Detection of Sybil Attack in VANETs by Trust Establishment in Clusters

Shivani Kanwar¹, Sandeep Joshi², Manu Sood³

¹²Department of Computer Science and Engineering, Manipal University, Jaipur, India
³Department of Computer Science, Himachal Pradesh University, Shimla, India

ABSTRACT

Vehicular ad hoc networks (VANET) are a class of ad hoc networks built to ensure the safety of traffic. Trust and security remain a major concern in VANET since a simple mistake can have catastrophic consequences. A crucial point in VANET is how to trust the information transmitted when the neighboring vehicles are rapidly changing and moving in and out of range. The main aim of this paper is to detect Sybil attack in VANET. A trust evaluation-based security solution is proposed to provide effective security decision on data protection, secure routing and other network activities. Therefore to overcome Sybil attack we presented trust algorithm for detecting Sybil attacks in VANET.

Keywords: VANET, Cluster, Sybil attack, Trust establishment, Trust computation, Cluster based routing protocol, Security.

INTRODUCTION

A Vehicular Ad-Hoc Network (VANET) facilitates communication between vehicles and between vehicles and infrastructure. Nowadays, road traffic activities are one of the most important daily routines worldwide. Passenger and freight transport are essential for human development. Thus, new improvements in this area are achieved every day - better safety mechanisms, greener fuels, etc. Driving is one of the most incident factors of traffic safety, so there is a clear need to make it safer [1]. Apart from partially automating this task, reliable driver data provisioning is critical to achieve this goal. An accurate weather description or early warnings of upcoming dangers (e.g. bottlenecks, accidents) would be highly useful for drivers. For this purpose, a new kind of information technology called VANET is being developed. In this paper we are detecting Sybil attack in VANET. The cluster based routing protocol is used for broadcasting and the highest degree clustering algorithm is used for cluster head selection in a cluster. The paper is organized as follows: Section 2 describes the work that has been done on detection of attacks using trust approach. Section 3 describes the proposed algorithm and the work related to it. Section 4 describes the results of proposed algorithm. Finally, Section 5 concludes the paper.
[2] RELATED WORK

[2.1] TRUST ESTABLISHMENT AND COMPUTATION IN VANET

The main objective of this paper is to detect Sybil attack in cluster based VANETs. Node to node system commonly relies on the existence of multiple independent remote entities to mitigate the threat of hostile nodes. Sometime single faulty node can produce various identities leading to control of substantial fraction of the system. These attacks are called Sybil attacks. Since few years, Vehicular Ad hoc Networks deserve much attention. In an ad hoc network, each node should not trust any peer. However, traditional cryptographic solution is useless against threats from internal compromised nodes. Thus, new mechanisms are needed to provide effective security solution for the ad hoc networks. A trust evaluation based security solution is proposed to provide effective security decision on data protection, secure routing and other network activities. Logical and computational trust analysis and evaluation are deployed among network nodes. Each node’s evaluation of trust on other nodes should be based on serious study and inference from such trust factors as experience statistics, data value, intrusion detection result and references of other nodes, as well as node owner’s preference and policy. In order to prove the applicability of the proposed solution, we used Cluster based routing protocol and analyze its security over Sybil attack.

Pirzada and McDonald in [2] describe how to compute the trust in pure ad-hoc networks. Trust computation involves an assignment of weights (representing utility or importance factor) to the events that were monitored and quantified. The assignment is totally dependent on the type of application demanding the trust level and varies with state and time. All nodes dynamically assign these weights based upon their own criteria and circumstances. These weights have a continuous range from 0 to +1 representing the Significance of a particular event, from unimportant to most important. The trust values for all the events from a node can then be combined using individual weights to determine the aggregate trust level for another node. We define this trust $T_i(y)$ in node $y$, by node $x$, as $T_i(x)$ and is given by the following equation:

$$T_i(y) = \sum W_i \times T_i(x)$$

Where, $W_i$ represents the weight of the $i^{th}$ trust category of node $y$ to node $x$ and $T_i(x)$ is the situational trust of node $x$ in the $i^{th}$ trust category of node $y$. The total number of trust categories $n$ is dependent on the protocol and scenario to which the trust model is being applied.

The distributed trust model proposed by Liu et al. in [3] makes use of a protocol to exchange, revoke and refresh recommendations about other entities. By using a recommendation protocol each entity maintains its own trust database. This ensures that the trust computed is neither absolute nor transitive. The model uses a decentralized approach to trust management and uses trust categories and values for computing different levels of trust.

Chauhan and Mahajan in [4] propose how to compute the global trust of the target node depending on its neighbour’s recommendations and their trust levels.

