Detection of Insider and Outsider Attack using Holistic Protocol in Vehicular Ad Hoc Networks

M.sharmila mari[1], M.Ponnrajakumari[2]
PG Scholar, Department of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India[1]
Assistant Professor, Department of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India[2]

***Abstract*— VANETs are an emerging research area and currently research on security is ongoing in wireless technology. Which includes solving the traffic related problems and provides safety for life's of people. Attackers could be able to reroute traffic if they insert malicious messages into traffic information systems. Knowledge able attackers will be able to access key material in vehicles they physically own. Using the obtained keys, attackers can generate wrong information or modify information .To strengthen the security and to detect the insider attack, we use Multi-hop data dissemination protocol to address the vulnerability inherited by the vehicular ad hoc network. This technique includes self reconfigurable concept in which if an attack is detected in a path then an alternate path is provided for the data transmission which is done by piggy backing messages To enhance the security level in the VANET, HOLISTIC PROTOCOL has been developed using HIDDEN MARKOV MODEL and TRUST AWARE methods. Our simulation results show that our scheme highly detects and avoids the insider and outsider attack.**

***Index Terms*— Vehicular ad hoc networks, Self-reconfigurable technique, Attacks in vanet, security, protocol analysis.**

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is highly dynamic version of (MANET), this means that every node can move freely within the network coverage and stay connected.

Vehicular Ad hoc Networks offer a wide range of applications including solving traffic related problems, safety and comfort for passengers.

In VANET inside vehicle need only small electronic device, which will provide Ad-Hoc Network connectivity for the passengers inside the vehicle. By this device operating the network does not need complicated connection and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. The existing approaches do not consider VANET protocols. Due to the focus on non malicious failure, the presented approaches usually consider the basic network connectivity when calculating the proposed metrics. To overcome this we have modified the graph based metrics for the performance evaluation. Attackers could be able to reroute traffic if they insert malicious messages into traffic information systems. Hence, cryptographic signatures cannot guarantee that messages contain correct information in networks mainly in multi-hop protocols.

The main Objective is to detect insider attack and provide an alternative path for the data transmission and then to develop a holistic protocol using trust aware routing and hidden Markov model for detecting insider and outsider attack. Combining two different platforms into a unique known as holistic so Trust aware can detect and avoid both the attacks and then hidden Markov model is used for fast and efficient dissemination of safety messages in vehicular networks.

II. MODIFIED GRAH BASED METRICS

Using graph theory we calculate the metrics in which an algorithm is developed using the self reconfigurable technique. Graphs are similar to trees except they do not have as many restrictions. Every tree has a root node, and all the other nodes in the tree are children of this node. Nodes can have many children but only one parent. When we relax these restrictions, we get the graph data structure Notice that our graph does not have a root node like the tree data structure did. Instead, any node can be connected with any other node. Nodes do not have a clear parent/child relationship like we saw in the tree. Instead nodes are called neighbors if they are connected by an edge. For example, node A has three neighbors: B, C, and D. Imagine the graph data structure could be useful for representing data. Perhaps each of the nodes above could represent a city and the edges connecting the nodes could represent roads. Or we could use a graph to represent a computer network where the nodes are workstations and the edges are network connections. Graphs have so many applications in computer science and mathematics that several algorithms have been written to perform standard graph operations such as searching the graph and finding the shortest path between nodes of a graph.

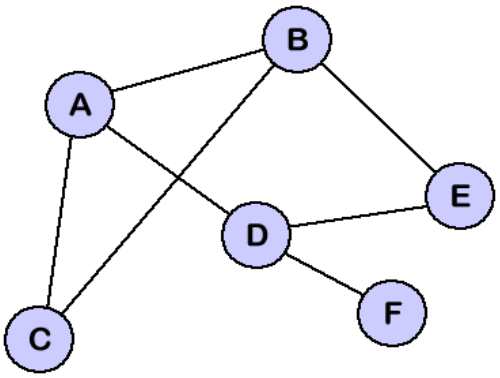

Fig. 1 Logical Representation of Typical Graph

III. Detection Of Insider Attack

A. Insider Attack

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.

Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks. An insider attack is also known as an insider threat.

