International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Minimization of Attacks in VANETs by using Intrusion Detection System

P. Anand Babu[1], R. Prasanthi[2]
[1]*M.Tech in TELEMATICS,* [2]*Assistant Professor, Electronics and Communication Engineering department*
Velagapudi Ramakrishna Siddhartha Engineering College, affiliated to Jawaharlal Nehru Technological University -Kakinada, Kanuru, Vijayawada-7, Andhra Pradesh

Abstract: ***Vehicular ad-hoc networks have been a research hotspot in wireless communication field. Security providing for data transmission in between nodes, attacks that are occurring in VANETs has become a big issue in VANETs.Usage of V2V (vehicle to vehicle) ad hoc networks and its internet applications has becoming an important task in present days, because of significant changes in network attacks. Intrusion detection system is a defense measure that reduces different tasks of computer networks and generates the attack sequences to the organizer of the network. So privacy and security is the most and effective measure for any type of network organization. So intrusion detection is an important research topic in network communication. AODV (Ad hoc On-demand Distance Vector) and Enhanced AODV's are the two approaches were used to support intrusion detection in static V2V (vehicle to vehicle ad hoc networks. To provide effective intrusion detection for dynamic ad hoc networks, in this paper, we propose and introduce a novel semi supervised approach i.e. Extended AODV Design. This approach is introduced to support two main issues, first one is select most relevant feature from network communication based on information gain, and second one is to split the value is chosen in such a way that makes the classifier impartial towards most regular values. Our experimental results will perform based on different attributes and also maintain equivalence simulation time in dynamic V2V (vehicle to vehicle) transmission. Proposed algorithm will use for signature based intrusion detection in V2V (vehicle to vehicle ad hoc networks.***

Keywords: V2V (vehicle to vehicle) Ad hoc networks, AODV (Ad hoc On-demand Distance Vector) , Classification, Feature Comparison.

I. INTRODUCTION

Now a days VANET technology V2V(vehicle to vehicle communication) V2I(vehicle to infrastructure communication) growing enormously to maintain the driving system more and more secure and trust worthy. Each vehicle is assuming as node. The main motive of this technology is to make the vehicle intelligent in transportation, fast decision taking in the risky situations, quick reaction to environmental situations during rain, fog and identifying the fake messages to not be deceived etc. It is also training in transforming the messages between the vehicles about road conditions like traffic, accidents, etc., to reduce the transportation time. For this purpose each vehicle has to exchange data each other about the conditions it had faced. By this data the neighbor vehicle can take decisions, in changing the direction due to heavy traffic and accidents. This type of actions reduces the congestion on the road makes transportation very fast. In this case every action is taken after exchanging the information. It is very essential to secure the data that is exchanging between the nodes. Sometimes the selfish node transmits a fake message for its own desire, showing traffic condition to other nodes to make itself clean road. Many types of attacks are injecting in to the VANETs (Vehicular Ad hoc Networks) to break the transportation and deceive vehicles by false information. To control these attacks several algorithms are written. Intrusion detection system (IDS) monitors the V2V (vehicle to vehicle ad hoc networks to configure the network tasks with reports does not assure the security measures in network administrator. Based on different configurations demonstrated in network implementation IDS's are classified into two categories, firstly Signature Based detection and secondly Anomaly based attack detection. Signature and misuse based IDS use different approaches to track similarity among network behavior and traditional attack sequences stored in signature data maintenance. Whereas anomaly based attack sequences deviates from normal user behavior stored in network profile data maintenance. For static network communication, traditionally developed AODV and enhanced AODV for intrusion detection with different node communications. AODV is applicable for the only falsehoods inactive behavior of the node in powerful topology, in inactive strikes, there is another problem faced i.e. accident centered strikes because of powerful redirecting series in ad hoc V2V(vehicle to vehicle networks, so node recognition and preserves separate information transmitting levels for V2V(vehicle to vehicle network communication. Enhanced AODV comprises node confirmation depending

on signature confirmation and then imitate powerful redirecting between different nodes with handling of effective information transmitting with fixed system topology. Procedure of the EAODV shown in figure 1.

