Asian Journal of Information Technology 14 (1): 37-41, 2015
ISSN: 1682-3915
© Medwell Journals, 2015

Energy Efficient IDS for Cluster-Based VANETS

K. Indira and E. Christal Joy
Department of Information Technology, Sathyabama University, Chennai, India

Abstract: Vehicular Ad hoc Networks (VANETs) are a foundation of the visualized Intelligent Transportation Systems (ITS). Vehicular ad hoc networks are an easy target to attacks as they run in an open medium and use collaborative strategies for network communications. To acquire a tolerable level of security for Vehicular Ad hoc Networks (VANETs), traditional security solutions like encryption are combined with intrusion detection mechanisms. Vehicular ad hoc network does not have central network authority where the Intrusion Detection System (IDS) can collect, log and analyze audit data for the whole network. One approach is to have an IDS client running on each and every individual VANET node which runs a local detection engine analyzing own log information to detect anomalies. A cooperative detection mechanism takes decision whether there is an intrusion with all the nodes participation in the decision process by voting. But VANET nodes typically have limited resources which is not efficient in making each node as a monitoring node which keeps a database to find out an intruder or to save information about intruder. Thus, in this study we propose the concept of a cluster by grouping of direct-link nodes which can randomly and impartially select a monitoring node, the Cluster Head (CH). The Cluster Head (CH) provides security by collecting information from other Cluster Members (CM) and make database and executing an intrusion detection algorithm on cluster head only instead of running IDS on every VANET Node (VN). This scheme provides a security and offers a new approach to save consumption of limited resources of vehicular ad hoc networks.

Key words: Vehicular ad hoc network, cluster, intrusion detection, AODV, collecting information

INTRODUCTION

A Vehicular Ad hoc Network (VANET) is a non-infrastructure based network that does not rely on a central administration for communication between vehicles. In a vehicular ad hoc network, the overlapping transmission range of each vehicle ensures a unified and common channel for communication between the vehicles. The pliancy of VANETs giving opportunities to originate a lot of applications those contribute to the safety and comfort of the vehicle passengers. Vehicular Ad hoc Networks are self-organizing networks established among vehicles equipped with communication facilities. The communication can be only Vehicle to Vehicle (V2V) or may also involve some roadside infrastructures. Some other applications have been proposed on VANETs for different purposes such as infotainment, safety, financial and navigational aid.

With improvement of vehicular ad hoc network applications and mobile devices, security becomes one of the main problems which ad hoc network faces nowadays. Vehicular ad hoc network has unique characteristics that make it more vulnerable to several types of attacks. Some of these characteristics include mobility, decentralized network topology, bandwidth and delay. Besides of these characteristics, understanding potential type of attacks is usually the first step towards developing good security solutions. These characteristics impose heavy limitation on functionality of an effective Intrusion Detection System (IDS). Therefore, securing vehicular ad hoc networks are a highly challenging issue.

In VANET usually for applications which require routing, AODV or DSR protocols are used. These protocols are damageable by major attacks such as black-hole attack, route request flooding attack, etc. for example AODV selects an optimized route when it contains the biggest sequence number and the smallest hop count, so malicious nodes that want to create a black-hole can easily change the values and confuse routing operation and hence all sent packets from a legitimate source to legitimate destination pass through the private tunnel of the malicious nodes but it will not forward that packets to the destination. In AODV, there is no authentication and protection in support of packets therefore routing packets will be affected easily as a consequence, routing operation is disturbed. In (Isaac *et al*., 2010) present, a major security attacks, issues and challenges that have reported on VANETs recently. The 1609.2 standard (Torrent-Moreno *et al*., 2005) proposes the functionalities of a security layer in

Corresponding Author: K. Indira, Department of Information Technology, Sathyabama University, Chennai, India

V2V communication. Several researches (Raya *et al*., 2006; Papadimitratos *et al*., 2006; Gerlach *et al*., 2007; Ghosh *et al*., 2009) investigate the requirements and challenges involved in providing secure V2V communication and propose general architectures for security in such scenarios. However, though some of these works stress the need for misbehavior detection, present and evaluate a misbehavior detection scheme for Post Crash Application (PCP).

