International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3S, February 2019

Hybrid Machine Learning Procedure to Handle Hybrid Attacks in Wireless Vehicular ad hoc Networks

Pavan Kumar B V S P, S.S.V.N. Sarma, C. Lokanatha Reddy

Abstract: ***Vehicular ad hoc networks (VANETs) are an emerging technology in modern environment transportation media. Because of VANET importance in information circulating through network is a crucial life in real time scenario. Combining information extraction from different vehicles is a complex need for real time applications. The volatile nature of the communication connections in network has made up VANET vulnerable to different types of security related attacks. Sybil, Distributed Denial of Service (DDOS) attacks are the major attack sequences that exhausts the network by illegitimately based on its resources. In this type attack sequences different types of fake identifiers consists spoofed vehicle id's based on related server ip_address to exhaust the network by circulating bogus messages from other vehicles present in VANETs. So that in this paper we propose Hybrid Machine Learning approach (which consists Support vector machine (SVM), artificial neural network classification and AODV protocol hierarchy) to handle Sybil with DDOS attack sequences and provide efficient communication between vehicle nodes in vehicular ad hoc networks. Attacks handle in this scenario consist two basic steps i.e first selects most relevant feature from network based on data transmission from one to different vehicular nodes, based on selected feature classify the attack and then handle the efficient data transmission process in vehicular ad hoc networks. Experimental results of proposed approach gives better simulation parameters with respect to delivery ratio, throughput and others in vehicular ad hoc networks.***

Index Terms - Vehicular ad hoc networks, Denial of service attacks, Sybil attacks, support vector machine, network communication, AODV.

I. INTRODUCTION

Fast utilization of VANET has expanded step by step as it upgrades the assurance of travelers. VANET is a specially appointed system so it likewise has the properties of self-sort out, versatile and transitory system. In VANET hubs are essentially vehicles they itself go about as a source, goal and switch to advance the information bundle from source to goal. VANET comprises of Vehicles and Road Side Units (RSU), correspondence units found aside the street that associates with the application server and the trust expert. Correspondence offices in VANET can be designed in three different ways viz. Between Vehicular correspondence, Vehicle-to-roadside and Routing Based Communication shown in figure 1.

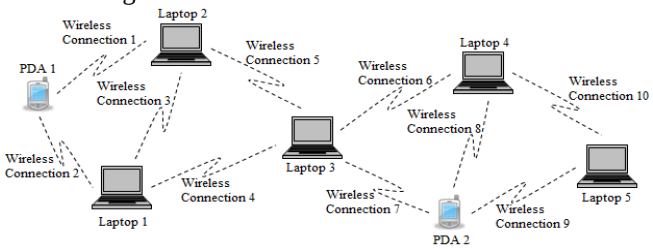

Figure 1.Inter communication between nodes in wireless network communication.

The Inter-Vehicle correspondence arrangement utilizes multi-bounce multicast to transmit traffic data over different jumps to a gathering of collectors. The correspondence happens between vehicles. In Vehicle-to-Roadside correspondence, vehicles convey utilizing RSUs. The design speaks to a solitary bounce communicate where the roadside unit sends a communication message to every prepared vehicle in the system. In Routing Based Communication, it is a multi-jump unicast where a message is sent in a multi-bounce style until the vehicle conveying the ideal information is come to.

The fundamental parts of VANET are:

On-Board Units (OBUs): These are the specialized gadgets mounted on vehicles to encourage correspondence with different vehicles and roadside units. They empower short-extend remote specially appointed systems to be framed. Roadside Units (RSUs): They used to encourage correspondence. The number and appropriation of RSUs rely upon the correspondence convention to be utilized.

