JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Efficient Approach with Secure Protocol for Detection and Prevention of Wormhole Attack in VANET Systems

[1]Kavita Ranjan[1], [2]Prof. Prabhat Sharma

[1]Research Scholar, [2]Assistant Professor

Department of Electronics and Communication Engineering,

Oriental Institute of Science and Technology, Bhopal, India

Abstract : Wireless network application and communication performance is increasing day by day. There is an increasing threat of attacks on the vehicular Ad-hoc Networks (VANET). Worm hole attack is one of the security threat in which the traffic is redirected this type of node that honestly does no longer exist inside the network. This paper presents wormhole attack protection using neural network (NN) and "On-Demand Multicast Routing Protocol (ODMRP)" VANET environment. This research work consider total number of nodes upto 100, where some of source node and some of destination node. The overall simulation time is reduced by proposed approach. There are two scenarios to calculate performance parameters. First is when consider worm hole attack another is when consider without attack. Proposed algorithm achieved significant better result than previous approach. Therefore proposed approach gives better result in terms of packet delivery ratio, end to end delay and throughput both case of attack for attack and without attack.

IndexTerms **- Wireless, ODMRP, Wormhole, Attack, NN, Routing, VANET, DOS, DDOS.**

I. INTRODUCTION

Road traffic accidents and their sequences increase dramatically worldwide and thus raising a demand for solutions to providing safety and control of vehicles on road when driving. This is one of the top priorities for modern countries focusing on enhancing citizens' quality of life by developing an Intelligent Transport System (ITS). Vehicular Ad hoc NETworks (VANETs) are recognized to be effective in realizing such a concept. Identifying the rising business applications of the MANET's network technology has perpetually been an elusive proposition at the best. The three on top of mentioned wireless technologies - cellular telephone, wireless web and MANETs networks - it's so the MANETs network technology that has been the slowest to materialize, a minimum of within the business domain. This can be quite stunning since the construct of MANET's wireless networking was born within the early 70's, simply months once the thriving preparation of the Arpanet, once the military discover the potential of wireless packet shift. Packet radio systems were deployed abundant before any cellular and wireless computer network technology.

A continue progress within the development and preparation of economic MANET's applications. Main reason is that the initial applications situations weren't directed to mass users. In fact, till recently, the driving application was instant preparation in using unfriendly, remote infrastructure-less area. Early agency packet radio situations were systematically that includes dismounted troopers, tanks and ambulances. A recent extension of the field is that the Homeland Security situation, wherever remote-controlled vehicles (UGVs and UAVs) are chop-chop deployed in urban are aggressive to man, say, to determine communications before causing within the agents and medical emergency personnel.

Recently a vital new construct has emerged which can facilitate extend MANETs networking to business applications, namely, the construct of timeserving MANET networking. This new trend has been partly prompted by the recognition of wireless telephone and wireless LANs, and therefore the recognition that these techniques have their limits.

Another necessary are that has propelled the MANETs construct is detector nets. Detector nets mix transport and process and amplify the necessity for low energy operation, low kind issue and low value - thus, these are specialized Manet's solutions. Still, they represent a really necessary growing market. Within the development we have a tendency to elaborate on two applications, the field and therefore the urban and field grid.