[3] PROPOSED WORK
[3.1] CLUSTER BASED ROUTING PROTOCOL

Cluster Based Routing Protocol (CBRP) is the hybrid routing protocol that ensure highly stable network. Some of its advantages are listed below:

• Higher Packet delivery ratio
• Avoid routing overhead
• Lesser network traffic as inter-cluster communication can be reduces to cluster head and gateway nodes
• Minimal information stored and propagated in the network
• Communication scalability for large number of nodes
• Help in route maintenance and route shortening

[3.2] HIGHEST DEGREE CLUSTERING ALGORITHM

The highest degree clustering algorithm is used for cluster head selection within a cluster. In highest degree heuristic [5], each node periodically broadcast its connectivity value to its neighbors and compares its connectivity value with them. Each nodes broadcasts HELLO messages to all the nodes that are within transmission range so as to discover the number of neighbors that each of them have. A node having the highest connectivity value (maximum number of neighbors) becomes the cluster head. If there is a tie between two or more nodes in terms of node degree, the node with lowest ID is chosen to be clusterhead.

![Figure: 1. Formation of Clusters during Highest Degree Clustering Algorithm](image)

Figure [Figure-1] shows formation of cluster when highest degree clustering algorithm is implemented. The nodes 7 and 3 are elected as cluster head due to the maximum node degree in the respective clusters. The node 6 that lies on the intersection between the two nodes represents the gateway node and the rest nodes(1,2,10,4,5,9,8,11) represents the member nodes.

[3.3] SYBIL ATTACK IN VANET
The Sybil attack is the case where a single faulty entity, called a malicious node, can present multiple identities known as Sybil nodes or fake nodes. This attack can affect the functionality of the network for the benefit of the attacker. Sybil attacks are also capable of disrupting the routing mechanisms in vehicular ad hoc networks.

Sybil attack was first introduced by J. R. Douceur in [6]. According to Douceur, the Sybil attack is an attack in which a single entity can control a substantial fraction of the system by presenting multiple identities. [Figure-2] shows an example of Sybil attack where malicious node introduces multiple fake identities s1, s2 and s3. These multiple identities are known as Sybil identities.

![Figure: 2. Sybil Attacker with Multiple Identities](image)

Sybil attacks can incur great security threats to VANETs:
1. In Sybil attack, a malicious node creates an illusion of the traffic congestion by claiming multiple identities. A greedy driver may convince the neighbouring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination [7].
2. Sybil nodes may directly or indirectly inject false data into the networks, greatly impacting on the data consistency of the system. For example, VANETs may rely on multiple vehicles voting to generate a traffic status report. However, if some of the voters are Sybil vehicles, the report may be deviated from the fact, depending on the benefits of the malicious.
3. Sybil attack can also launch DoS attacks such as channel jamming attacks and message suppression attacks.

[3.4] TYPES OF SYBIL ATTACK

Sybil attack can disrupt the network or steal the identity of other nodes through several ways. Newsome et al. in [8] describe the types of Sybil attacks that can occur in a network. [Figure-3] represents the different types of Sybil attack.
[3.4.1] DIRECT OR INDIRECT COMMUNICATION

In direct communication is between the legal node and the Sybil node. The malicious node allows nodes to communicate with neighbouring legitimate nodes. Indirect communication is between the legal node and copy of the Sybil node. The malicious node does not allow the Sybil nodes to communicate directly with the neighbouring nodes. The malicious node vary the transmission power the Sybil nodes, so that it do not join the other legitimate nodes.

[3.4.2] STOLEN OR FABRICATED IDENTITY

Stolen identity is that identity in which the malicious node takes from the legitimate node and uses for attack. It cannot be identified or find if the legitimate node is destroyed. Fabricated identity is that in which the malicious node or the copy node takes the identity from legitimate node or we can say use the same exact identity as that of legitimate node. This is known as identity replication in which same identity is used many time in a same network.

[3.4.3] SIMULTANEOUS AND NON SIMULTANEOUS ATTACKS

In simultaneous attack, all the copy nodes or the Sybil identities participate at the same time, but since they have only one identity so this simultaneous attack is supported by the cycling of identities between all nodes. Non-Simultaneous attacks are those in which the attacker uses the same number of identities equal to number of devices.

[3.5] THE DETECTION ALGORITHM

The detection algorithm of the Sybil attacks in VANET is done by using a security system based on trust management that involves developing a trust model, assigning credentials to nodes, updating private keys, managing the trust value of each node, and making appropriate decisions about nodes access rights. We have taken VANET scenario where Road Side Unit (RSU) is not available. If malicious node becomes cluster head, then it can control and disrupt the network. The main advantage of the proposed scheme is malicious will not be allowed to become cluster head. Trust is an important aspect in the design and analysis of secure distribution systems. The communication success through some node will increase the trust index of that node. The communication failure through that node will
DETECTION OF SYBIL ATTACK IN VANETS BY TRUST ESTABLISHMENT IN CLUSTERS

decrease the trust index attached to that node. Just like human being's communications, the trust we established on one person is generally based on the proportion of communication success and the level of satisfaction.