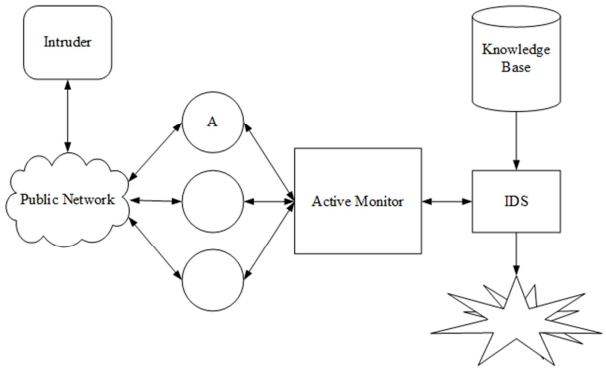

Figure 1: AODV based attack detection procedure.

Moreover, one additional area in the method concept is suggested to allow the monitoring shown in figure 1. The dynamic and helpful nature of V2V (vehicle to vehicle network presents considerable difficulties in securing these systems. Dissimilar to wired systems which have a more elevated amount of security for passages and switches, specially appointed systems have the qualities, for example, progressively evolving topology, powerless physical assurance of hubs, the nonappearance of unified organization, and profoundly reliance on inborn hub participation. As the topology continuing changing, these systems don't have a very much characterized limit, and subsequently, organize based get to control components, for example, firewalls are not specifically appropriate. To incorporate the dynamic ad hoc networks IDS detection, various types of classification algorithms are applicable to misuse and anomaly based attacks in V2V(vehicle to vehicle networks. So in this paper, we propose and introduce a novel semi supervised classification approach i.e. CPHC (Classification Pattern based Hierarchal Clustering) to classify the data input as normal node and anomalous node in V2V (vehicle to vehicle) ad hoc network communication. The classification rules are formed by path selection from input root node between leaf nodes in network communication. To isolate each information, first the root hub is picked as it is the most conspicuous ascribe to isolate the information. The tree is developed by recognizing characteristics and their related values which will be utilized to examine the information at each middle of the road hub of the tree. After the tree is shaped, it can prefigure recently coming information by crossing, beginning from a root hub to the leaf hub going to all the interior hubs in the way relying on the test states of the characteristics at every hub. KDD (Knowledge Discovery Data set) is the most recent data set for the intrusion detection. This dataset comprises of 41 features, however not every one of the elements is of equivalent significance. On the off chance that entire list of capabilities is utilized for order input information, at that point, the classifier will set aside greater opportunity to recognize intrusion and they can likewise influence the precision of the classifier. That is the reason before playing out any order; we have to lessen this set by applying some component choice technique. Highlight determination is done to expel superfluous and repetitive highlights.

The rest this paper organized as follows: Section 2 describes related work regarding different classification approaches for intrusion detection in V2V(vehicle to vehicle networks. Section 3 defines background procedure i.e. EAODV regarding IDS in V2V(vehicle to vehicle) ad hoc networks. Implementation design for CPHC discussed in section 4. Experimental evaluation results will discuss in section 5. Section 6 concludes overall conclusion regarding IDS detection in V2V(vehicle to vehicle ad hoc networks.

II. RELATED WORK

This section describes review has been included latest approaches that performs testing and training of network system on KDD data sets. Elekar, and Waghmare actualize distinctive classifiers, for example, C4.5 choice tree, Random Forest, Hoeffding Tree and Random Tree for intrusion location and look at the outcome utilizing WEKA. The outcomes demonstrate that the Hoeffding Tree gives the best outcome among the different classifiers for distinguishing assaults on the test information. Aggarwal and Sharma assess ten arrangement calculations, for example, Random Forest, C4.5, Naïve Bayes, and Decision Table. At that point they mimic these arrangement calculations in WEKA with KDD'99 dataset. These ten classifiers are investigated by measurements, for

example, exactness, accuracy, and F-score. Arbitrary Tree demonstrates the best outcomes in general while the calculations that have high recognition rate and low false caution rate were C4.5 and Random Forest.

In [7] the creators demonstrate how helpful the NSL-KDD for different intrusion location models is. For dimensionality lessening, PCA (Principle Component Analysis) system was utilized as a part of this paper. Six unique calculations, specifically, ID3, Bayes Net, J48, CART, SVM , and Naïve Bayes were utilized for the experimentation with and without include diminishment, and from the outcomes unmistakably SVM gives the most astounding exactness for the over two cases. In [8], the creators outlined a multi-layer cross breed machine learning IDS. PCA was utilized for property determination and just 22 highlights were chosen in the first layer of the IDS. GA was utilized as a part of the following layer for creating identifiers, which can recognize typical and unusual conduct. In the third layer, characterization was finished utilizing a few classifiers. Results exhibit that the Naive Bayes has great precision for two sorts of assaults, specifically, User-to-Root (U2R) and Remote-to-Local (R2L) assaults however the choice tree surrenders higher exactness to 82% for Denial-of service assaults and 65% of test assaults.

