International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-10, August 2020

Sybil Attack Detection in Vehicular Ad-hoc Networks using Direct Trust Calculation

Sunil Kumar V, Ramesh Babu D R

Abstract*: *Vehicular Ad-hoc Networks (VANETs) are gaining rapid momentum with the increasing number of vehicles on the road. VANETs are ad-hoc networks where vehicles exchange information about the traffic, road conditions to each other or to the road-side infrastructures. VANETs are characterized by high mobility and dynamic topology changes due to the high-speed vehicles in the network. These characteristics pose security challenges as vehicles can be conceded. It is critical to address security for the sake of protecting private data of vehicle and to avoid flooding of false data which defeats the purpose of VANETs. Sybil attack is one of the attacks where a vehicle fakes multiple vehicle identity to compromise the whole network. In this work, a direct trust manager is introduced which derives the trust value of each of its neighbor nodes at a regular interval of time. If the trust value is deviated, it confirms sybil attack. The proposed system is compared with the existing system to prove improved sybil attack detection ratio, thus providing better security. NS2 environment is used to prove the simulation results. The experimental results show that the attack detection ratio of SAD-V-DTC is 5 times better than that of the existing system. The packet delivery ratio shows an improvement of 27.27% while the false positive shows a good increase of 65.80% than the existing system.

Keywords: VANET, Sybil Attack, RSA Algorithm, Location Certificate, Direct Trust Calculation, AODV, NS2.

I. INTRODUCTION

VANETs offer communication among the moving vehicles and fixed infrastructure unit with the purpose of promoting comfort, safety, and efficiency. The decentralized nature and wireless communication medium bring numerous security threats to vehicular networks. Sybil attack is a serious threat in VANET where the malicious vehicle spoofs multiple identities in order to counterfeit the events for enhancing driving experience personally. Sybil attack is difficult to identify as sybil nodes behave to be legitimate nodes and the attack is not visible until it becomes apparent to other vehicles. The Sybil attacker takes acquisition of the entire VANET operations and inserts false-hearted event information which results in erroneous decisions in vehicles. For instance, the VANET system produces a traffic event report based on information collected from numerous vehicles. Here, the traffic event report is deviated from the realistic situation when some of the vehicles are Sybil. Consequently, the Sybil attacker uses it for his own benefit and creates data inconsistency in the network. Location-based Sybil attack detection mechanism utilizes the motion pattern of vehicles in which the vehicles cannot fake other vehicles under different RSUs for attack detection. However, an ingenious attacker may compromise the RSUs for legitimate trajectories and also reinforce the attack level. Hence, it is crucial to detect the Sybil attack without revealing the location privacy and real identity without compromising both vehicles and RSUs. In order to improve attack detection and routing performance," Sybil Attack Detection in Vehicular Ad-hoc Networks using Direct Trust Calculation" (SAD-V-DTC) is proposed. The main objective of SAD-V-DTC is to improve attack detection ratio and increase packet delivery ratio. In this work, a direct trust manager is introduced which derives the trust value of each of its neighbor nodes at a regular interval of time. If the trust value is deviated, it confirms sybil attack. To further mitigate sybil attack, the sybil nodes are stored in blacklist. When a source node wants to communicate to another node, it checks the blacklist and bypasses the sybil route to reach the target node. By following this method, sybil node is detected quickly and malicious nodes are made aware to all the neighboring nodes in the network.

Revised Manuscript Received on August 30, 2020.
* Correspondence Author
Sunil Kumar V, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, affiliated to Visvesvaraya Technological University, Bangalore, India. Email: sunil.manasu@gmail.com
Prof. (Dr.) Ramesh Babu D R, Department of Computer Science and Engineering, Dayananda Sagar College of Engineering, affiliated to Visvesvaraya Technological University, Bangalore, India. Email: bobrammysore@gmail.com

II. LITERATURE REVIEW

One of the most important characteristics of security is authentication. Every node has unique identity in the network. Sybil attack is an attack which compromises on authenticity of a node. An attacker fakes multiple identity of a legitimate node or even fake nodes for his personal benefit. The attacker misuses the identities to transmit false messages in the network or may limit the resources leading to DoS attack. This is a dangerous attack as it leads to other form of attacks as well like DoS, impersonation attack, bogus attack, etc. Different works are carried out in order to prevent or detect sybil attack in VANETs. Few of the works are discussed next. In order to preserve the privacy of vehicles like unique identity, location, driver details etc., pseudonyms are created. The pseudonyms are used in the message exchange rather than the original identity.

