Feature Reduction in MANET using Machine Learning Language

T.J. Nagalakshmi, V. Veeramanikandan, S. Ravichandran

Abstract*: *Mobile ad-hoc network (MANET) is an infrastructure-less network. Therefore, MANET involves a selection of exact security schemes to notice the false entrance of the mischievous nodes. Along these lines, we require solid instrument to identify these pernicious nodes and to arrange ordinary and irregular nodes based on the conduct or performance of nodes. Machine learning system nowadays used to built a best IDS for recognizing exception or misbehaving nodes rapidly and precisely give grouping by watching conduct of those nodes in the system. In MANET system, numbers of parameters are taken for analysation. It makes the IDS system complex. To avoid this complexity many techniques are derived for feature reduction. In this proposed work, we are testing how feature reduction can be done using Python machine learning program.

Keywords*: *Portable impromptu system, Machine Learning Procedures, Bundle Dropping Assaults..

I. INTRODUCTION

A wireless Ad-hoc network contains wireless nodes transmitting lacking require for a central management. A gathering of self-directed nodes which transmit with every other with making a multi-hop radio system as well as managing property in a deconcentrated way [1]. There is no stationary transportation for the system, for example a base station. The plan of this system is to maintain healthy as well as proficient process in mobile wireless networks by comprising rootling practicality into mobile nodes [2]. Fig. 1 demonstrates an instance of an ad hoc network, here there are several compounding of communication fields for dissimilar nodes. From the sender to the receiver, there can be dissimilar routes of association at a specified point of time. Here, every node generally has a restricted field of communication with the elliptical ring about every node [3]. A sender communicates information to node B except B can communicate information moreover to C or D. It is a difficult job to select an actually superior method to set up the association among a sender as well as receiver thus they can travel approximately also broadcast strong transaction. Many routing protocols are available such as AODV, DSR, and DSDV. All these protocols are improved by many performance analysation techniques [4].

Revised Manuscript Received on December 11, 2019.
***** Correspondence Author
T.J. Nagalakshmi *, Asst. Prof., Dept. of ECE, Saveetha School of Engineering, Chennai, India.
V. Veeramanikandan , Dept. of ECE, Saveetha School of Engineering, Chennai, India.
Dr. S. Ravichandran, HOD & Prof., Computer Science Department, Annai Fathima College of Arts & Science, Madurai, India.

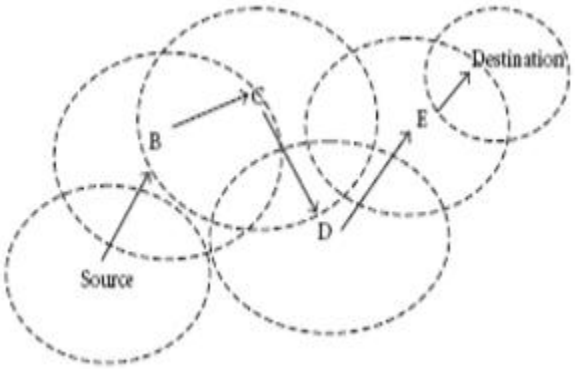

Fig. 1. Adhoc Network Model

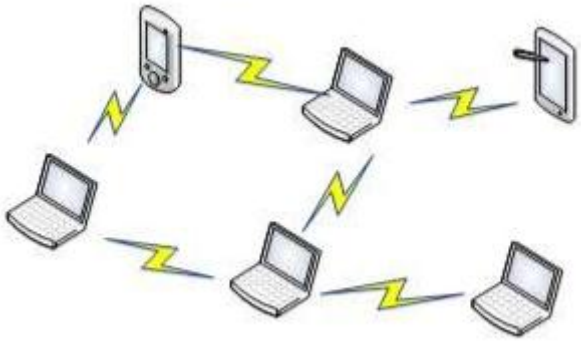

Fig. 2. MANET architecture

Fig 2 explains the MANET architecture. All nodes are not fixed and they won't follow the fixed connectivity. Depending upon their urgency, traffic, size of packets to be delivered the routing path will change [5]. In this wireless architecture intruder can attack is possible. Any hacker can easily establish their route in this architecture and they can hack the information. Types of attacks are possible. It is broadly classified into (i) Active Attack (ii) Passive Attack [6] are shown in figure 3.

A. Active attack

Active attacks are harmful to the network and make serious damages to the entire network. Various activities of active attacks are altering, interjecting, devising, inventing and losing of information or routing packets [7]. This type of attack can be caused by single instance created by lone attacker or series of instances by group of attackers.