Confided in Authority (TA): They are outsider endowed with the activity of authentication age, circulation and denial

1. Vehicle demand RSU to issue endorsement.
2. RSU forward to TA.
3. TA sends endorsement to RSU.

Numerous analysts have done their exploration in VANET arrange with respect to directing conventions, security issues. VANETs are defenseless against sort of dangers like dangers to accessibility, dangers to legitimacy, and risk to classification [10]. Sybil, DDoS is a sort of danger to accessibility. To incorporate the dynamic ad hoc networks IDS detection, carious types of classification algorithms are applicable to misuse and anomaly based attacks in wireless networks.

Manuscript published on 28 February 2019.
* Correspondence Author (s)
Pavan Kumar B V S P, Scholar, Department of Computer Science, Dravidian University. Kuppam. Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, Telangana. (bvsppkumar@gmail.com)
Dr. S.S.V.N. Sarma, Dean, Vaagdevi Engineering College, Warangal, Telangana.
Dr. C. Lokanatha Reddy, Dean, School of Science & Technology, Dravidian University, Kuppam

So that in this paper, we propose Hybrid Machine Learning approach (which consists Support vector machine (SVM) classification and AODV protocol hierarchy) to handle Sybil with DDOS attack sequences and provide efficient communication between vehicle nodes in vehicular ad hoc networks.

II. REVIEW OF LITERATURE

Hu et al.[8] gave another system "Ariadne" in context of the DSR strategy for diverting security. Two or three confirmation structures, for example, automated engravings, MACs discovered with join canny key fundamental segments, or TESLA could be utilized with the proposed strategy. Hash shops are utilized to check each bearing energy protecting the framework from over-inconvenience, thusly refusal of association strikes are stayed away from. Attacks from affected base focuses from messing on with the positive focuses are too much avoided by the proposed system. Blends of TESLA authenticators (MACs) are consolidated by front line switches and a hashing technique to verify the discovered tracks. The proposed procedure's security frameworks are doable and can also apply to wide combination of possessing techniques.

III. HYBRID MACHINE LEARNING PROCEDURE

In In this section, we discuss about the implementation procedure of Hybrid machine learning approach (which is the combination of support vector machine, artificial neural networks and AODV protocol) to describe feature extraction from node to detect malicious nodes in wireless ad hoc network.

Basic representation of intrusion detection in wireless ad hoc networks with trusted node communication for traing nodes which have features related to DDOS, Sybil, and other attack seqeunces shown in figure 2

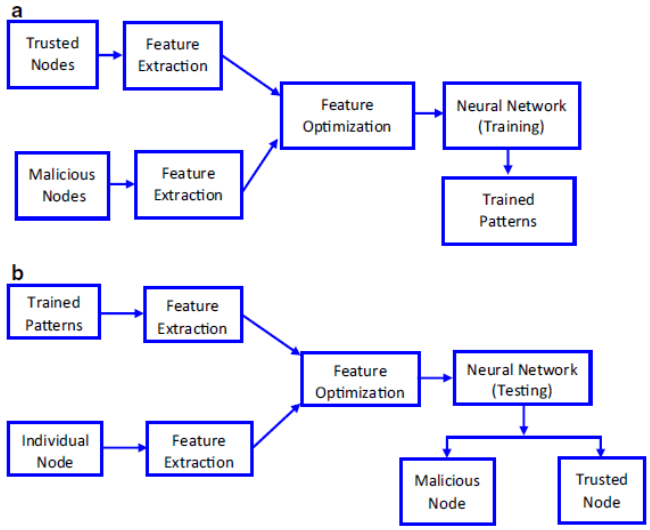

Figure 2. Trainig and tesing features in detection of attacks in wireless ad hoc networks.

As shown in figure 2, in training data, features are extracted from both malicious and non-malicious nodes in wireless vehicular ad hoc networks, these features are optimized to improve the classification accuracy in detection hybrid attacks. In testing node, Feares are extracted from node with pre-defined rules related to trained patterns data.