B. Problems with Insider Attack

This noisy attack could have easily been detected if the network administrators had utilized an internal IDS system. IDS could have not only detected the attack, it could also have allowed administrators to learn of vulnerable services, and figure out who the attacker really was. Insider Attacks are an unusual type of threat. Unlike external attacks, the intruder is someone who has been entrusted with authorized access to the network. In fact, the attacker requires access in order to fulfill their obligations to the victim organization. Furthermore, they often have a substantial amount of knowledge about the network architecture, including where their targeted files or systems are located. Because many organizations' security is focused on protecting the perimeter of the network, little attention is paid to what is occurring within the system. As a result, insider attacks may not be discovered for months after the attack, long enough for the perpetrator to get off scot-free.

C. Piggybacking scheme

To strengthen the security and to provide reliability of the data transmission, the piggy backing messages is used to provide reliability and reduce number of retransmission. To strengthen the security and to provide reliability of the data transmission, the piggy backing messages is used to provide reliability and reduce number of retransmission. Vehicles are assumed to be equipped with Global Positioning System (GPS) receivers. Periodic beacon messages are exchanged to update the vehicles' local topology knowledge. The position of the sender is included within the beacons, which suffices to calculate a CDS backbone after each beacon message round. The source node transmits the message. Upon receiving the message for the first time, each vehicle initializes two lists: list R containing all nodes believed to have received the message (according to local knowledge gained via beacons), and list N containing those neighbors in need of the message. Then, each receiving node sets a time-out waiting period. If a node is not in the CDS, then it selects longer time-out than the nodes from the CDS, so that the latter reacts first. . For each further message copy received, and its own message sent, every node updates R, N, and the time-out. At the end of the time-out period, it transmits if N is nonempty. Both ways, the message is buffered until it expires. For each beacon message received, N and R are updated according to the presence or absence of acknowledgment.

Nodes that are no longer one-hop neighbors are eliminated from these lists. Regardless of previous decisions, all nodes that so far received the broadcast message check whether N becomes nonempty. If so, they start a fresh time-out. In addition, acknowledgments of received broadcast messages are piggybacked to periodic beacons. Nodes those were included in R because they were believed to have received the message, but did not actually get it, are later removed from R and inserted into N. This algorithm is executed for each different message.

D. Implementation of self reconfigurable technique

Self-reconfiguration is a technique using which configured logic can quickly modify itself at runtime to suit application required.