The dynamic and dense VANET topology and the harsh VANET environment, produce many challenges for communication and networking. In traditional Mobile Ad hoc Network (MANET) research these difficulties were often overcome by a clustered topology. As a result, clustering has become a common topic in the vehicular ad hoc network research community. One of the many challenges for VANETs is the dynamic and dense network topology, resulting from the high mobility and high node-density of vehicles (Raya *et al*., 2006). This dynamic topology causes routing difficulties as well as congestion from flooding and the dense network leads to the hidden terminal problem. A cluster model can make the network looks smaller and more stable in the view of each node. Clustering the vehicles into group according to similar mobility, the relative mobility between neighboring nodes within the transmission range will be automatically reduced, leads to increase the stability within the cluster. In addition to that the hidden terminal problem can be diminished by clustering (Gunter *et al*., 2007).

CLUSTERING SCHEME

The cluster formation proceeds through the following way. Our clustering scheme will form the clusters with 1-hop connectivity, relative speed and same direction.

Initially node ID will be generated for all the nodes. Each node finds its neighbors by broadcasting HELLO packets in regular interval period of time and looking for responses. Thus, every node collects its neighbor information. Initially every node is in the initial state. Here, each node creates single node cluster and runs an intrusion detection engine on it (Fig. 1).

After that combine the several nodes into cluster where every pair of members can communicated directly. After forming this group those nodes are having the relative speed in the same direction form the cluster and elect the Cluster Head (CH) based on which node speed is nearest to the average speed of the all nodes in that cluster. To form a cluster, this proposed scheme considers the relative speed should be from 0-3 to make a cluster is more stable. The formula which is used to find out the relative speed between two VANET nodes (node x with respect to node y) is:

$$\text{Relative speed (x, y)} = \text{absolute } (\text{speed}_x \text{-speed}_y)$$

When a cluster member moves out of range of its cluster head, its find out any other cluster is having same relative speed in same direction with 1-hop connectivity. If it found any cluster satisfying above parameters, its joins with that cluster by sending the join message to that cluster head. Otherwise, it will form the new cluster. A CH will only consider a change of its head state if it receives a message from another CH. At that time which one is having minimum relative speed that acting as a cluster head, other one will become the cluster member. Also to ensure unpredictability, we use a lowest node ID, helps in resolving conflicts among nodes with exactly same speed. From this clustering scheme we can reduce rate of change of cluster head. One cluster head will exchange the attack alters, safety and non-safety data with another cluster head through the Gateway Node (GN) the node which is common to two or more clusters.

To implement these changes, we propose the protocol whose finite state machine is shown in Fig. 2. A

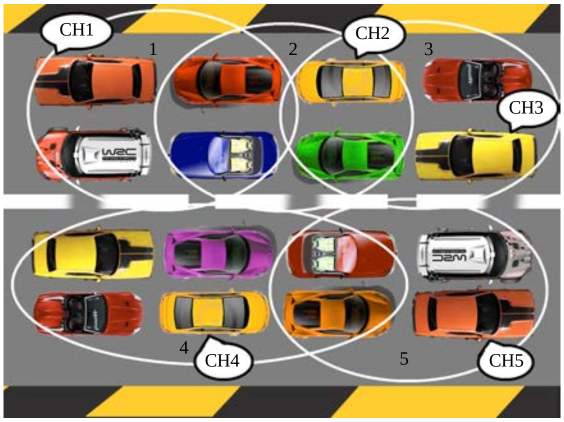

Fig. 1: Structure of clusters

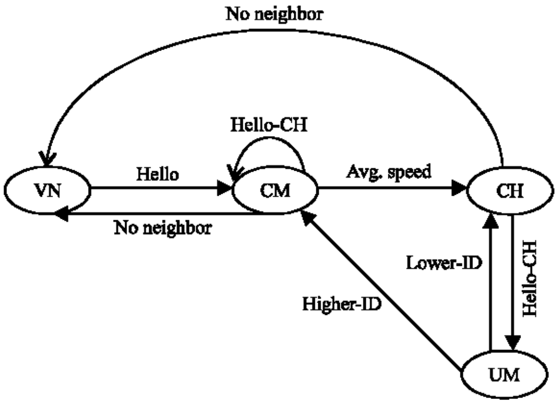

Fig. 2: State diagram for cluster formation

node starts in the VN (VANET node) state where it listens to the wireless channel and periodically sends hello packets with relative speed and direction to announce its presence in the neighborhood. Now all the nodes become Cluster Member (CM). Among the cluster member one node will change its state as Cluster Head (CH) based on which one is having nearest average speed of that cluster. While in CM, the node only changes its state in two circumstances:

- No hello-CH message has been received within the timeout interval (meaning that there is no cluster head in the neighborhood)
- There are no neighbors which condition is detected via another timeout-while expecting any hello message

The case of a node in CH state is more complex. If a cluster head does not receive hello packets from any other cluster head, it continues in the present state. If the node detects that it has no neighbors (general hello timeout) then it will return to the VN state. The important part happens when two cluster heads are communicating neighboring nodes and exchange packets among themselves. After receiving a packet from the other Cluster Head (CH) again they will compare relative speed and elect the Cluster Head (CH) in which one node remains in the same CH state, the other one immediately changed to the CM state. If conflict occurs, both are enter into the Unpredictable Mode (UM). Based on the lowest node ID one node is changed as CH, another one changed as CM.

INTRUSION DTECTION SYSTEM

Intrusion Detection System (IDS) is a type of security system for individual computers and networks. An IDS gathers and analyzes information from various parts within a computer system or a network to pinpoint possible security violations which include both intrusions from outside the network and attacks from within the network. An IDS uses vulnerability scanning which is a technology developed to examine the security of a computer system or network. It processes audit data, performs investigation and takes some set of actions against the intruder such as blocking communication with them or send notification to the system administrator. Ad hoc networks lack in centralized audit points thus it is mandatory to use the IDS in a distributed manner. This also supports to reduce bandwidth consumption on each node. The proposed clustering algorithm combined with the concept of intrusion detection model to examine the traffic regularly is done at the Cluster Head (CH) to provide security as well as improve the performance of routing in VANET.

The IDS can be categorized as misuse detection system or anomaly detection system. Misuse detection (or signature detection) system is generally used for known patterns of unauthorized behavior (or attack signatures). The anomaly detection system identifies intrusions using ‘normal’ activity behavior. It achieves this with ‘self-taught’. The misuse detection system often fails if the database of attack signatures is not updated regular basis. The other problem with misuse detection system is the bulk of database which a vehicular ad hoc node cannot handle due to memory constraint if it contains all the known attack signatures. Therefore, anomaly detection technique is used that is trained with passage of time for normal traffic and this information is then further used in the testing period to detect abnormal activities/behavior deviated from normal activity. Anomaly intrusion detection model is built on a long run examine and then only classify a normal or abnormal behavior. Ad hoc wireless networks are very dynamic in structure, giving rise to apparently random communication patterns thus making it challenging to build a reliable behavioral model and it is possible that the anomaly detection system will create a lot of false positives. Thus in such a highly mobility environment, the simplest and the most authentic technique of anomaly detection is threshold based intrusion detection. If a node go beyond a small threshold of such allowed “misbehavior” it will be detected and classified as anomaly. A few of the general network parameters that can be monitored are:

- Forward percentage
- Malicious flooding

Attacks: In wireless ad hoc networks, routing relies on the trust worthiness of all the nodes that are participating in the routing process. Several research papers discussed various types of attacks that can be easily performed against the routing protocol in ad hoc networks. In this study, we simulate two common attacks to evaluate the implementation of proposed intrusion detection system. The more complex attacks will be further investigated.

Black hole attack: The malicious node listens to a ROUTE REQUEST packet in the network and responds with claim of having an extremely short route to the destination node, even if it does not have any such route. As a outcome, it decline the communication to take place. A malicious node catches all the routes and reroute itself. Finally, it receives all the packets but it never forwards any packet to anywhere.

Routing request flooding attack: The malicious node intensively floods the whole network with meaningless route discovery messages to prostrate the network bandwidth and freeze the network.