Some of the active attacks are: Black hole Attack, Denial of Service attack, Man in the Middle attack, Wormhole Attack [8].

Wormhole attack is one type of severe attack that alters the routing process and form a tunnelling between two networks. The worm hole attack can be launched in two mode hidden mode and participation mode .In Hidden mode the attacker do not show the identity and remain hidden [9]. In this mode attacker acts as a two simple Trans receiver it receives the packet from one end and replicate to another end and form a virtual link between two nodes and drop the entire packet. In Hidden mode attacker do not require cryptographic keys. In Participation mode attacker require cryptographic key, without virtual link it is capable of transferring the data from one node to another with smaller hop count [10].

B. Passive Attack

This type of attacks does not disturb or harm the network topology or operation of the routing protocol. These attacks are meant to learn and gain knowledge about the network topology, its traffic pattern and type of activities carried out in the network. These things would help the attacker to locate participating nodes or identify the important node [11-12].

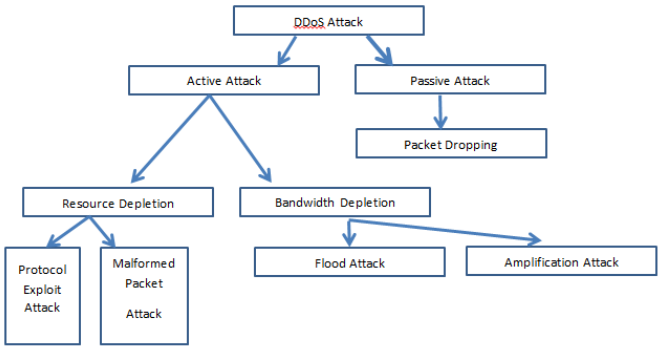

Fig. 3. Kind of Assaults in MANET

Many features are taken for analization of the intruder detection system. In KDD CUP dataset we can analyse 42 parameters. But as the number of features are more system will be more complicated. So we are now reducing the number of features by feature reduction technique [13-14].

II. PROPOSED WORK

In this proposed work, we are analyzing an ad hoc network which is having 100 nodes, using AODV routing protocol. Simulation area for this architecture is 1000*1000. In this work we are analyzing with network layer attacks. The simulation parameters are shown in Table 1.

By using ns2 simulator tool with the wormhole attack, simulation was performed. And the following parameters are measured:

A. Percentage of Route changed (PRC):

It defines the percentage of route changes in the particular interval. It is the ratio between sum of routing entries increased and routing entries deleted during particular interval to total number of routing entries.

$PRC = (|RE_2 - RE_1| + |RE_1 - RE_2|) / |RE_1|$

RE1 - number of routing entries in routing table at time t1

RE2 - number of routing entries in routing table at time t2.

$|RE_2 - RE_1|$ - number of path entrances increased through the instant period (t2 – t1)

|RE1 – RE2| - Number of path entrances deleted through the instant period (t2-t1)

B. Percentage of Hop Count changed (PHC):

It defines the sum of hop count in the entire routing entries changes through the instant period (t2 –t1)

$PHC = (HC_2 - HC_1) / HC_1$

HC_1– Sum of hop counts of all routing entries at time t1

HC2 – Sum of hop counts of all routing entries at time t1

C. Maximum Changes in Sequence Number (Max_Seq):

It defines the number of maximum changes in sequence number in the routing table for all active routes

D. Maximum Changes in Hop Count (Max_Hop):

It defines the number of maximum hop count changes in the routing table for all active routes.

E. Average Difference in Sequence Number (Diff_Seq):

It defines the average difference between the source node sequence number and sequence number in routing table entry.

F. Average Difference in Hop Count (Diff_HC):

It defines the average difference between the source node Hop count and sequence number in routing table entry

G. Percentage of Delay changed (PDC):

It defines the average value of delay changed in percentage for all received packets during the time interval t1 to t2

$PDC = |d_2 - d_1| / d_1$

d1 – Average packet receiving delay at time t1

d2 – Average packet receiving delay at time t2

H. Percentage of Receive Power changed (PRPC):

It defines the average value of receive power changed in percentage for all received packets during the time interval t1 to t2

$PRPC = |P_2 - P_1| / P_1$

P_1 – Average packet receiving power at time t1

P_2 – Average packet receiving power at time t2

I. Percentage of Drop Ratio changed (PDRC):

It defines the average value of packet drop ratio changed in percentage for the node during the time interval t1 to t2

$PDRC = |DR_2 - DR_1| / DR_1$

DR1 – Average packet dropping ratio at time t1

DR2 – Average packet dropping ratio at time t2

J. Percentage of Neighbour count changed (PNCC):

It defines the average value of neighbour count changed in percentage for the node during the time interval t1 to t2

$PNCC = |NC_2 – NC_1| / NC_1$

NC1 – Average neighbour count of the node at time t1.