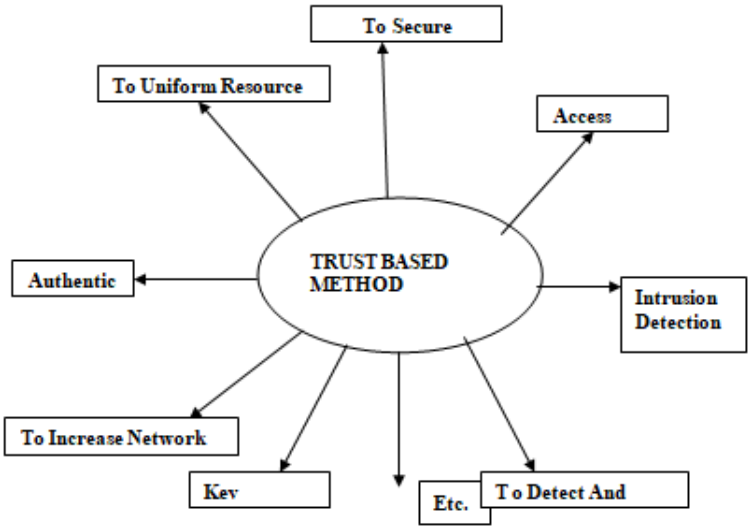

Figure 1: Design purposes of Trust-based Methods

II. PROPOSED METHODOLOGY

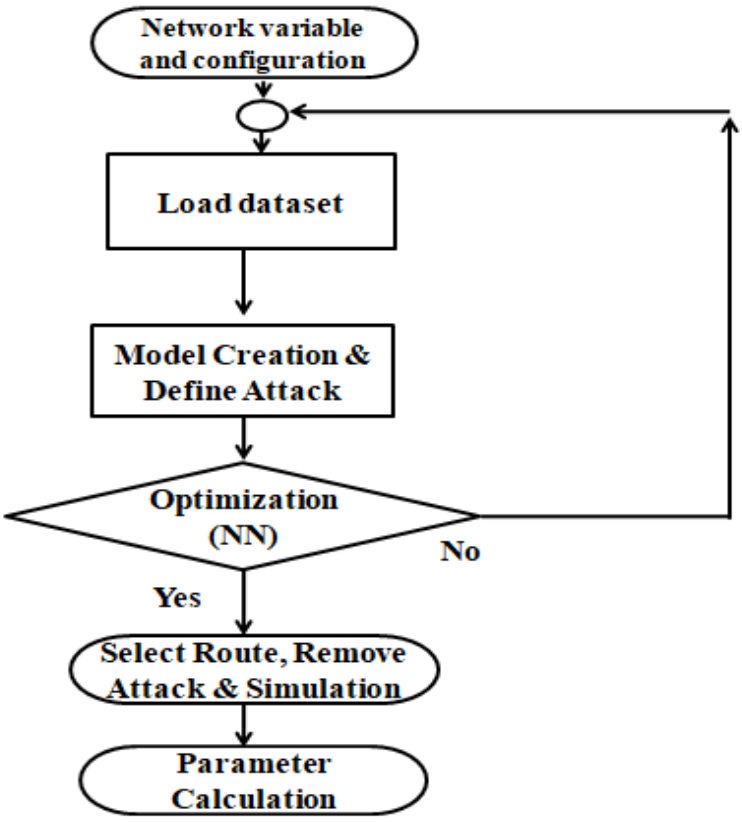

Figure 2: Flow Chart

Algorithm:

Step-1: Reading configuration, runtime variables total packets generated in the simulation
Step-2: Load data set, MAC protocol, Agents used in this simulation
Step-3: Creation of network model and introduce 2 worm-hole attack nodes
Step-4: Optimization of attack node using neural network methodology. Then due to high security such attacking node is identified and removed or stop.
Step-5: Select route using ODMRP protocol then update topology matrix, and update plot graph and simulation of nodes in environment.
Step-6: Various simulation parameters calculation

Simulation constants ----------
NODES = 100 ; total nodes in simulation
SENDERS = 30 ; total senders in simulation

RECEIVERS =20 ; total receivers in simulation

Global variables ----------
SIMTIME = 1000 ; simulation time, ms
SAMPLING = 100 ; network event update, ms
DELAYPLOT = 10 ; delay in plot update, ms
SQUARE = 200 ; square area, m
SPEED = 14 ; max speed of movement, m/s
RADIO = 200 ; range of the radio, m
LOSS = 0 ; loss percent per link, %
Define attacks ----------
Attacker node 1 at n1=8
Attacker node 2 at n2=21
Create network and Route Discovery:
Optimization based on iteration approach
Apply neural network ----------
Attack identified and fixed, Define type of a sent packet
Supplementary info of the Node (bottom left to the Node)
Define Topology, keep Node coordinates, Select route using ODMRP protocol
Enable real RF range calculation based on PHY
Carrier frequency, Hz, enable MAC protocol, all packets delivered successfully
Calculate packet delivery ratio, Total packet sent and receiver etc.

III. SIMULATION RESULTS

The usage of the proposed calculation is done over MATLAB 9.4. The ad-hoc network and communication commands and function such us to utilize the capacities accessible in MATLAB Library for different techniques like moving, scaling and so forth.