Extraction of Features in Classification

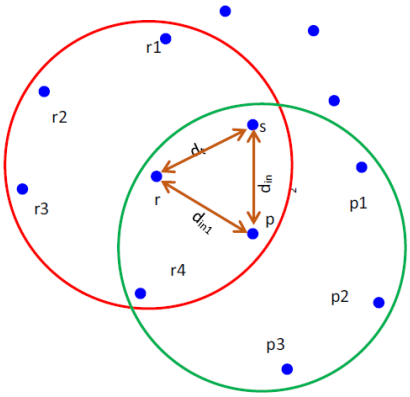

Figure 3 Trusted estimation of rule with different specifications.

As shown in figure 3, it describes trusted values estimation of each rule with different distances from node-to-node communication. Direct or indirect features of each node explored and defined individual node values based on estimated functionality. Features extracted from node r to rn then directed node specified values is categorized as follows:

$$d_t = \sum_{a=1}^{X_a} (a-u)^2 \times J_i$$

Existency emerging metric values is calculated by Ji, no. of packets contracted by r with in time limit ‘t’. Average no.of packets contracted at each node ‘r’ with time period ‘t’.

Emergency metric evaluation at each calculated as

$$J_a = \frac{\alpha_a - \beta_a}{\alpha_a}$$

αi is no. of packets retrieved at a time t, βi be the no. of packets sended over time ‘t’. Estimated value between ‘j’ and ‘r’ is

$$d_{an-l} = \sum_{a=1}^{N_a} (a-u)^2 \times J_a \times W_a$$

N_1 is sum of associated nieghbor nodes over estimated node j, weight of individual node with respect to node j to be calculated as,

$$w_a = \frac{\sum_{a=1}^{N_a} J_a \times X_a}{k}$$

k is kappa factor and it is calculated as,

$$k = \sum J_a$$

s and j are the estimated nodes

$$d_{an-2} = \sum_{a=1}^{N_2} (a-u)^2 \times J_a \times W_a$$

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

N_2 is associated node s with respect to neighbor node. Individual node estimation value is as follows:

$$d_{an} = d_{an1} + d_{an2}$$

Different node communication as follows:

$$d_d + d_{an}$$

After training optimize the features for efficient classification using following procedure.

Input: Packets (p), and sequence number Seq_num (sq-n), Classification Rule Set {R={r1,r2,r3,.....}}.
Output: Intruder detection based on rules
Step -1: Initially Extend Original classification rule set {R}
Step-2: Initially extended rule set E=∞, and then insert rule set E=Insert (R,E),
Step -3: For all Rule Structure Er from E.
Step 4: Compare and calculate each match rule from original rule set and matching rule set i.e. Mi = Mu; where Mi is super rule set and Mu is sub rule set from overall rule set.
Step -5: Repeat 2,3,4 step for each packet transfer from one to another node with respect to packet header(which contains source_ip and destination_ip)
Setp-6: Each client header check with original rule set with seq_num.
Step -7: Increase and classify intruder client based on matching rule set Er with Mu mobility in sub rule set.
Step -8: Notify Packet loss where intruder detect from original data set.

Algorithm 1. Optimized procedure to detect attacker

The straight mapping of info and yield tests is accomplished utilizing a back spread neural system grouping approach.

Based on above procedure, proposed approach decreases error rate, weight and edge estimation of transaction layers in neural system. Estimation attack sequences based on rules related to attack with error rate at each node to improve performance of network The separated highlights from the arrangement of hubs of a MANET are isolated into preparing, approval and testing highlights. If there should be an occurrence of preparing mode, the notable highlights from both pernicious and genuine hubs are encouraged into the structured neural system to get the prepared examples or examples. Approval mode is used to decide if the preparing of the MANET is sufficient to decrease the error rate. After the approval mode is executed, the highlights from every hub in the system are tried utilizing prepared and approval examples to accomplish low error rate.