The framework proposed by Raeeyat et al. in [9] comprises of 4 modules, in particular, Data pre-preparing module, Misuse identification module, and irregularity discovery module also, Evaluation and examination module. Information was preprocessed before going to alternate modules by information pre-handling module. In the abuse identification module, pre-prepared information is given to PCA to take out critical elements. After that, the information was analyzed utilizing Ad boost calculation in view of the C4.5 choice tree to know whether it is a typical parcel or an intrusion. At that point, the result of choice tree is passed on to the following module for assessment and correlation. Whenever the information is sent to abuse identification module it is all the while sent to irregularity discovery module too. The connection among highlights was additionally discovered by the relationship unit by utilizing Pearson Correlation. Information connection chart is utilized to demonstrate deviation of conduct from the ordinary conduct. At that point, the assessment and correlation module decide if the occurrence is an intrusion or not by taking the yield from abuse and oddity identification module and if both the module demonstrates that it is an intrusion then just that occurrence is considered as an intrusion

III. EAODV BASED IDS DETECTION

V P Krishna Anne et.al [1] discuss about advanced implementation of EAODV to detect relative based IDS in V2V(vehicle to vehicle ad hoc networks. Improved AODV to identify internal strikes against AODV in V2V(vehicle to vehicle) ad hoc systems. It is depending on powerful or state less path series, which is variety centered or network centered attack in fixed topology V2V(vehicle to vehicle) ad hoc networks. In [1], discuss about EAODV procedure for IDS detection in V2V(vehicle to vehicle) ad hoc networks. Procedure of the EAODV for IDS discussed in Algorithm 1 with step by step procedure.

Input Requirements
SN: Source Node
IN: Inner Node
DN: Destination Node
ACK: Acknowledgement

1. Install V2V(vehicle to vehicle communication with basic parameters.
2. Dynamically select source and destination with RREP and RREQ.
3. SN evaluates intermediate nodes notifications based on ACK with respect destination Sequence number.
4. If any intermediate node give false ACK regarding data transmission at destination node.
5. Then SN fails to send packets to destination because of false notification from intermediate nodes
6. To avoid packet loss because of IDS in

data transmission

7. Automatic route request (RREQ) and response process (RREP) codes will generate on demand ACK for all the available routes while data transmission.
8. Maintain secure signature generation for data transmission.
9. Destination node follows unicast data delivery to dynamic source and dynamic destination for conveying data transmission.

Output Data Access: Efficient data delivery to dynamic ad hoc networks.

Algorithm .1. Procedure of the EAODV for IDS in V2V(vehicle to vehicle Communication**.**

IV. EXPERIMENTAL RESULTS

Experimental evaluation of proposed algorithm is done by the comparison of previous approaches like EAODV and others, this evaluation done by different parameters like packet delivery ratio, throughput, and execution time and accuracy based on attack detections in dynamic ad hoc networks. For topology construction and data communication may accessed with following simulation parameter.

Table 1: Network Simulator Parameters.

Parameter	**Parameters**
Area 600*600	Packet Size 40000 bits
Node number 30	Eelec 50nJ/bit
Simulation Time	30S
Mobility Speed	0-30m/sec
Number of attacker nodes	03
Simulator Version	NS-3
Check point nodes	4 nodes(Fixed)
Transmission Range	$250^2 \times \pi$ m2.

Using the above simulated parameters, we design network topology with different simulated parameter sequences in data transmission.

A. Data Set

The efficiency of the proposed approach is evaluated with different experiments with KDD- Cup data sets, which is the extension of KDD data sets, why we are using KDD-cup data sets, because redundant records used in training and testing dataset. We register data pick up of the considerable number of characteristics of the informational collection. We found that there are 16 properties whose data pick up is more prominent than the normal data pick up. That is the reason in the preprocessing step, we can pick 16 or under 16 properties for additionally preparing in view of data pick up in light of the fact that the rest of the elements won't have much impact on the order of the dataset.