NC2 – Average neighbour count of the node at time t2

K. Percentage of average difference in neighbour count with all neighbours changed (PDNCC):

It defines the average value of difference in neighbour count with all neighbours changed in percentage for the node during the time interval t1 to t2

$PDNCC = |DNC_2 – DNC_1| /DNC_1$

DNC1 – Average Difference in neighbour count with all neighbours of the node at time t1

DNC2 – Average Difference in neighbour count with all neighbours of the node at time t2

L. Percentage of Packet Sent Count changed (PPSC):

It defines the average value of neighbour count changed in percentage for the node during the time interval t1 to t2

$PPSC = |PS2 – PS1| / PS1$

PS1 – Number of packets sent by the node at time t1

PS2 – Number of packets sent by the node at time t2

Table 1 shows the simulation parameters of this system.

System Construction:

Simulation tool	ns2
Routing Protocol	AODV
Number of Nodes	100
Simulation area	1000*1000m
Simulation period	200s
Connection type	CBR
MAC type	802.11
Packer Size	512 bytes
Initial Energy	100J
Attacker	1-5
Antenna model	Omni Antenna
Number of Attacker	1-10

Table 1: Simulation parameters

III. RESULT AND DISCUSSION

NS2 is used for region is 1000*1000 meter. There are 100 nodes deployed in random position .All the node are AODV changed transmitting the route request for destination node In this scenario node 10 is used source of the worm hole and node 45 is used as worm hole sink to apply tunnel between them. In this experiment, we are analyzing the relationship between all the parameters. We analysed with hyper plane method and heat map method. From both the methods the features which can mainly affect the IDS is Receiver Power, Diff_sent, Percentage of Hop count changed. These, can be inferred from the plots shown in Fig 4 to 11.Fig 11 gives the information about the relationship between the features in network layer in terms of heat map.