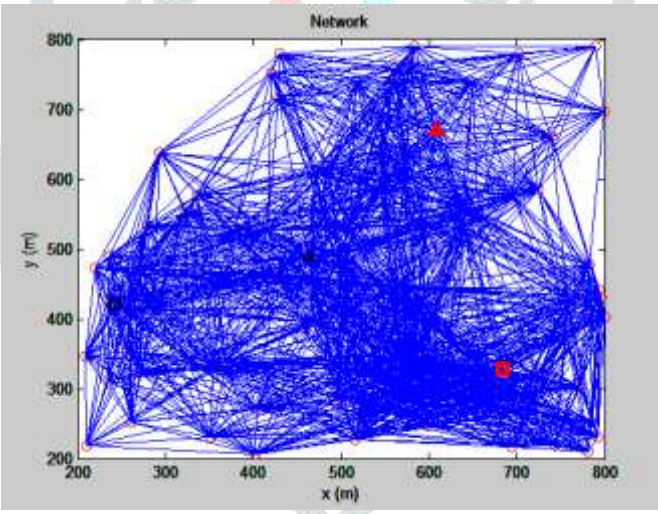

Figure 3: Network model creation and attack introduce

This figure shows the attack introduce, here node number 8 and node number 21 is assigned as a wormhole attack

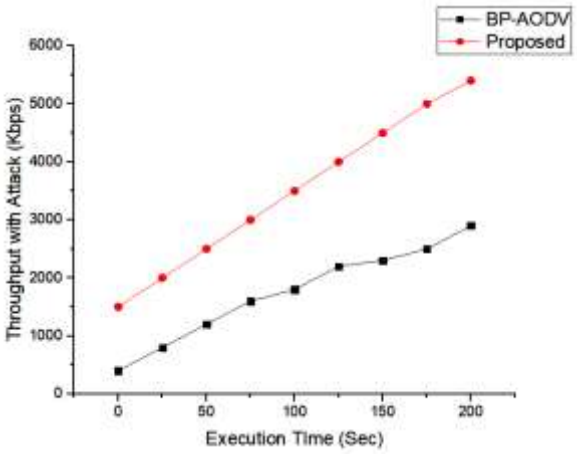

Figure 4: Throughput with attack

This figure shows throughput with attack condition. Proposed algorithm achieves upto 5400Kbps while previous it achieves upto 2600Kbps.

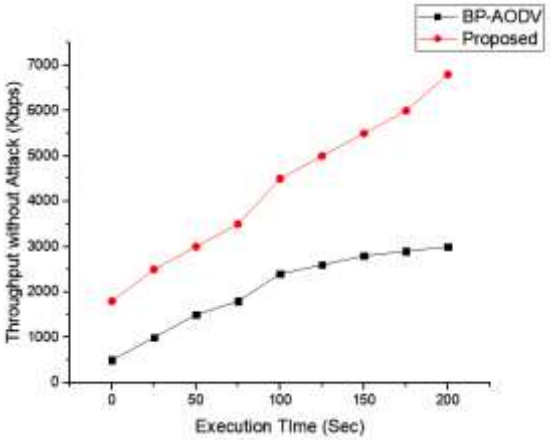

Figure 5: Throughput without attack

This figure shows throughput without attack condition. Proposed algorithm achieves upto 6800Kbps while previous it achieves upto 2800Kbps.

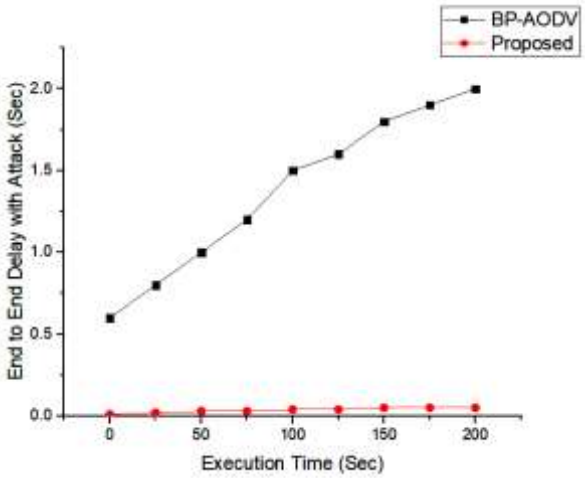

Figure 6: End to End Delay with attack

This figure shows end to end delay with attack condition. Previous delay achieved upto 0.2 Sec while proposed algorithm reduced delay time and it achieved upto 0.05Sec.