However, the pseudonyms too can be compromised leading to sybil attack. In [3], the trusting authority distributes multiple pseudonyms for same vehicle to RSU. These multiple pseudonyms are hashed to a common value. Whenever the RSU encounters a vehicle with a pseudonym that does not belong to the pool of pseudonyms with a common hash value, it identifies that node as the attacker. It is important to note that this method works well as long as the RSU is not compromised. If RSU is compromised, then all the pseudonyms are comprised as sybil attack cannot be prevented. In [4], another sybil detection method is proposed by using footprint (locations traversed) of the vehicles as the main baseline. When a vehicle encounters RSU, it authorizes itself with proof of location at that particular time. The next RSU it encounters concatenated the proof of location at that point of time. This consecutive series of location information is called the trajectory of the vehicle. The RSU signs anonymously, thus preserving the privacy of RSU with respect to location and identity. This ensures that the RSU cannot be compromised. Another rule incorporated is temporarily linkable, which means that two messages are valid if they are generated by the same RSU within a given period of time. If the messages cross the given time period, they become invalid. When a vehicle wants to communicate information to RSU or another vehicle, the RSU checks the trajectory and confirms it with other consecutive neighboring RSUs. If trajectory is found, it is a valid node, else it is a sybil node and is removed from the network. In [5], a hybrid scheme is proposed which combines P2DAP [3] and footprint [4]. P2DAP performs better than footprint with the increase in number of vehicles while the footprint outperforms P2DAP when the speed of vehicles increases. Hybrid scheme was introduced with the intent of higher performance and higher detection rate. It works by applying footprint when the vehicle speed increased (if speed exceeds 40km/hr.) and applying P2DAP when the number of vehicles is more. In [6], a detection system for Sybil attack using each RSUs neighboring list, called IOAC (Infrastructure Observation-based Affinity Computation) is proposed. It uses fake IDs instantaneously to distinguish malicious nodes from legitimate nodes. This system is built on two evidences that observing two neighborhood RSUs identities at the same time tells that they are related, while observing two identities of two different neighborhood RSUs with no interconnected zone of communication range concurrently states that the two identities are not related. With this knowledge, IDs that are strongly involved to each other are found thus they might belong to the identical vehicle.

In [7], an active algorithm for detecting sybil attack is proposed. After receiving a message from a suspicious node, the distance between the host node and the suspicious node is calculated, using the GPS coordinates. The transmission power to be used for the detection packet is calculated. Host node sends the detection packet. If detection packet does not cause a delay, then this node is labeled as sybil else new transmission power is calculated which excludes doubting node. If detection packet does not cause a delay, then this node is labeled as honest else it is a sybil node.

In [8], a method for detecting sybil attack is proposed based on similarity measuring of RSSI time series. A vehicle sends the basic information on control channel periodically. Neighboring nodes will determine received signal strength indication value for each received packet. Each vehicle monitors the control channel and records all the latest messages within the observation time. For each packet, voiceprint stores the ID and received signal strength indication and for each received ID it generates RSSI time series. Each two RSSI time series is compared and distance is measured. If the distance between the nodes are closer to zero the it is marked as sybil nodes.

In [9], an authentication framework is proposed to preserve the privacy of vehicles to prevent against impersonation and sybil attack. When a vehicle enters and exits a particular area, it inscribes itself to trusted authority. TA will allocate the identities of RSUs to all vehicles. RSUs disseminates its info to all the vehicles within its territory. Vehicles will request for offline signature with RSU by communicating and acquiring RSUs information. Offline signature will be created by RSUs by using Id Based Signature strategy. RSUs will send the offline signature to the desired vehicle and to all vehicles within its range. Vehicle will create its own online signature by using the offline signature and it is performed by using Identity Based Online-Offline Signature system. When a vehicle wants to communicate with other neighboring vehicles, it sends a request using its online signature. Receiving vehicle will authenticate the originator vehicle's request message. Communication will be established if it is valid and after accepting the request, else it will discard the request.

