DIGITAL SIGNATURE APPROACH FOR TRUST BASED COMMUNICATION OVER SELFISH NODE ATTACK IN VANET

P.Prittopaul\textsuperscript{1}, M.Usha\textsuperscript{2}, Vignesh CS\textsuperscript{3} and Eswaran VA\textsuperscript{4}

ABSTRACT: Security and safety in vehicles’ is gaining more and more priority as the number of accidents and other unfortunate events increase side by side with the number of vehicles being used. VANET is a ad-hoc technology employed by few automobile manufacturers for the same purpose. However, it possess certain drawbacks. Among which is the most common one, Denial of Service (DoS) attack. Many protocols and algorithms have been used to overcome DoS attacks that occur either intentionally or non-intentionally. But the solutions provided to all attacks do not emphasize much on trust between nodes which leads to unauthenticated communication. This paper suggest and demonstrates the usage of Trust based model with the help of Digital signature and Certified Authentication to prevent DoS attacks in an efficient manner. The model is compared and with the existing model and has proved to have an upper hand against the existing model in terms of security and reliability.

Key words- Wireless Sensor Networks, Trust value, energy efficiency, VANET.

I. INTRODUCTION

VANET is a new generation of technology where Ad hoc concepts are applied to vehicular field to provide safety and security to the travelers. It does not employ any infrastructure based components to transfer data packets between nodes. It is a dynamic network, formed when a group of vehicles come together sharing status messages of themselves with all other vehicles in the network. The message transmitted may consist of the vehicle’s speed, acceleration, traffic details, etc. VANET comprises of two types of communication.

\begin{itemize}
  \item \textbf{V2V}(Vehicle to Vehicle)
  This takes place between the smart Vehicles without any link to the infrastructure.
  \item \textbf{V2I}(Vehicle to Infrastructure)
  The nodes are connected to the infrastructure with the help of the road side units that serves as a mediator between the server, internet, etc. and the vehicular nodes.
\end{itemize}

VANETs are gaining more and more attention and importance in the last couple of years as it has a high potential to serve as the base for a new technology that provides an efficient travel scenario by enhancing the travel quality and safety along the nodes providing comfort to passengers and drivers.

1.1 Road Side Unit

RSU units are components placed every 300-400 meters along the sides of the road that serves as an access point to the server and internet for the vehicular nodes. The road side unit has several other functions such as storing location of the nodes that frequently broadcast their status messages, providing authentication in the communication between the nodes, etc. The road side unit are themselves connected with each other via the infrastructure. The communication between the vehicles and the road side unit is called as vehicle to Infrastructure.

\textsuperscript{1} Dept of CSE, Velammal Engineering College, Chennai, India
\textsuperscript{2} Dept of CSE, Velammal Engineering College, Chennai, India
\textsuperscript{3} PG Student, Dept of CSE, Velammal Engineering College
\textsuperscript{4} PG Student, Dept of CSE, Velammal Engineering College
communication. Road side units in short exploit the infrastructure on behalf of the VANET nodes to improve the network performance.

1.2 Security in VANET

The VANET, like any other network is prone to external attacks either intentionally or intentionally. Despite the strong structure of the network, the fact that any node can enter and exit the network and can also influence the packet transmission attracts a lot of attention on the security issues of VANET arousing a need for standard security metrics development. Standardized security measurement builds consumer confidence towards VANET measurement builds consumer confidence towards VANET applications and assures predictability as well as applications and assures predictability as accountability for a VANET security mechanism.[2] Enrique Alba, Sebastian Luna, and Jamal Toutouh, “accuracy and efficiency in simulating VANETs” on 04 March 2016. In this article they have measured the differences between the Simulation versus the real results with actual moving cars in order to quantify the accuracy of the VANET simulations inside the EuropeanCARLINK Project[1]. Vinh Hoa LA and Ana Cavalli “security attacks and solutions in vehicular ad hoc networks: a survey”, International Journal on Ad hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes [1]. Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan, “Enhancing Security and Privacy for Identity based Batch Verification Scheme in VANET” The proposed IBV scheme provides the provable security in the random oracle model. In addition, the batch verification of the proposed scheme needs only a small constant number of pairing and point multiplication computations, independent of the number of messages. We show the efficiency merits of the proposed scheme through performance evaluations in terms of computation delay and transmission overhead. Moreover, the extensive simulation is conducted to verify the efficiency and applicability of the proposed scheme in the real-world road environment and vehicular traffic [9]. Security issues and challenges of Vehicular Ad Hoc Networks (VANET) VANET facing many challenges that been addressed in this research, they have also discussed a set of solutions presented for these challenges and problems; and they made critics for these solutions and proposed suitable solutions for some of the problems on security issues in VANET[3].