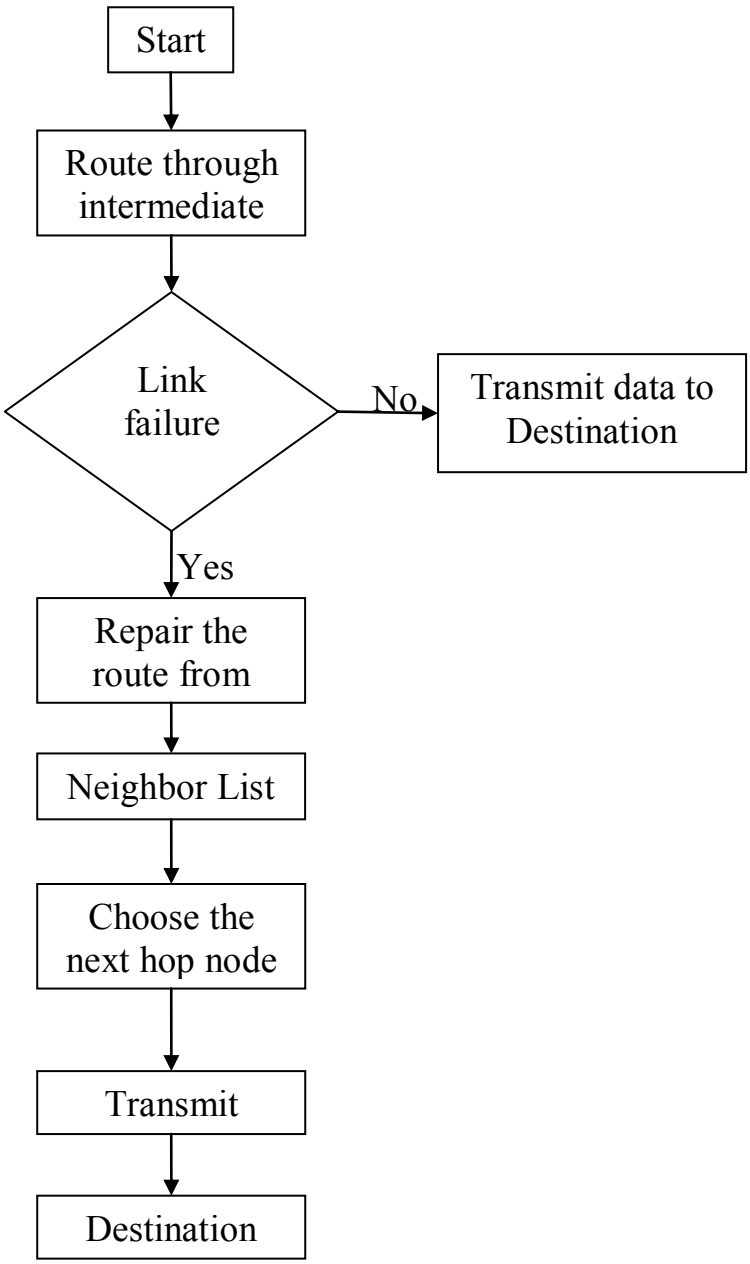

Fig. 2 Flow chart of self reconfigurable technique

Although performance improvements using self-reconfiguration have been demonstrated, the technique itself

has been only informally described. Based on an abstract reconfigurable device model, a precise definition of self-reconfiguration is presented in this paper.

Self-reconfiguration is found to require significantly lesser area as well as significantly lesser time compared to the attached processor approach. An algorithm is developed for

implementation. The process of self reconfigurable technique is explained in the flow model, which describes the transmission of data in case of link breakage. Data are transmitted in a route in case of any link breakage then it repairs the route from the neighbor list and hops to next route and achieves the destination.

IV. HIDDEN MARKOV & TRUST AWARE

A. Hidden markov model

Hidden Markov Models (HMMs) are learnable finite stochastic automates. Nowadays, they are considered as a specific form of dynamic Bayesian networks. Dynamic Bayesian networks are based on the theory. A Hidden Markov Model consists of two stochastic processes. The first stochastic process is a Markov chain that is characterized by states and transition probabilities. The states of the chain are externally not visible, therefore "hidden". The second stochastic process produces emissions observable at each moment, depending on a state-dependent probability distribution.

The first step is to check if the laws for Markov chains are fulfilled, that means if it is a Markov process as defined above. If these laws are fulfilled, exemplary models can be structured with the help of the understanding of the relationships between the states of each Markov Model. Deterministic and stochastic characteristics in the process shall be clearly separated. After all of these steps are executed, the technical requirements of the system considered. It is very important to consider the specification of the signal processor in the running device.

B. Trust aware

Using the trust aware routing protocol we can easily detect and avoid both insider& outsider attack in VANET. It provides trust worthy and energy-effective route against harmful attack**.** Vehicular ad-hoc network (VANET) offers a large number of new potential applications. Drivers may benefit from collision warning, road sign alarms and in-place traffic view, and others. This network tends to operate without any infra-structure or legacy client and server communication. However, due to some special properties such as high mobility, network partitioning, and constrained topology, situations in which the network topology changes dynamically are tempting to attackers for various reasons like faked location.comparing metrics such as throughput, packet loss ratio, packet delivery ratio.

V. SIMULATION RESULTS

The coding for the implementation of insider attack detection is been implemented using the ns-2 simulator tool. And the results are obtained as follows. The screenshots of the obtained results are given below.

A. Insider attack detection

In the above screenshots the values that are set to the variable are assigned and configured to the nodes by using $ symbol. Nearly about 31 nodes are generated and each node is assigned as road side unit, source and its destination. In the below screen-shot the insider attack is detected and then an alternative path is made available to reach the destination using self reconfigurable technique.