IV. EXPERIMENTAL EVALUATION & RESULTS

In this section, we describe performance of approach with respect to different traditional approaches with respect to data delivery ratio in detection of hybrid attacks i.e. Sybil, DDOS, woemhole and other attacks in wireless based vehicular ad hoc networks. Basic simulation parameters described in table 1.

Property	Value
Coverage Area	1700*1800
Number of Nodes	22
Simulation Time	35S
Transmission Range	350 m
Mobility Speed	0-30m/sec
Number of attacker nodes	03
Check point nodes	4 nodes(Fixed)

Table. Description of different parameters in wireless ad hoc networks.

Using above descriptive parameters develop simulation parameters and compare with AODV, improved AODV and hybrid approach with different node communication with knowledge based discovery datasets. Results appeared in our simulation as follows: Packet loss with different nodes described figure 4.

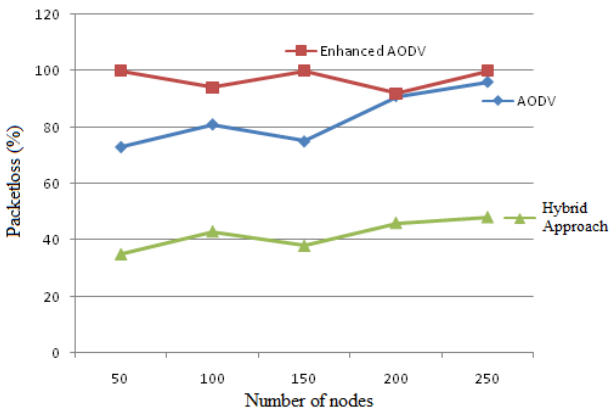

Figure 4. Performance of hybrid approach in terms of packet loss with different nodes.

Throughput analysis of different approaches with respect to different node communication with efficient routing between nodes in network communication shown in figure 5.

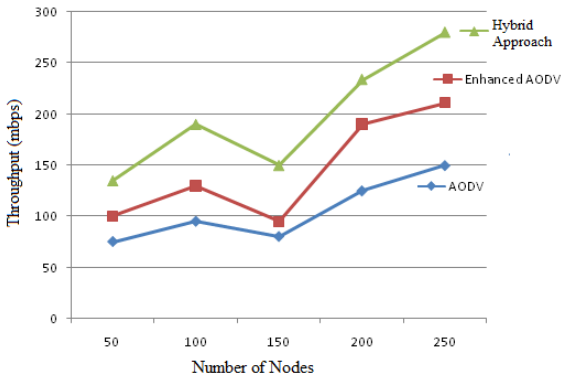

Figure 5. Performance of throughput with respect to different nodes.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Time efficiency for efficient data transmission with respect to hybrid approach and other approaches shown in figure 6.

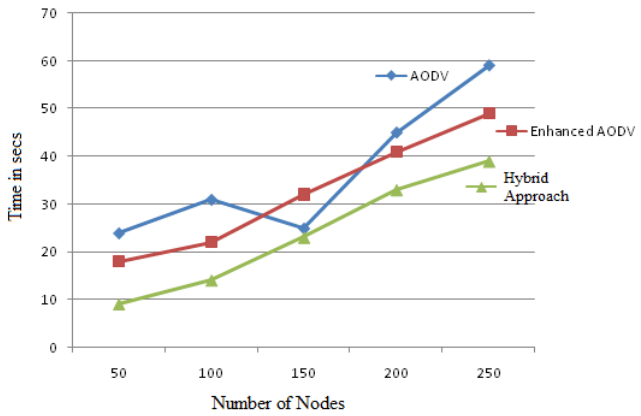

Figure 6. Performance of time comparison in wireless ad hoc networks.

Based on above results Hybrid approach give better solution for efficient data transmission with throughput analysis in wireless ad hoc network communication.