In [10], a privacy-retaining authentication and Sybil detection procedure is proposed. Each vehicle is registered with the trusted authority. Each vehicle is inserted into a set of vehicles that has a property of k-anonymity set. Vehicle requests temporary keys form the RSU. RSU checks if group revocation token of vehicle is not in the revocation list and timestamp is within threshold then same RSU generates new set of keys, authenticates them and sends it to vehicle. If vehicles are in the same current anonymity set, then these vehicles attach the digital certificate of the deeper anonymity set into the beacon messages. This approach informs other vehicles that there are no Sybil attackers nearby. This approach also makes a Sybil attack difficult to launch.

In [11], a security protocol to overcome network attacks is proposed. It is divided into three phases:

BS and RSU communication phase - Base station sends a group identity and random variable to RSU to check the mode of RSU. RSU responds whether it is active or not. Upon receiving the response from RSU, base station sends the certificate to RSU. The channel is encrypted by using a random variable and upon receiving the certificate it is decrypted by using same random variable.

RSU and vehicle authentication phase - Vehicle sends its identity to RSU. RSU in response sends its certificate and identity. Vehicle stores the certificate of RSU and sends the message to RSU. RSU receives the message.

Vehicle to Vehicle communication phase - The vehicle will send the certificates to each other. If the certificate is same and authenticated the communication will continue.

In [12], the basic idea of sybil attack is exploited for detecting the sybil node. The nature of sybil is to fake identities of multiple vehicles.

The proposed idea involves nothing more than the list of neighboring RSU which is already present in the trusted authority eliminating overhead. The detection of malicious node is based on two observations:

- If two vehicles are observed at the same location, then it is confirmed that they are related.
- If two vehicles are observed at two different RSUs where the area does not intercept it confirms that they are not related.

These observation for a certain period of time detect sybil nodes.

In [13], paper uses Advanced Driver Assistance System (ADAS) sensors which are already mounted on the vehicles to detect sybil attack without the use of any infrastructure or authorizing party. ADAS sensors can include radar, camera, lidar mounted on the vehicles. The images identified in raw format is processed by On-Board Units (OBU) to identify objects around it at a particular angle and distance. When a target node receives Global Positioning System (GPS) message from another vehicle, it first checks if that node is valid within the radius. If the first condition is satisfied, the target node computes the distance and the angle of the source node from which it received. It compares this data with the ADAS sensor data to check if that vehicle really exists at that location where it claimed to be. If the source vehicle is found, it is a genuine node otherwise location spoofing is identified.

In [14], a merged technique is introduced by combining two security mechanisms. The first level involves Public Key Infrastructure (PKI), and the second level involves hashing function. The PKI ensures non-repudiation by using private key known only to the vehicle and by sharing the public key which can be verified by any entity. This way, the attacker will not be able to get the protected data. The message is hashed with the MAC address of the vehicle and is sent to the target node. The target node checks for the hash. If hash is not present, it is discarded straight way, if hash is present it tries to match it with the registered hash value, if it matches it is accepted else it is discarded. This second level of security thus ensures integrity.

III. IMPLEMENTATION

The main intent of proposed protocol is to improve the attack detection and increase packet delivery ratio over the existing system. The existing system [15] uses location certificate to detect the sybil attack only when an event occurs. This means that the system does not actively check for malicious nodes until an event occurs. The proposed system actively checks for the malicious nodes at regular intervals making the system more resistant to the sybil attack. In order to achieve this objective, the proposed protocol exploits location certificate along with direct trust calculation. Fig. 1 below shows the flow chart of the process of SAD-V-DTC.