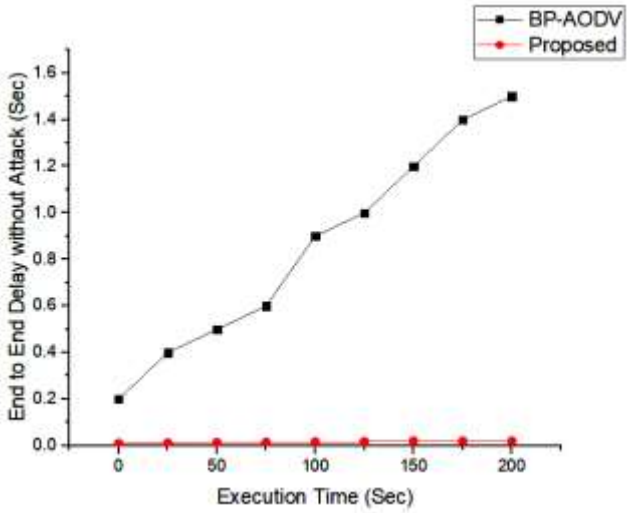

Figure 7: End to End Delay without attack

This figure shows end to end delay with attack condition. Previous delay achieved upto 0.18 Sec while proposed algorithm reduced delay time and it achieved upto 0.01 Sec.

Table 1: Comparison of proposed work with previous work

Sr No.	Parameters	Previous Work [1][2]	Proposed Work
1	Methodology	Key agreement Protocol	ODMRP & NN Algorithm
2	Protocol	MAC and BP-AODV	ODMRP
3	Number of nodes	100	100
4	Packet size (B)	1000	1024
5	Source node (Avg)	15	20
6	Destination node (Avg)	15	20
7	Simulation time with attack (Sec)	200	135
8	Simulation time without attack	190	83
9	Packet delivery ratio with attack	0.9	3
10	Packet delivery ratio without attack	1	6
11	End to End delay with attack (sec)	2	0.05
12	End to End delay without attack (sec)	1.5	0.01
13	Throughput with attack	2600	5400
14	Throughput without attack	2800	6800

IV. CONCLUSION

A vehicular ad-hoc network (VANET) comprises a dynamic set of self-organizing mobile devices or nodes that directly communicate to each other without any fixed infrastructure. Thus, nodes in VANET perform the tasks of both hosts and routers to forward packets toward their destinations based on the employed routing protocol. Routing protocols utilized by VANET can be classified based on topology into: proactive, reactive, and hybrid protocols. This paper presents wormhole attack protected On-Demand Routing Protocol with authentication algorithm for VANIT. This research work consider total number of nodes upto 100, where some of source node and some of destination node. Proposed method that is “On Demand Multicast Routing Protocol” and NN for optimization gives significant better performance than previous approach.

REFERENCES

1. C. Chen, Y. Chen, C. Lee, Y. Deng and C. Chen, "An Efficient and Secure Key Agreement Protocol for Sharing Emergency Events in VANET Systems," in IEEE Access, vol. 7, pp. 148472-148484, 2019, doi: 10.1109/ACCESS.2019.2946969.
2. O. R. Ahutu and H. El-Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Vehicular ad-hoc networks," in IEEE Access, vol. 8, pp. 63270-63282, 2020, doi: 10.1109/ACCESS.2020.2983438.
3. D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in VANET," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-8.
4. R. Kolandaisamy, R. M. Noor, M. R. Zaba, I. Ahmedy and I. Kolandaisamy, "Markov Chain Based Ant Colony Approach for Mitigating DDoS Attacks Using Integrated VANET Mode Analysis in VANET," *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*, Chennai, India, 2019, pp. 1-5.
5. B. Luo, X. Li, J. Weng, J. Guo and J. Ma, "Blockchain Enabled Trust-based Location Privacy Protection Scheme in VANET," in *IEEE Transactions on Wireless Technology*.
6. Y. Zeng, M. Qiu, J. Niu, Y. Long, J. Xiong and M. Liu, "V-PSC: A Perturbation-Based Causative Attack Against DL Classifiers' Supply Chain in VANET," *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, New York, NY, USA, 2019, pp. 86-91.
7. W. Li and D. Zhang, "RSSI Sequence and VANET Driving Matrix Based Sybil Nodes Detection in VANET," *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Chongqing, China, 2019, pp. 763-767.
8. Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Wireless Ad Hoc Network," in *IEEE Access*, vol. 7, pp. 154560-154571, 2019.
9. J. R. and N. S. Bhuvaneswari, "Malicious node detection in VANET Session Hijacking Attack," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2019, pp. 1-6.

10. M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," in *IEEE Access*, vol. 7, pp. 158481-158491, 2019.
11. S. Kumar and K. S. Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, London, United Kingdom, 2019, pp. 89-94.
12. A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6.