Anomaly based IDS architecture: A flow model of anomaly based intrusion detection architecture is presented in Fig. 3 which consists of four modules. These modules are linked with each other for effective intrusion detection. The information collected during the training phase in the logging module is passed regularly to the intrusion information module to perceive a threshold value for the normal traffic. This threshold value is further used during the testing phase to check malicious behavior. If some abnormal behavior is found, an alert is generated by the intrusion response module. The functionality of each module is given.

Logging module: Cluster Head (CH) logs all the traffic transferred through its radio range. It captures all the traffic in the promiscuous mode and maintains the required fields in a database. It keeps the data related to traffic such as number of packets sent, received, forwarded or dropped. The traffic can either be data traffic or the control traffic. The control traffic includes RREQ, RREP, RERR packets of AODV and HELLO packets. It keeps the count of packets transmitted or received for each sampling period. These logs can be helpful for detection of many attacks such as black-hole, wormhole, sleep deprivation, malicious flooding, packet dropping, etc. (Fig. 3).

Intrusion information module: All the unauthorized or attack signatures, origin to an intrusion must be stored in the database. For anomaly detection technique, the unusual behaviors must also be well defined with proper upper and lower threshold values. Anomalous values can be dynamically updated in particular time interval. The required values which are maintained in logging module are used to conclude upper and lower threshold values for the misbehavior signature. Mean and Standard Deviation Model is one of the approach to process the data and measure the expansion of normal traffic. Mean (M) and standard deviation (S) is calculated for each sample of data and formula used to conclude the upper and lower limit threshold values is given below:

$$M_i + d \times S_i$$

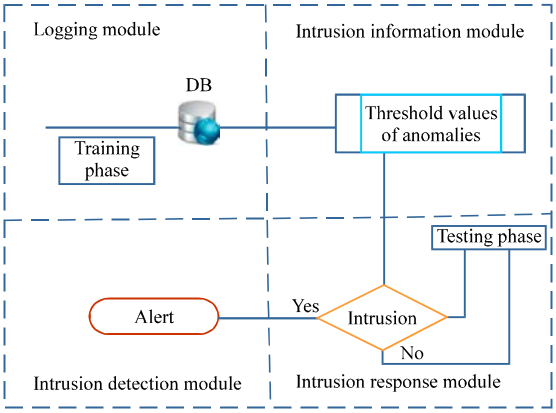
Logging module
Intrusion information module
DB
Training phase
Threshold values of anomalies
Testing phase
Alert
Yes
Intrusion
No
Intrusion detection module
Intrusion response module

Fig. 3: Intrusion detection process flow

Intrusion detection module: When the nodes are trained they detect the intrusions by analyzing and comparing the traffic patterns with the normal behavior. The cluster head still captures the traffic in the promiscuous mode and compares its behavior with the normal traffic behavior. If anomaly is found in the data, the cluster head raises the alarm and increases the monitoring level and analyzes the traffic in more detail to find out the attack type and identity of the attacker. To preserve the resources, the cluster head initially log only a few details of the traffic such as packet count. When an anomaly is found, the packet monitoring level can be increased such as analyzing the packet in depth according to resources availability. If the intruder does not belong to the same cluster in which the suspicious behavior is detected, the cluster head may ask neighbor cluster-heads to cooperate.

Intrusion response module: To inform other nodes about some intrusion, head and member nodes generate alerts. The response may be local to the cluster or global by sending alters to the neighboring cluster heads through Gateway Node (GN) covering the whole network. Cluster head generates intrusion responses in two situations: after log-based detection or after getting response from adjacent cluster. In this case, all the nodes in the network are notified about a misbehaving node. The response taken due to found intrusion can be one of the following: removing the malicious node 'M' from the route, reducing trust level of node M or blocking all the traffic from node M, etc. The trust level reduction can be support as preemptive measure so that:

- Node M is not elected as a Cluster Head (CH) in the future
- No route involving node M is encouraged

Performance evaluation: To evaluate the effectiveness of our proposed intrusion detection approach, we have simulated two common attacks against ad hoc routing protocols using the ns-2 network simulator. In simulation of nodes, random waypoint model is used and maximum speed of them is 20 m sec^{-1} in 140 m field. The 100 nodes are distributed randomly in 1200×1200 m free space.