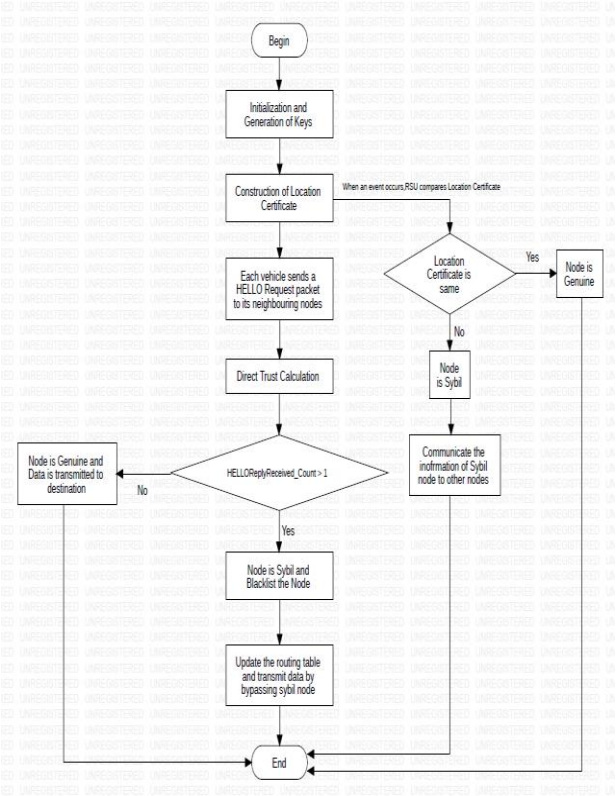

Fig. 1. Flowchart of SAD-V-DTC

A. Modules

The implementation module can be divided into 4 modules as follows:

1. System Initialization
2. Construction of Location Certificate
3. Direct Trust Calculation
4. Detection of Sybil Attack

1. System Initialization

In system initialization stage, RSUs are divided into groups. Each group covers certain regions or a road section. RSUs within each group generates public and private key pairs by using RSA algorithm. To make sure RSUs are distributing location certificate for genuine vehicles, each vehicle produces a set of public and private key pairs by using RSA algorithm. Vehicles get certificates for each public key from the RTA during vehicle registration so that vehicles can secretly authenticate themselves to the RSUs.

2. Construction of Location Certificate

Construction of Location Certificate stage explains how a vehicle can establish its location certificate with an example. Suppose a vehicle v_1 is moving across the following RSUs [R_1, R_2, R_3, R_4], then v_1 begins constructing its location certificate as follows:

- When v_1 encounters R_1, it sends its pseudo ID and public key [PK_1].
- R_1 authenticates v_1 if it is genuine to request a location confirmation by examining the v_1's certificate.

Then, it generates a location proof message $m_1 = \{ID_1, t_1, d_1\}$ where ID_1 is the pseudo ID of v_1, t_1 is the current timestamp and d_1 is the distance between v_1 and R_1. Distance between vehicle and RSU is calculated by using Euclidean Distance. Then R_1 encrypts the message and sends to v_1.

- When v_1 encounters R_2, R_2 generates $m_2 = \{(ID_1, t_1, d_1) \,||\, (ID_1, t_2, d_2)\}$ and sends the message back to v_1. Similarly, R_3 and R_4 generates $m_3 = \{(ID_1, t_1, d_1) \,||\, (ID_1, t_2, d_2) \,||\, (ID_1, t_3, d_3)\}$ and $m_4 = \{(ID_1, t_1, d_1) \,||\, (ID_1, t_2, d_2) \,||\, (ID_1, t_3, d_3) \,||\, ||\, (ID_1, t_4, d_4)\}$ respectively to form a location certificate.

3. Direct Trust Calculation

In Direct Trust Calculation stage, the trust value is calculated based on the received hello packet reply count. Each vehicle sends a unique identity HELLO request to its neighbors and waits for unique HELLO reply from each neighbor. If a vehicle receives more than one HELLO reply for a unique vehicle identity from a neighbor, then the vehicle recognizes that its neighbor is representing more than one identity. The HELLO replies for same unique identity are generated from false identities of its neighborhood. Then the node counts the number of received HELLO reply. If the number of HELLO reply count is greater than 1, then the node identifies that its neighbors as Sybil attacker. The information of the sybil node is disseminated to the other neighboring nodes. The source node also adds the sybil node in its blacklist for quick identification in the future.