V. CONCLUSION

In this paper, introduce Hybrid approach which consists classification approach for feature comparison which attack describes in wireless ad hoc networks and AODV protocol for efficient routing between nodes for dynamic data transmission in wireless ad hoc networks. This approach gives better and accurate results with respect to packet delivery ratio, throughput and other parameters in wireless ad hoc networks. Based on Hybrid approach, it detects DDOS, Sybil and other related attacks in wireless vehicular ad hoc networks.

REFERENCES

1. T. Kavitha & K. Geetha & R. Muthaiah, “India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach”, Journal of Medical Systems (2019) 43:179.
2. K. Murugan and P. Suresh, “E_cient Anomaly Intrusion Detection Using Hybrid Probabilistic Techniques in Wireless Ad Hoc Network”, International Journal of Network Security, Vol.20, No.4, PP.730-737, July 2018 (DOI: 10.6633/IJNS.201807 20(4).15).
3. Moudni, H., Er-Rouidi, M., Mouncif, H., and El Hadadi, B., Performance analysis of AODVrouting protocol in MANET under the influence of routing attacks. Proceedings of 2016 International Conference on Electrical and Information Technologies, 2016.
4. Gopalakrishnan, S., and Kumar, P., Performance analysis of malicious node detection and elimination using clustering approach on MANET. Circuits and Systems. 7:748–758, 2016.
5. Kavitha, T., and Muthaiah, R., Position aided cluster based routing for extending MANET lifetime. Res. J. Pharm. Biol. Chem. Sci 8(1):1436–1449, 2017.
6. Petersen, E., To, M. A., andMaag, S., A novel online CEP learning engine for MANET IDS. IEEE 9th Latin-American Conference on Communications (LATINCOM), Guatemala City, Guatemala, 2017.
7. Chang, J.-M., Tsou, P.-C., Woungang, I., Chao, H.-C., and Lai, C.- F., Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J. 9(1):65–75, 2015.
8. Patel, K. S., and Shah, J. S., Detection and avoidance of malicious node in MANET. International Conference on Computer, Communication and Control (IC4), Indore, India, 2015.
9. R. Mitchell and I. R. Chen, \Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 16{30, 2015.
10. A. Mitrokotsa and C. Dimitrakakis, \Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," Ad Hoc Net-works, vol. 11, pp. 226{237, 2013.
11. N. Mohd, S. Annapurna, H. S. Bhadauria, \Taxonomy on security attacks on self configurable networks," International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 44{52, 2015.
12. F. Nabi, M. M. Nabi, \A process of security assurance properties unification for application logic," International Journal of Electronics and Information Engineering, vol. 6, no. 1, pp. 40{48, 2017.
13. S. OzgeCepheli G. Kurt, \Hybrid Intrusion detection system for DDoS attacks," Journal of Electrical and Computer Engineering, vol. 2016, pp. 1{8, 2016.
14. K. Pavani and A. Damodaram,. "Multi-class intrusion detection system for MANETs," Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 93{98, 2015.
15. E. M. Shakshuki, N. Kang and T. R. Sheltami,\EAACK - A secure intrusion-detection system for MANETs," IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089{1098, 2013.
16. N. Shah and S. Valiveti, \Intrusion detection systems for the availability attacks in ad-hoc networks," International Journal of Electronics and Computer Science Engineering, vol. 1, no. 3, pp. 1850{1857, 2012.
17. T. Sheltami, A. Basabaa and E. Shakshuki,\A3ACKs: Adaptive three acknowledgments intrusion detection system for MANETs," Journal of Ambient Intelligence and Humanized Computing, vol. 5,no. 4, pp. 611-620, 2014.
18. B. Subba, S. Biswas, S. Karmakar, \Intrusion detection in mobile ad-hoc networks: Bayesian game formulation," Engineering Science and Technology, vol. 19, pp. 782{799, 2016.
19. M. Usha and P. Kavitha, \Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classi_er," Wireless Networks, vol. 23, no. 8, pp. 2431{2446, 2017.2