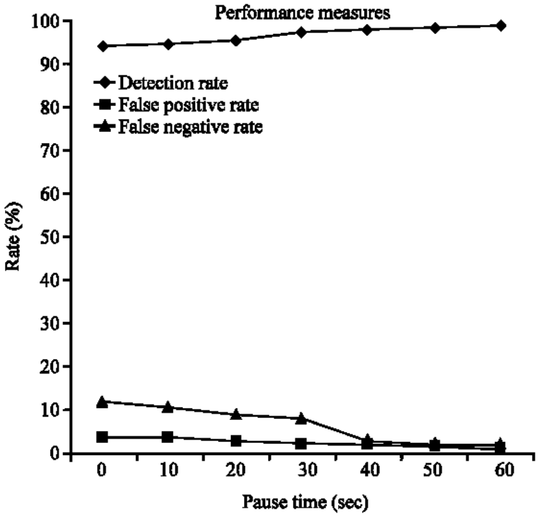

Fig. 4: Performance evaluation

A distance of 100 m between nodes is considered as neighbor node. Setup positions of nodes are selected randomly. Each node has Constant Bit Rate (CBR) traffic output with 64 bytes packet size and 4 pkts $\sec^{-1}$ rate. We first simulate normal network activities (without any intrusive activities involved) in different scenarios: the initial network topology is randomly generated, each node follows the random mobility model and the network traffic patterns are generated in a random way. After the simulation time, we extract the pre-defined features from the network log files with a sampling period of 1 sec and generate a normal dataset. The normal dataset is further divided into two parts, one for training phase and the other part for testing phase. The training part consists of 10% of the whole normal patterns. It is then applied to the training phase of the proposed anomaly detection model (Fig. 4).

CONCLUSION

VANETs exhibit idiosyncratic characteristics demanding networking solutions especially geared to their environment. By self-organizing themselves into clusters, vehicular nodes create a hierarchy within the network which helps them optimize resources and reduce communication burden. However, the highly dynamic topology of a vehicular network results in propensity for frequent cluster formation and re-organization which decreases cluster stability. This proposed clustering scheme provides significantly higher cluster stability.

In this stduy, the proposed concept is anomaly detection system based on threshold value to identify intrusions in VANETs. This method created low overhead in terms of number of messages exchange for network while it secured it against black hole and flooding and can detect malicious nodes as far as possible. Standard measures for evaluating IDSs are detection rate and false alarm rate these measures are achieved best in this proposed approach.

REFERENCES

Gerlach, M., A. Festag, T. Leinmuller, G. Goldacker and C. Harsch, 2007. Security architecture for vehicular communication. Proceedings of the 5th International Workshop on Intelligent Transportation, March 2007, Hamburg, Germany.

Ghosh, M., A. Varghese, A.A. Kherani and A. Gupta, 2009. Distributed misbehavior detection in VANETs. Proceedings of the IEEE Wireless Communications and Networking Conference, April 5-8, 2009, Budapest, pp: 1-6.

Gunter, Y., B. Wiegel and H. Grossmann, 2007. Cluster-based medium access scheme for VANETs. Proceedings of the IEEE Intelligent Transportation Systems Conference, September 30-October 3, 2007, Seattle, WA., pp: 343-348.

Isaac, J.T., S. Zeadally and J.S. Camara, 2010. Security attacks and solutions for vehicular ad hoc networks. IET Commun., 4: 894-903.

Papadimitratos, P., V. Gligor and J.P. Hubaux, 2006. Securing vehicular communications-assumptions, requirements and principles. Proceedings of the Workshop on Embedded Security in Cars Conference, November 14-15, 2006, Berlin, Germany, pp: 1-10.

Raya, M., P. Papadimitratos and J.P. Hubaux, 2006. Securing vehicular communications. IEEE Wireless Commun., 13: 8-15.

Torrent-Moreno, M., M. Killat and H. Hartenstein, 2005. The challenges of robust inter-vehicle communications. Proceedings of the IEEE 62nd Vehicular Technology Conference, Volume 1, September 25-28, 2005, IEEE Computer Society, Washington DC. USA., pp: 319-323.