4. Detection of Sybil Attack

In this stage, sybil node is detected by comparing location certificate and checking the count of direct trust value. In case of an event, a vehicle will send an event to the nearby RSU. Upon receiving an event, RSU will compare the location certificate of vehicle and if it found different then the sybil node is detected. Since this comparison happens only when an event occurs, attack detection is not effective. To overcome this, direct trust calculation is done. In direct trust calculation the malicious nodes are checked at regular intervals. and if the count of received hello reply packet is greater than 1, it considers that neighboring node as Sybil. The source node will broadcast the RREQ packet to discover the shortest route towards the destination and attempts to collect information of all neighbor nodes and register Sybil node into the routing table. Once the sybil node is detected it is blacklisted that is malicious node entry will be deleted from the source node routing table. Next time, when source attempt to forward packet towards a destination, it verifies node information from blacklist and avoid the malicious route and takes shortest alternate path.

B. Pseudocode of SAD-V-DTC System

The pseudocode begins with the generation of public and private keys for the purpose of location certificate generation at RSU. This verification happens only when any event like traffic jam or accident occurs. This is followed by the direct trust calculation module which monitors the system continuously for any sybil node.

The pseudocode of the SAD-V-DTC is as presented in Fig 2.

```
Begin:
Divide RSUs into groups
Deploy nodes for simulation as per user requirements
Generation of public and private key pairs by vehicles and RSU using RSA
algorithm
For (each vehicle v)
        For (each RSU r)
            Construction of location certificate
        End for
End for
While (forwarding data packets)
  //Direct Trust Calculation
        Each vehicle broadcasts a HELLO Request packet to its
        neighbors and receives HELLO Reply packets and maintains
        count of the received HELLO Reply packets.

        If (count > 1)
                Node is Sybil
                Blacklist sybil node
                Update the routing table and transmit data by avoiding
                sybil node
        Else
                Node is genuine
        End if
  //When an event occurs
        If (location certificate is same)
                Node is Genuine and Forwards the data packet to
                destination
        Else
                Node is Sybil
        End if
End
End
```

Fig. 2. Pseudocode of SAD-V-DTC

IV. SIMULATION AND RESULTS

A. Environment Setup

The VANET system is modelled by randomly deploying vehicles and RSU in a rectangular area. The RSUs are static and vehicles are dynamic. The environment is simulated by varying nodes in number of 30,50,70 and 90. The popular AODV routing protocol is the base for the system model. Table 1 contains the NS2 environmental set up used for simulation. The VANET system is modelled by randomly deploying vehicles and RSU in a rectangular area. The RSUs are static and vehicles are dynamic. The environment is simulated by varying nodes in number of 30,50,70 and 90. The popular AODV routing protocol is the base for the system model. The performance is assessed using following metrics - Attack Detection Ratio, Packet Delivery Ratio, Normalized Routing Overhead and False Positive Rate.

Table- I: NS2 Environmental Setup

SIMULATOR	Network Simulator 2.35
NUMBER OF NODES	30, 50, 70, 90
AREA	600m x 600m
COMMUNICATION RANGE	250m
PACKET SIZE	512 bytes
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE	IEEE 802.11p
QUEUE TYPE	DropTail/Priority Queue
QUEUE LENGTH	50 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	TwoRayGround
ROUTING PROTOCOL	AODV
SIMULATION TIME	50 Seconds

A. Attack Detection Ratio

Attack Detection Ratio is the proportion of sum of attackers detected successfully and total attackers. Attack Detection ratio is determined by using the following formula: ADR = Number of attackers detected / Total number of attackers (1)

In existing system when an event occurs, RSU starts comparing location certificate to detect the sybil node, this means that the sybil node is not detected when there are no events. In the graph, at 50 and 90 nodes, the attack is not detected hence shows zero attack detection ratio. In SAD-V-DTC system, each vehicle transmits HELLO request packet to its neighboring nodes at regular intervals. System checks for malicious node continuously. Hence possibility of attack detection is high.