The detection is carried out in Cluster based routing protocol (CBRP) where the cluster head contains the trust database and the information about all the nodes within the cluster. The node trust value is updated on the trust database every time the trust value of a node increases or decreases. The detection procedure of the Sybil attack is the following:

1. Vehicles with Unique Id and Master Key are registered in cluster head.

2. Vehicles generate anonymous Id and send it to the cluster head to which vehicle X belong.

3. Cluster head validate anonymous Id of vehicles X in trust table.

4. Vehicles X and local cluster head generates trust value (based on timestamp). They generate vehicle X trust value with the Session Key.

5. Vehicle X sends the trust value based on Session Key and message hash value to vehicle Y.

6. Vehicle Y validates vehicle X’s Id by requesting vehicle X trust value based on Session Key to local cluster head.

7. If authentication of vehicle X trust value based on Session Key is not correct it is taken into account that a certain vehicle attacked Y after stealing vehicle X’s Id and it is called Sybil attack. If vehicle Y detects the Sybil Attack it sends the result to the Cluster Head and to the Base station. After that it will send to the destination. If vehicle X’s Id validates vehicle Y, which receives vehicle X message makes Hash Value with a message integrity is validated by comparing vehicle y hash value to the hash value which vehicle X sent.

8. Vehicle Y validates the position which vehicle X sends and vehicle Y checks whether vehicle X is on the same location as other vehicles. If the roads are overlapped on a boundary the position must be selected in the light of vehicle direction.

[4] RESULTS

Simulation environment is created on wireless network topology and implemented with cluster based routing protocol. VANET topology is created with 50 vehicles and existing protocol is used to transfer message from one node to other. The circle represents the node coming in range of each other and becoming neighbours exchanging messages among them. [Figure-4] depicts the VANET Mobisim.

VANET topology is created considering 50 vehicles and Sybil attack is implemented on highest degree clustering algorithm using cluster based routing protocol to transfer message from one vehicle to another vehicle. [Figure-5] represents the NAM file of the Sybil attack in VANET. The malicious node introduces the multiple Sybil nodes and attempts to disrupt the network. The black node represents the malicious node, the blue node represents
the gateway node between the clusters and the green nodes represent the member nodes of the cluster.

Figure: 4. VANET Mobisim

Figure: 5. Nam File of Sybil Attack
[4.1] PERFORMANCE ANALYSIS OF PROPOSED SYSTEM

Three performance metrics are considered: Packet delivery ratio, End to End delay and throughput. They are measured for Sybil attack detection algorithm using trust calculation.
The graphs in [Figure-6], [Figure-7] and [Figure-8] shows the comparison of the three performance metrics namely Packet Delay Ratio, Throughput and End-to-End Delay respectively between Sybil attack and TrustCBRP. [Figure-6] shows that with the increase in simulation time, the packet delivery ratio also increases in case of TrustCBRP whereas it decreases in case of Sybil attack. [Figure-7] depicts that with the increase in simulation time, the throughput is also increasing in case of TrustCBRP and decreasing in case of a Sybil attack. Finally, [Figure-8] shows that with the increase in simulation time, the end-to-end delay is decreasing in TusrtCBRP and increasing in case of a Sybil attack.

[5] CONCLUSION

VANETs are facing a number of security threats, which might impair the efficiency of VANETs and even life safety. One of these threats is Sybil attacks, in which a malicious vehicle creates illusion of traffic congestion by claiming multiple identities. We propose a security system based on trust management that involves developing a trust model, assigning credentials to nodes, updating private keys, managing the trust value of each node, and making appropriate decisions about nodes access rights. Through the presentation of a formal security analysis of the trust system, we verify that the stated goals are achieved and that malicious nodes can be effectively excluded from ubiquitous and pervasive computing environments. The present study was conducted using Network Simulator for detecting Sybil attack in VANET. The simulation results show that our algorithm is effective in the detection of malicious nodes in VANET. The probability of malicious to become cluster head is less in our proposed scheme. Finally the comparison is done based on the performance analysis between the Sybil attack and proposed detection algorithm.

REFERENCES


Author[s] brief Introduction

Ms. Shivani Kanwar is pursuing M.Tech in Computer Science and Engineering from Manipal University, Jaipur( Rajasthan), India

Dr. Sandeep Joshi is currently working as Associate Professor in the Department of Computer Science and Engineering, Manipal University, Jaipur( Rajasthan), India

Dr. Manu Sood is currently working as Professor in the Department of Computer Science, Himachal Pradesh University, Shimla(Himachal Pradesh), India

Corresponding Address-

Shiva cottage, near dav school, Sunny side, Solan(H.P.)

Pin-Code: 173212