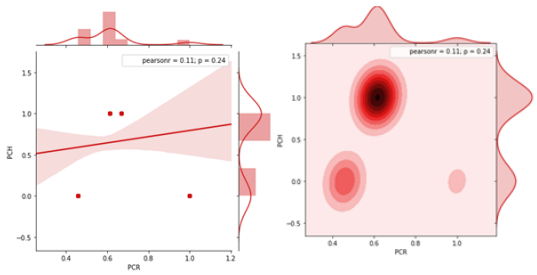

Fig. 4. Plot between PCH Vs PCR and its heat map

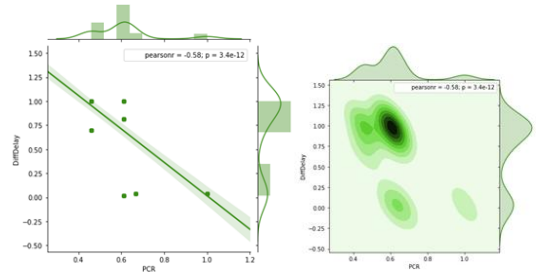

Fig. 5. Plot between PCR VsDiffDelay and its heat map

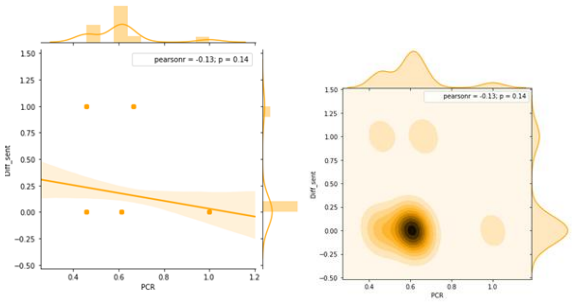

Fig. 6. Plot PCR VsDiff_sent and its heat map

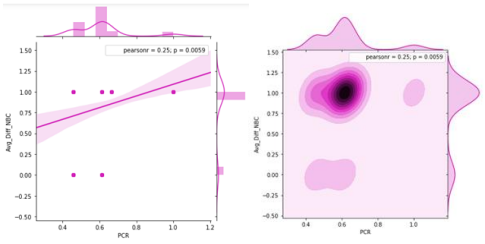

Fig. 7. Plot Avf_diff_NBCVs PCR and its heat map

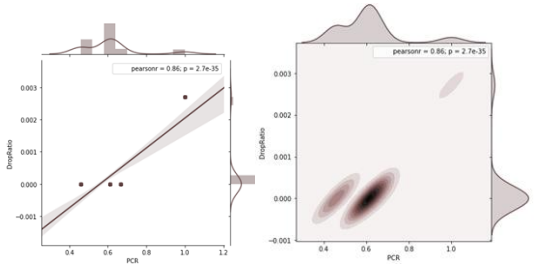

Fig. 8. Drop Ratio Vs PCR and its heat map

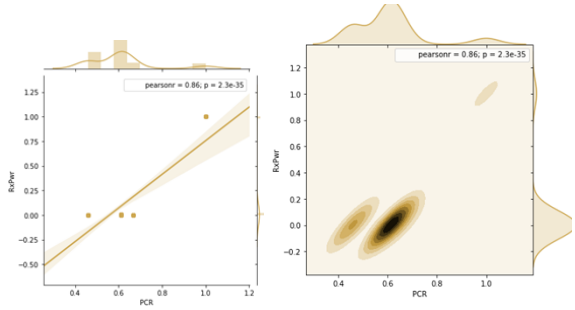

Fig. 9. Receiver Power Vs PCR and its heat map

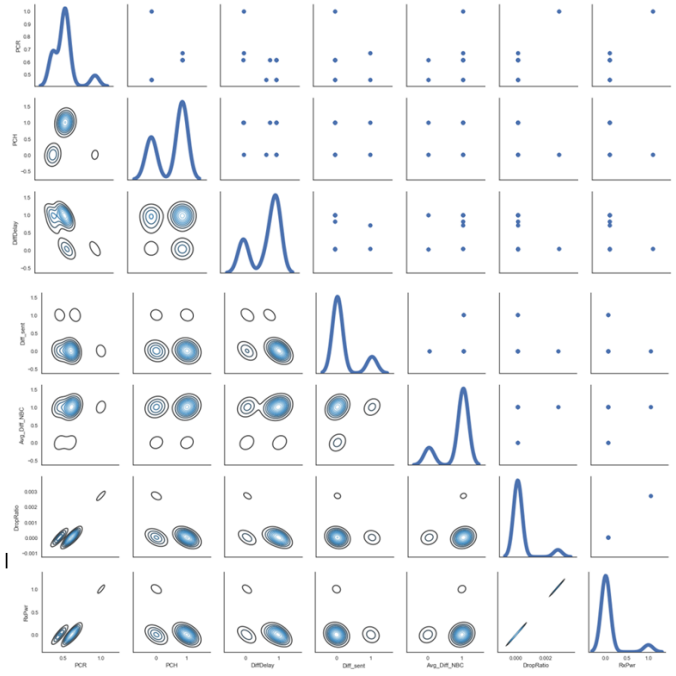

Fig. 10. Relationship between all parameters.

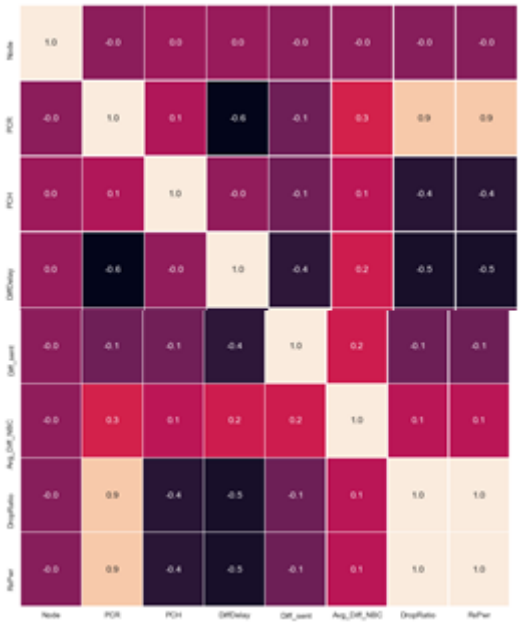

Fig. 11. Heat Map

IV. CONCLUSION

The features are reduced to (1)RxPwr (2)Diff_Sent (3) PCH. In this work, we reduced the number of features that can be used in Intruder Detection System. In the enhanced next work, the feature set is used in IDS and attacker nodes can be detected. And the accuracy of the result is analysed by applying many algorithms.