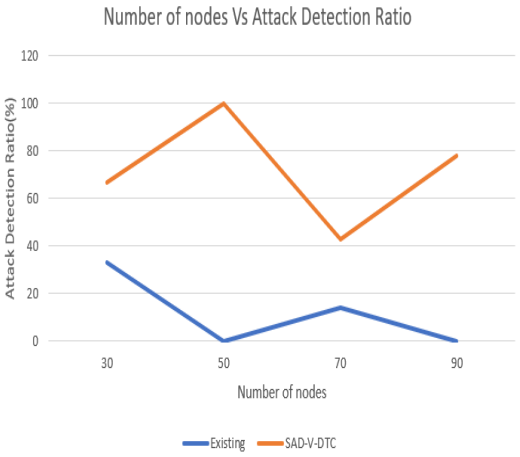

Fig. 3. **Number of nodes Vs. Attack Detection Ratio**

In the graph, Fig 3, Attack Detection Ratio is best for 50 nodes. SAD-V-DTC protocol detects for sybil attack at regular intervals of time. If the time interval is large, the possibility of attack detection ratio will be low. At the same time if the time interval is less then overhead will be high. For 70 and 90 nodes attack detection ratio is less since the attack might have occurred between the time intervals. SAD-V-DTC is 5 times better than existing system.

B. Packet Delivery Ratio

Packet Delivery Ratio in the network is the proportion of total number of received packets and total number of packets transmitted from source to destination. It is computed by using below formula: PDR = Total number of received packets / Total number of packets transmitted (2)

When the value of PDR in the network is high then performance will be better. VANET which has better authentication systems will have a greater PDR than the network without any authentication schemes. If the number of malicious nodes increases, then PDR decreases. Higher mobility of nodes results in PDR to decrease. From the graph Fig 4, in existing system, for 30 and 50 nodes PDR is almost same and it increases for 70 and 90 nodes. Existing system takes more time to detect attacker which causes an attacker to drop packets in the network and the time taken by the RSU for disseminating the information of sybil node to non-affected nodes is high because it has to compare location certificate of vehicles and transmit data to destination. Hence PDR is less.

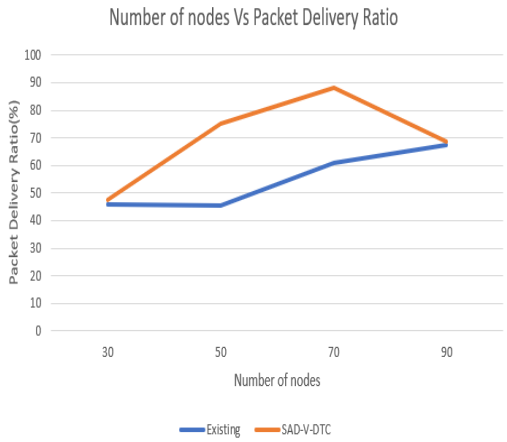

Fig. 4. **Number of nodes Vs. Packet Delivery Ratio**

SAD-V-DTC is based on Direct Trust Calculation. The attack detection in this scenario is very high therefore attackers are immediately identified and isolated from the system. Blacklist of attackers is maintained so that attacker can be detected in the next try. Since attacker is quickly isolated, the possibility of sybil node dropping the packets in the network is less and hence the data reaches the genuine intermediaries to reach the destination. SAD-V-DTC is 27.27% better than existing system.