Fig. 3 Inter-vehicle communication

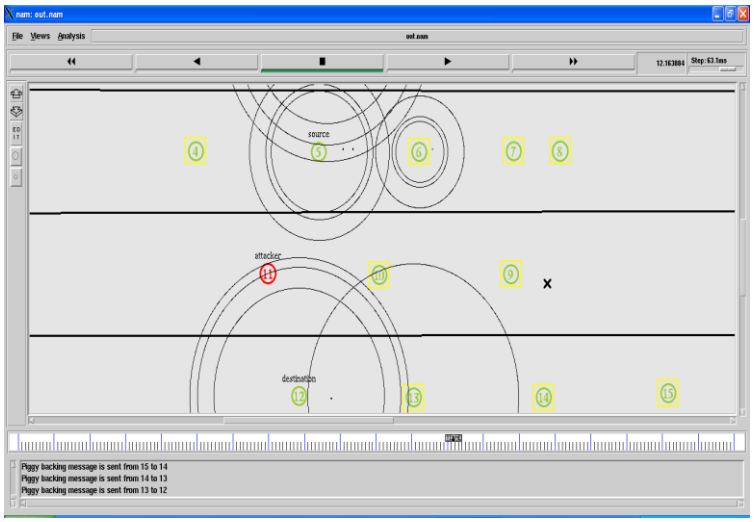

Fig. 4 Attack detection in VANET

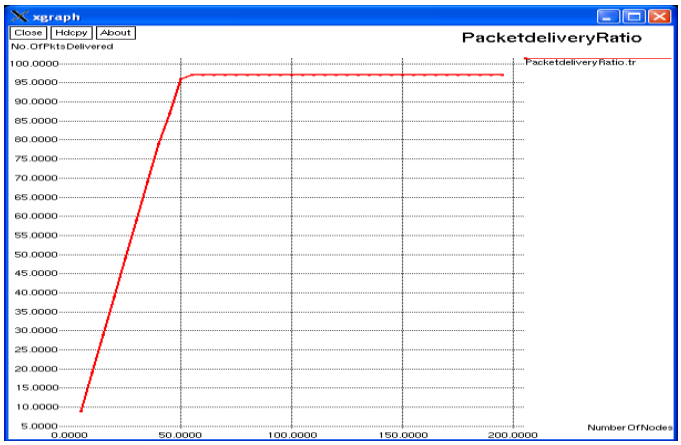

Fig. 5 Screen shot of Packet Delivery Ratio

VI. CONCLUSION AND FUTURE WORKS

Although insider attacks pose some unique challenges for security administrators, they can be detected by various

types of detection systems in VANET. By these systems, attacks can not only be detected, they can also be properly investigated by identifying attack trends and patterns. The piggybacking scheme in multi-hop allow us to accomplish these goals must also be protected against attacks as well, to prevent the corruption of attack data. It is only through identifying attack trends and patterns, and keeping logs un-corrupted. However by the existing method data transferred using piggybacking, and the insider attack is detected using multi-hop data dissemination protocol and then an alternate route is made available using self reconfigurable technique through which the data are transferred in secure. This process has some disadvantages like packet drop .so for overcoming the drawbacks we go for holistic protocol. By which both insider & outsider attacks are detected and avoided for enhance the network security. The holistic protocol will be implemented with probabilistic approaches in future, and the result obtained from the existing method will be compared with the proposed technique and the disadvantages of the present method will be overcome by the future method. Increase in performance evaluation can be shown in graphical representation.

REFERENCES

[1] Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl, "Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols" IEEE transaction of vehicular technology ,vol. 62,no. 4, May 2013.

[2] Nan Zhang, Wei Yu, Xinwen Fu, and Sajal K. Das, "Maintaining Defender's Reputation in Anomaly Detection Against Insider Attacks",IEEE transactions on systems, man, and cybernetics—part-B cybernetics,vol. 40, No.3, June 2010.

[3] N. Bissmeyer, C. Stresing, and K. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *Proc. IEEE VNC*, Dec. 2010, pp. 166–173.

[4] L. Sitanayah, K. Brown, and C. Sreenan, "Fault-tolerant relay deployment for k node-disjoint paths in wireless sensor networks," in *Proc. IFIP WD*, Oct. 2011, pp.1–6.

[5] H.-C. Hsiao, A. Studer, R. Dubey, E. Shi, and A. Perrig, "Efficient and secure threshold-based event validation for VANETs," in *Proc. 4th ACM Conf. WiSec*, New York, 2011, pp. 163–174.

[6] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks" IEEE transactions on parallel and distributed systems, Vol. 21, NO. 9, September 2010.