II. TRUST IN VANET

Security in VANET is a major area of concern as the nodes in the network as susceptible to attack from both insiders and outsiders. Many cryptographic algorithms were made available for tackling the attacks and providing enhanced security in communication domain but these algorithms are not enough to fight against attacks in wireless sensor networks. Identifying malicious nodes and selfish nodes inside a network cannot be done by the Cryptographic mechanisms and are useless to attacks from the inside. It does not provide additional security or no explicit rules to protect each node and also no enhancement of distributed data gathering and collaborative data processing in networks[4]. The main purpose of the trust model is to enhance the overall performance by monitoring network activities, minimizing the risk and ensuring the network activities of entity such as data gathering and data processing. This trust model is required to find malicious, selfish and compromised insiders by evaluating trust worthiness of sensors in the network [4].

- Computation of Trust

A trust value has to be calculated for every node before it can be authenticated to participate in the network. The trust of a node can be calculated can be calculated using three parameters which are i) Experience: The history of previous successful transmission by or through the node which is stored in a table that each node possess. ii) Recommendation: i.e. The broadcasting of the experience table throughout the network. iii) Knowledge: The Knowledge about the previously calculated trust value. The calculation of Trust can be either Centralized or distributed.

- Centralized Trust Establishment

Centralized trust establishment scheme assumes a trust agent (TA) that can be accessible by all nodes in the group. Trust Agent can either compute trust for the whole network or can assist nodes in their trust computation by providing initial trust value on target nodes. A centralized cluster head based trust computation works as follows. The cluster head provides every node in the cluster with the initial trust value on every other node. Each node will combine its own calculated trust value based on experience with the initial trust value obtained from the cluster head [4].
Distributed Trust Calculation

2.1 Direct Trust: Every node observes their neighbors for their event reports and stores the reports in their knowledge cache. A trustor node (trust measuring node) compares its own observation report on event with the observation report it received from the trustee node. Trust factor is determined based on the amount of deviation between the observation reports [4].

2.1.1 Recommendation based Trust: Trust relationships on nodes are established based on recommendations alone. Every node will monitor its one hop neighbor nodes and generate a “trust report” based on the neighbor nodes’ behaviour. Initially all nodes will have a random unknown trust level on other nodes. Once the trust report is generated it will be either broadcasted to all nodes or it can be flooded controllably in the network [4].

2.1.2 Hybrid Method: Trust on a node is computed based on direct experience and also recommendations from other nodes [4]. Since we are dealing with a dynamic system we will concentrate only on the distributed trust calculation.

III. PROPOSED MODEL

In the existing work, no emphasis is laid on the confidentiality and authentication issues that might occur in data transmission in a VANET network. The Stochastic automata network technique used in the existing model requires calculation of the distance of each of the node with its neighboring node. Hence for each addition and deletion of nodes from the network, each node will have to change their table content and one can easily understand the difficulty involved if there are hundreds of vehicles moving in the same direction. Besides, No authentication mechanism is provided which results in the consequence of any node entering into the network without any permission and transmitting messages with other genuine nodes. This is indeed a very serious issue as it might result in scrambling or loss of important data. And the usage of Markov chain to calculate the distance of each of the nodes might drain away the energy resource of the nodes which in turn may cause the issue of selfish node attack on the network. Thus, security concerns are not given enough importance in the existing model which we look to tackle in our proposed model.

The problems discussed above are tackled in our idea by making two changes and introducing a security concept in it. Initially, instead of Markov chain model, we make use of LAR protocol combined with Global Positioning system which avoids the need to calculate the distance by directly obtaining the position of each node using GPS and then deciding the node near by. Then we make use of a trust model to create a trust between the nodes before transmission occurs so that any ineligible node is identified to be capable or incapable of transmission prior to it by making use of certain parameters the node has broadcasted.

Another concept introduced is the use of Digital Signature standard approach for data transmission. The advantage of DSS approach is that it is an Asymmetric Encryption technique and that is session oriented. The usage of Multiple keys makes it harder for external attacker to hack into the network and gain access to authenticated data packets. By implementing these three concepts in the VANET system, the delay which was earlier observed in the existing model is reduced a little. The throughput though is very similar to the existing model shows a very small increase which can be further enhanced in the future.

3.1 Proposed Architecture

System architecture is usually a high-level architecture depicting the system entities involved in the system. The Figure displayed below depicts the system model along with the protocol and encryption techniques being used for the proposed work. The Architecture diagram gives a front end view about how the nodes and other components are connected with each other in the VANET system.

![Figure 4.1 Proposed Architecture Model](image-url)
Ad hoc wireless networks employed in Vehicles provide a scenario where vehicles moving along a path can communicate with each other without any access points or infrastructure based components. The System architecture model displayed above gives an overview of interlinking between various components present in the general VANET system and the proposed system.

The proposal consists of four modules which are listed below
(i) Formation of vehicular Network Model
(ii) Trust based model.
(iii) Digital signature standard approach.