C. Normalized Routing Overhead

Normalized Routing Overhead is the total sum of routing packets broadcasted for a data packet delivered to the destination. Ratio of network control packets to all delivered packets. It is computed as follows: NRO = Total sum of routing packets transmitted / Total sum of received data packets (3)

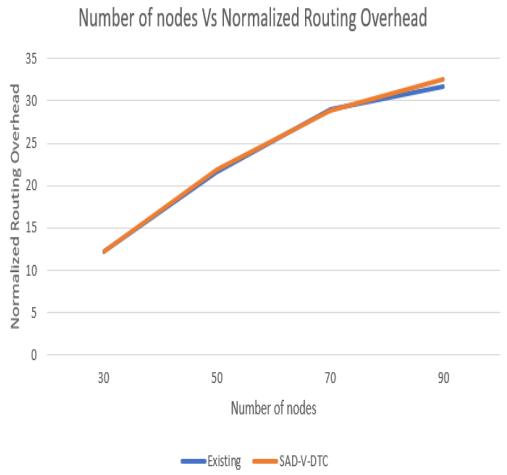

Fig. 5. Number of nodes Vs. Normalized Routing Overhead

SAD-V-DTC system is continuation to existing system that is Direct Trust Calculation is done in addition to location certificate comparison. Direct Trust Calculation is simple calculation of trust values among the node and neighboring nodes within a certain radius. The control packets required for route discovery process is same in both existing and SAD-V-DTC.

Hence overhead involved in Direct Trust Calculation is almost same as existing system. Fig 5 shows a very slight increase in overhead at 90 nodes for proposed as compared to existing system.

D. False Positive

False Positive is the ratio of all sybil nodes that are identified as genuine nodes to that of total number of sybil nodes. It is computed by using the following equation:

FP = Total number of sybil nodes identified as genuine / Total number of sybil node (4)

In existing system, sybil attack is detected only when an event occurs that is when an event has not occurred the attacker is not detected which means attacker is considered as genuine until an event occurs and detected by RSU. There is a possibility that attacker can compromise an RSU so that RSU cannot detect the attacker. Hence false positive is high. In SAD-V-DTC protocol, trust values are calculated at regular intervals. Sybil nodes are checked at regular intervals by pinging the neighboring nodes with HELLO Request packets. Hence the number of attackers detected in proposed system is higher as compared to existing system from Fig 6. The advantage of proposed system lies in selecting times interval for Direct Trust Calculation. If the time interval selected is higher then there is a possibility of considering a sybil node as genuine node. Hence proposed system is still vulnerable to false positive cases. SAD-V-DTC is 65.80% better than existing system.

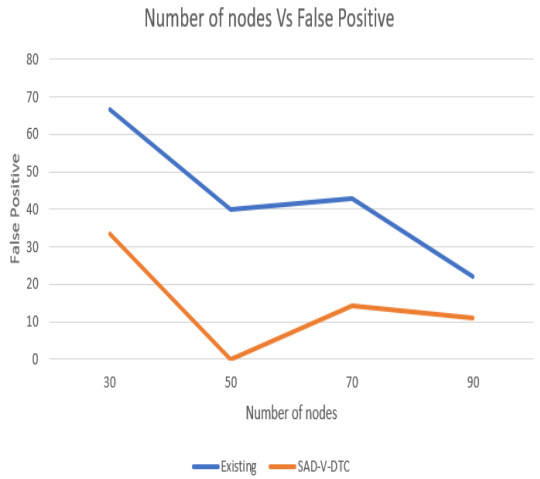

Fig. 6. Number of nodes Vs. False Positive

V. CONCLUSION

Security in VANETs is a hot research topic in the present days and is continuously worked upon to make the security system more robust. Out of many attacks that affect VANETs, the proposed system considers sybil attack. The SAD-V-DTC protocol has made an attempt to detect the sybil node faster than the existing system. The direct trust calculation module continuously monitors the system at regular intervals in addition to the former location certificate method to identify the sybil node for effectively. The direct trust calculation involves monitoring of simple count calculation of hello request and reply packets between the source and its neighboring nodes. Parameters like attack detection ratio, packet delivery ratio, normalized routing overhead and false positive are compared to prove the efficiency over the existing system. The existing and proposed system are compared by testing the parameters at 30, 50, 70 and 90 node densities. From the experimental results, it is proven that the attack detection ratio of SAD-V-DTC is 5 times better than that of the existing system due to the introduction of direct trust calculation. The packet delivery ratio of SAD-V-DTC is 27.27% better than existing system since the sybil node is detected quickly and the data is transmitted to the right node. The normalized routing overhead remains almost same except for negligible increase at 90 nodes since the direct trust calculation does not involve any complex calculation. There is also an improvement of 65.80% of false positive in SAD-V-DTC as compared to the existing system.