B. Results

The experimental results of proposed approach are compared with the executable performance of EAODV. Basic comparison results are taken from the accuracy in detecting different attack sequences in V2V(vehicle to vehicle ad hoc networks. Design of the proposed approach with attack detection shown in figure 2,

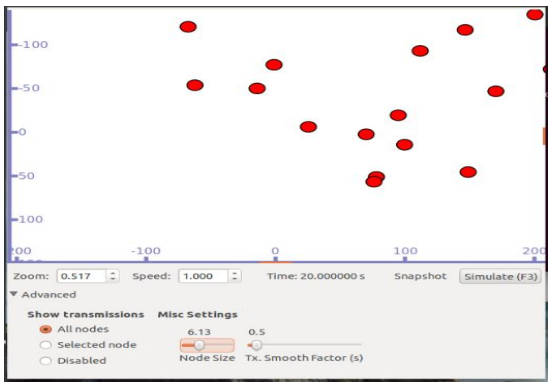

Figure .2. Dynamic topology construction with different nodes.

Figure 2 shows the different nodes with different topologies with sequence of execution between nodes in data transmission. Attacks sequences with different mobility positions in network transmission are shown in figure3.

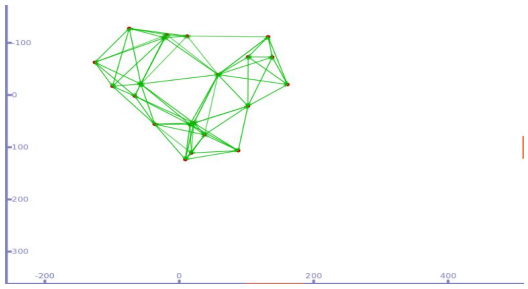

Figure .3. Network topology representation with attack presentation in mobility sequences.

Accuracy of the proposed approach with comparison of traditional approaches like AODV, and EAODV in terms of % of packet loss with different formation in dynamic network transmission shown in figure 5

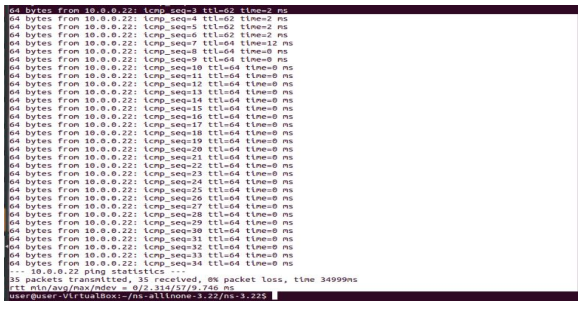

Figure 4: IDS detection results between different vehicular nodes in VANETs.

IDS detection procedure with generation different sequence numbers in relevant data formations may formed to present in figure 4 with irresponsible vehicle node data delivery.

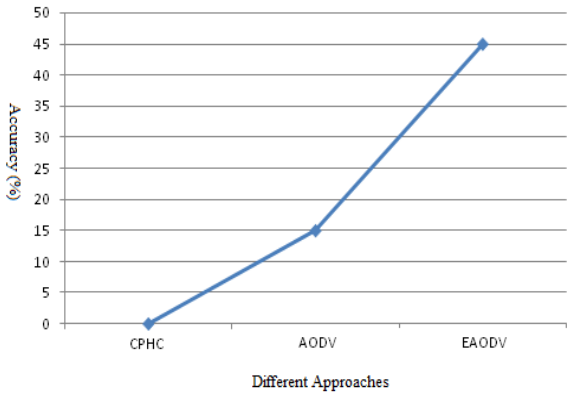

Figure .5. Accuracy comparison of proposed algorithm with traditional techniques.

Fig 6 defines the throughput with traditional presentations based on practical implementation shown in table 2.

Number of nodes	AODV	Extended AODV
10	75	135
20	85	190
30	95	210
40	105	250
50	125	325

Table 2. Throughput values for different nodes.

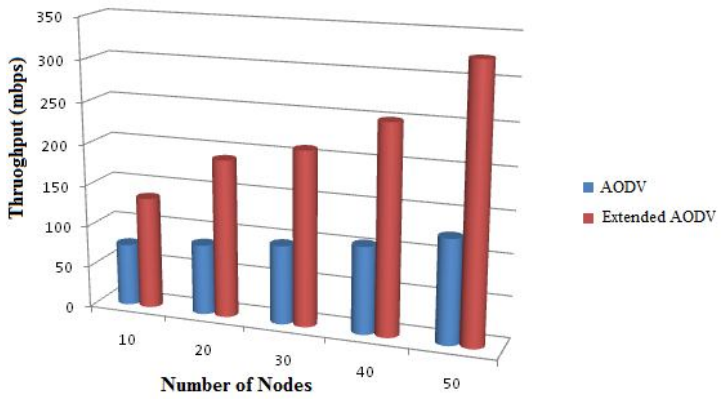

Figure 6. Throughput with respect to different nodes in both techniques

It can be seen from the results that with the proposed technique, instead of training with all the features we get good accuracy with even less number of features selected using information gain.