3.1.1 Formation of vehicular Network Model
The nodes in a VANET are dynamic in behavior and mobility and hence do not possess a fixed topology. So we consider a dynamic topology for the nodes. The nodes broadcast their status messages to the nearby nodes on a regular basis. Each vehicular node is connected to the road side unit. The road side unit is an infrastructure oriented component placed every 300-400 meters along the sides of the roads providing functions such as storing the location of the nodes that have been established during communication, Granting authentication during communication between nodes and connecting the nodes to the internet or any other infrastructure. Location Aided Routing protocol with the help of Global Positioning system has been used to obtain the location of the nodes avoiding the need for calculation of distance and hence the location of every node at every instance of communication.

3.1.2 Trust based model
Identification of malicious nodes helps in avoiding the routing of packets to malicious nodes and in providing authentication to suitable nodes. In the proposed system, the authentication process, the permission for a node to participate in a communication is done using a Trust parameter. Two nodes that are to communicate with each other must initially create a trust between them to notify the other that it is worthy of data transmission and packet forwarding. Various trust parameters have been suggested by many authors but we choose three parameters that are considered effective in our view.

(i) Energy Level of the nodes: The energy level of the destination node should be greater than or equal to a threshold value that has been calculated or assigned for the network. Or else the node is considered not trustworthy.
(ii) Time in the network: To make sure that a node is not an external attacker and that the node belongs to the network, every node must spend enough time in the network which is indicated by a directly calculated or assigned Timestamp.
(iii) History of previous successful transmission: When there are two or more nodes that have satisfied the above two parameters, a third parameter i.e. the number of previous successful transmission by and through the node is calculated and the node that higher value in this is given the priority.

When all this three parameters have been met, a trust is created between the two nodes that are about to communicate with each other.

3.1.3 Trust based Digital Signature Standard
After the nodes have been given authentication, there is a great necessity to ensure integrity and security during data packet transfer. Powerful encryption technique is required for this purpose. Asymmetric encryption supported by Digital certificates suffices these requirements very well. The road side unit serves as the Certified Authenticator for this process connecting the nodes to the server providing certificates and public keys to the node. Since two keys are involved in the process, decryption of the data packets by a third unauthorized party is prevented to a large scale. Another major advantage of Digital Signature Standard procedure is that it is session oriented and because of this, the security features are further enhanced.

a. steps in Trust based DSS approach
Step 1: When a node N1 wants to send a message to node N2, It intimates the CA providing its Identity-1/Request/Timestamp.
Step 2: The CA receives it and by decrypting the request identifies the destination node and gives the public key of the node N2 to node N1.
Step 3: The node N1 using the public key encrypts the request message and sends it to node N2
Step 4: Node N2 receives the message and sends a packet to CA comprising of Identity-2/Request/Timestamp. The RSU unit gives a certification for the node N1 and its trustworthiness for data exchange
Step 5: Node N2 sends and acknowledgement to Node N1. At this point, a Handshake is said to have been occurred.
Step 6: The messages are then transferred by encrypting with the public key and decrypting with the private key.
IV. PERFORMANCE EVALUATION

The throughput though is comparatively steady for the proposed system unlike the existing system that shows a rise in the graph initially and then maintains a steady state after a minor drop. The steadiness in the proposed system is because it uses Asymmetric encryption technique that takes constant time for authentication providing procedure for every node. However it more than makes up in the security features it provides.

![Comparison of Throughput with Proposed Work](image)

It can be seen from the graph 1, the delay in existing system is high mainly because of the stochastic automata technique used in calculation of the routing protocol. The calculation requires updating the routing table frequently and as the No of nodes increases, the amount of time taken becomes awfully high causing much delay in the routing.

![Delay in Existing System](image)

![Delay in Proposed Work](image)

V. CONCLUSION

As movement of people from place to place on a regular basis increases, they look for safety and security in their travel. Seeing the technology takes leap after leap, they expect a lot from these to protect them from any kinds of danger including the ones they meet on roads. VANET, though is an excellent invention to serve this purpose, still needs a long way to go before they can earn the trust of the people. Along the process comes or proposal wherein we use a trust based model with the highly regarded Digital Signature Standard approach in a VANET network. Because of the usage of Location Aided Routing Protocol, the latency caused due to distance calculation has been avoided. Adopting Trust based model in node authentication prevents participation of ineligible node and maintains continuity in message passing through the network. Since DSS mechanism is session oriented and Asymmetric, it is secure from external interface or hacking and messages are safely transmitted between the nodes. The trust based model along with the DSS approach has proven to improve the communication between two VANET nodes in terms of Authentication and confidentiality.
REFERENCES

[5] Young-Bae Ko and Nitin H. Vaidya ,“Location-Aided Routing (LAR) in mobile ad hoc networks”
[8] Enrique Alba, Sebastian Luna, and Jamal Toutouh, “accuracy and e£ciency in simulating VANETs” on 04 March 2016
[9] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan, “Enhancing Security and Privacy for Identity- based Batch Verification Scheme in VANET”