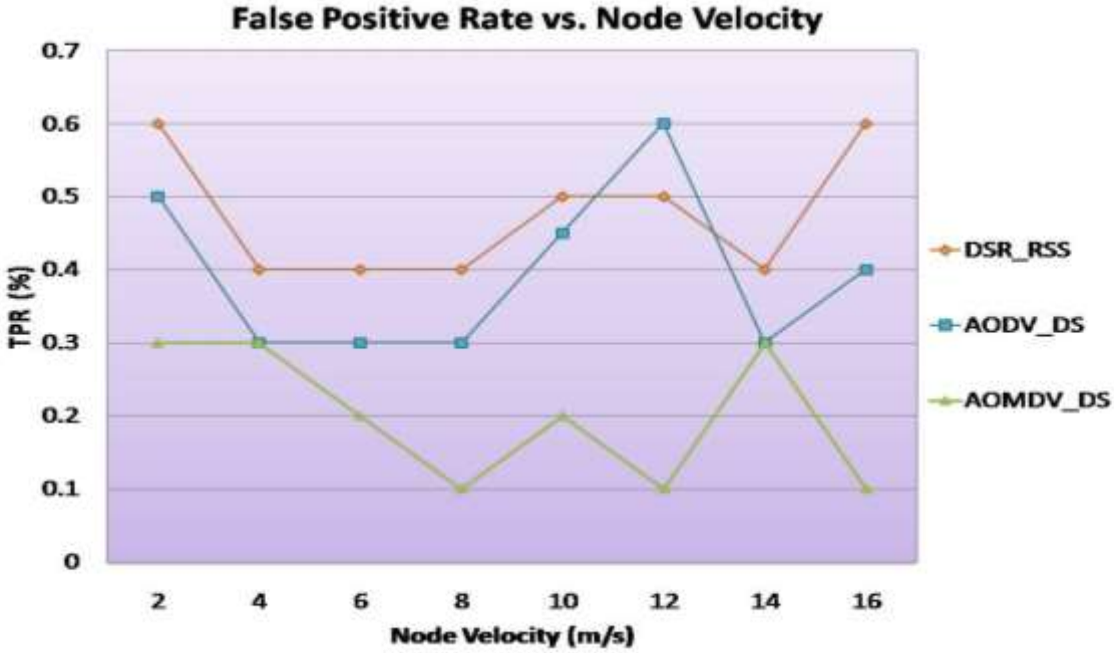


Figure 12: False Positive Rate

VI. CONCLUSION & FUTURE WORK

In this paper the problem of Sybil attack is studied as it is a harmful threat to the security of Mobile Ad Hoc Networks. An existing technique is studied which is based on the computation of Received Signal Strength (RSS) to detect the Sybil Attack. The method takes use of the received signal strength (RSS) to calculate the distance between two identities to further calculate the position of fabricated identities. Then Digital Signature based SYDECT algorithm is proposed to detect Sybil Attack; which can be used for MANET environment. In this research work, the proposed method is tested under three routing protocols, namely DSR, AODV and AOMDV routing Protocols. The main motive to select three different routing protocols is that at the end of simulation performance it could be easily conclude that at which routing protocol, the proposed SYDECT method is performing well. The four main parameters are evaluated to check the performance of each routing protocol using SYDCT method each, they are Average Throughput, Packet Delivery Ratio, and Average Delay and Normalized Routing Load. In parametric evaluation of routing protocols, simulation results show that AODV performs better than DSR and AOMDV routing protocol. Also we have achieved better delay performance using SYDECT method as compared with the RSS based detection method. Furthermore, the investigation to know the efficiency of proposed SYDECT algorithm is performed based on three parameters; namely Detection Rate, True Positive Rate and False Positive Rate. Among three routing protocols, AOMDV is found to be more effective to detect the Sybil attack since it has showed higher TPR rate.

Future work of this research work relies on improving the performance of SYDECT method. Although proposed method successfully detect the Sybil attack during run-time of simulation, but it must be able to eliminate it from the network also; this work is left for the future work. Also this research work is presented for small MANET environment; it will be tested for larger MANET environment having thousand numbers of nodes with more attacker nodes.

REFERENCES

[1] Ean-pierre hubaux, Srdjan capkun, and Jun luoe "The security and privacy of smartvehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May 2004.

[2] Inyuan Sun, "An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks" in workshop on Hot Topics in Networks(HotNets-IV),2005.

[3] B Xiao,B Yu and C Gao, "Detection and localization of Sybil nodes in VANETs", DIWANS '06 Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks,2006.

[4] Maxim Raya, "Eviction of Misbehaving and Faulty Nodes in Vehicular networks", IEEE 1-4244-1455-5/07/$25.00 c, 2007.

[5] Jesus Tellez Isaac, "A Secure Vehicle-to-Roadside Communication Payment Protocol in Vehicular Ad Hoc Networks", IEEE communication networks,2008.

[6] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial ," Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", International Journal of Network Security, Vol.9, No.1, PP.22 33, July 2009.

[7] Jinyuan Sun, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transcations On Vehicular Technology, Vol.X,No.X,Xx 2010.

[8] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, "On Data-centric Misbehavior Detection in VANETs", International journal of Network Security& its applications, 2011.

[9] Ramakrishna M, "DBR: Distance Based Routing Protocol for VANETs", International Journal of Information and Electronics Engineering, Vol. 2, No. 2,March 2012.

[10] V. Geetha Devi, P.Shakeel Ahmed, P.Babu, " A Route map for Detecting Sybil Attacks in Urban Vehicular Networks", International Journal of Modern Engineering Research (IJMER Vol.3, Issue.2, pp-1157-1160 ISSN: 2249-6645,2013.

[11] Muhammad Al-Mutaz, Levi Malott and Sriram Chellappan, "Detecting Sybil attacks in vehicular networks", Journal of Trust Management 2014.

[12]