V. CONCLUSION

CPHC helps the system executive to choose the approaching activity, i.e., regardless of whether the coming information is malevolent or not by giving a model that isolates malignant and non-noxious movement. By altered the split esteem figuring by taking the normal of the considerable number of qualities in the area of a trait. The calculation gives uniform weightage to all the values in the area. It permits taking less number of characteristics and gives adequate exactness in the sensible record of time. From the after effects of the analyses, it is presumed that the proposed calculation for signature based interruption identification is more proficient concerning discovering assaults in the system with less number of elements and it requires less investment to develop the model

REFERENCES

[1] S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, “Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach”, 2009 International Conference on Future Computer and Communication.
[2] A. Ebner, H. Rohling, M. Lott, R. Halfmann, “Decentralized Slot Synchronization In Highly Dynamic Ad Hoc Networks”, Proc. 57th IEEE Vehicular Technology Conference, Jeju, South Korea, 2003.
[3] Philippe Golle, Dan Greene, Jessica Staddon, “Detecting and Correcting Malicious Data in VANETs”, Proc. First Interna- tional Workshop on Vehicular Ad-hoc Networks, pp. 29-37,Philadelphia, USA, Oct. 2004.
[4] P. Papadimitratos, V. Gligor, J-P. Hubaux, “Securing Vehicular Communications Assumptions, Requirements, and Principles”, Proc. The Workshop on Embedded Security on Cars (ESCAR) 2006, November 2006.
[5] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, “Securing Vehicular Communications”, IEEE Wireless Communications, pp. 8-15, October 2006.
[6] Tim Leinmuller, Elmar Schoch, and Frank Kargl, “Position Verfication Approaches for Vehicular Ad Hoc Networks”, IEEE Wireless Communications, pp. 16-21, October 2006.
[7] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya, “Architecture for Secure and Priviate Vehicular Communications”, Proc. The 7th International Conference on ITS Telecommunications, June 2007.
[8] Maxim Raya, and Jean-Pierre Hubaux, “Securing Vehicular Ad hoc Networks”, Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.
[9] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, “Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks”, Proc. Forth Annual Conference on Wireless on Demand Network Systems and Services, 2007.
[10] Patrick P. Tsang and Sean W. Smith, “PPAA: Peer-to-Peer Anonymous Authentication” Proc. 6th International Conference on Applied Cryptography and Network Security, (ACNS ’08), pp. 55-74, New York, NY, USA, June 3-6, 2008.
[11] Frederik Armknecht, Andreas Festag, Dirk Westhoff, Ke Zeng, “Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication”, Fourth Workshop on Mobile Ad- Hoc Networks (WMAN), Bern, Switzerland, March 2007.
[12] Sumair Ur Rahman and Urs Hengartner, “Secure Crash Reporting in Vehicular Ad hoc Networks”, Proc. Third International Conference on Security and Privacy in Communication Networks (SecureComm 2007), Nice, France, September 2007.
[13] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, Antonio Lioy, “Efficient and Robust Pseudonymous Authentication in VANET”, VANET’07, Montral, Qubec,Canada, September 2007.
[14] Frank Kargl, Zhendong Ma, and Elmar Schoch, “Security Engineering for VANETs”, 4th Workshop on Embedded Security in Cars (escar 2006), Berlin, Germany, 2006
[15] Adam D. Woodbury, Daniel V. Bailey, Christof Paar, “Elliptic curve cryptography on smart cards without coprocessors”, The Fourth Smart Card Research and Advanced Applications (CARDIS 2000) Conference, September 20-22, 2000, Bristol,UK.
[16] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, “Elliptic Curve Cryptography”, ACM Ubiquity, Volume 9, Issue 20, May 20 26, 2008.
[17] N. P. Smart, “How secure are elliptic curves over composite extension fields?”, EuroCrypt 2001, pp. 3039, May 2001.
[18] Istvan Zsolt BERTA, and Zoltan Adam Mann, “Implementing elliptic curve cryptography on PC and smart card”, Periodica polytechnica ser. El. Eng., Vol. 46, No. 1-2, pp. 4773, 2002.
[19] M. Aydos, B. Sunar, and C. K. Koc, “An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication”, 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pp. 1-12, Dallas, Texas, October 30, 1998.