The main intent of higher attack detection of sybil nodes is achieved in SAD-V-DTC. Also, there is improvement in packet delivery ratio and false positive. The project intends to extend the proposed protocol to real time scenario to compare the theoretical and practical values. There is scope for testing other parameters like latency, throughput, packet drop when the number of nodes is very high. The project can be further fine-tuned to improve attack detection ratio by considering other parameters in the system.

REFERENCES

1. A. Luckshetty, S. Dontal, S. Tangade and S. S. Manvi, "A survey: Comparative study of applications, attacks, security and privacy in VANETs," *2016 International Conference on Communication and Signal Processing (ICCSP)*, IEEE, Melmaruvathur, 2016, pp. 1594-1598.
2. H. Hamed, A. Keshavarz-Haddad and S. G. Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," Iranian *Conference on Electrical Engineering (ICEE)*, Mashhad,2018,pp.602-606.
3. T. Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty, "P2DAP — Sybil Attacks Detection in Vehicular Ad Hoc Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582-594, March 2011.
4. S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103-1114, June 2012.
5. Salam Hamdan, Amjad Hudaib & Arafat Awajan (2019): Detecting Sybil attacks in vehicular ad hoc networks, International Journal of Parallel, Emergent and Distributed Systems.
6. H. Hamed, A. Keshavarz-Haddad and S. G. Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," *Iranian Conference on Electrical Engineering (ICEE)*, Mashhad, IEEE, 2018, pp. 602-606.
7. M. S. Mohamed, P. Dandekhya and A. Krings, "Beyond passive detection of sybil attacks in VANET," *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, IEEE, Noida, 2017, pp. 384-390.
8. Y. Yao *et al*., "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, IEEE, Denver, CO, 2017, pp. 591-602.
9. J. Jenefa, E. A. Mary Anita," Secure Vehicular Communication Using ID Based Signature Scheme," Springer Science+Business Media, 2017.
10. T. M. de Sales, H. O. Almeida, A. Perkusich, L. de Sales and M. de Sales, "A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks," *2014 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, 2014, pp. 426-427.

11. N. Varshney, T. Roy and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth," *2014 International Conference on Communication and Signal Processing*, IEEE, Melmaruvathur, 2014, pp. 768-772.
12. H. Hamed, A. Keshavarz-Haddad and S. G. Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," *Iranian Conference on Electrical Engineering (ICEE)*, Mashhad,2018,pp.602-606.
13. K. Lim, K. M. Tuladhar and H. Kim, "Detecting Location Spoofing using ADAS sensors in VANETs," *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2019, pp. 1-4.
14. S. A. Syed and B. V. V. S. Prasad, "Merged technique to prevent SYBIL Attacks inVANETs," *2019 International Conference on Computer and Information Sciences (ICCIS)*, IEEE, Sakaka, Saudi Arabia, 2019, pp. 1-6.
15. M. Baza et al., "Detecting Sybil Attacks using Proofs of Work and Location in VANETs," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.299

AUTHORS PROFILE

Sunil Kumar V completed his B.E in Information Science from Visvesvaraya Technological University, Karnataka. He is currently pursuing his MTech at Dayananda Sagar College of Engineering, Bengaluru, Karnataka in Computer Science Engineering. His areas of interest include Network Security, Web Application Development, Digital Image Processing and Machine Learning.

Dr. Ramesh Babu D R received his B.E from University of Mysore, Karnataka in 1997, MTech and PhD from University of Mysore, Karnataka in 1999 and 2004 respectively. He is currently Vice Principal and Head of Computer Science Department of Dayananda Sagar College of Engineering. His areas of interest include Algorithms, Image Processing and Computer Vision.