REFERENCES

1. Michie, Donald, David J. Spiegelhalter, and C. C. Taylor. "Machine learning." *Neural and Statistical Classification 13* (1994).
2. Çelebi E. Performance evaluation of wireless multi-hop ad-hoc network routing protocols. pdf. 2002. http~ ecelebi/esim
3. Basangi,S.,Conti,M.,Giordano,S.andStojmenovic,I.,"Mobile adhoc networking" , *IEEE Press, Wiley- Interscience, IEEE*,2004 pp-282,.
4. B Li,Wenjia,AnupamJoshi,andTimFinin.,"SMART: AnSVM-based Misbehavior DetectionandTrust Management Frameworkfor Mobile Adhoc Networks.", *In MILITARYCOMMUNICATIONS CONFERENCE,20Il-MILCOM20Il, IEEE,2011*.,pp-1102-1107
5. R. Anto Pravin, Umamaheswari, "Preserving Privacy Using an Unobservable Secure Routing Protocol for MANETs," *International Journal of MC SquareScientific Research, vol.5, no.1, 2013, pp. 1-10.*
6. Michie,Donald,DavidJ.Spiegelhalter,andCharlesC.Taylor., "Machine learning, neural and statistical classification.", 1994..
7. J Dr. SaurabhMukherjeea, NeelamSharmaa, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction", *SciVerse Science Direct, Procedia Technology 4 (2012),pp*- 119 – 128..
8. Forster,Anna.,"Machinelearningtechniquesappliedto wireless ad-hoc networks:Guide and survey.",In Intelligent Sensors, Sensor Networks and Information, 2007, ISSNIP2007,*3rdInternationalConferenceon, IEEE, 2007*,pp-365-370.
9. JayshreeJha, LeenaRagha, Ph.D, "Intrusion Detection System using Support Vector Machine", *International Journal of Applied Information Systems (IJAIS)* – ISSN : 2249-0868.
10. Weston, J., Mukherjee, S., Chapelle, O., Pontil, M., Poggio, T. and Vapnik, V., 2001. "Feature selection for SVMs". *In Advances in neural information processing systems* , pp. 668-674.
11. Akbani,Rehan,TurgayKorkmaz,andG. V.S.Raju.,"A Machine Learning BasedReputation System for Defending Against Malicious Node Behavior.",*In GlobalTelecommunications Conference, 2008,IEEE GLOBECOM 2008,IEEE*,pp-1-5.
12. Deng, H., Zeng, Q.A. and Agrawal, D.P., 2003, October. "SVM-based intrusion detection system for wireless ad hoc networks" *In 2003 IEEE 58th Vehicular Technology Conference*. VTC 2003-Fall (IEEE Cat. No. 03CH37484) ,Vol. 3, pp. 2147-2151.
13. Kulothungan, K., Ganapathy, S., Yogesh, P. and Kannan, A., "An Agent based Intrusion Detection System for Wireless Sensor Networks Using Multilevel Classification" *International Journal of Modern Engineering Research (IJMER)*, 1(2), pp.55-60.
14. Patel,Meenakshi, SanjaySharma, and DivyaSharan., "DetectionandPreventionofFloodingAttackUsingSVM.",InCommunicationSystemsandNetworkTechnologies(CSNT),2013.*InternationalConference IEEE,2013*, pp-533-537.

AUTHORS PROFILE

Ms. T.J.Nagalakshmi ME., (Ph.D.), working as a Asst. Professor in Department of Electronics and Communication Engineering at Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu State, India. She has 11 years of teaching experiences in Engineering Colleges. She has published 20 papers in International journals and has presented in 5 International Conferences at various Engineering Colleges. Her areas of specialization are VLSI, Artificial Intelligence, Networks and Compilers.

Dr. S. Ravichandran, M.C.A., M.Phil., M.Tech., ME., Ph.D., working as a HOD & Professor in Department of Computer Science at Annai Fathima College of Arts & Science, Madurai, Tamilnadu State, India. He has 21 years of teaching experiences in various Colleges. He has published 20 papers in International journals, he has presented in 15 International Conferences & presented in 19 National Conferences at various Engineering Colleges. His areas of specialization are Cloud Computing, Artificial Intelligence, Networks and Compilers.

Veeramanikandan, is a UG student doing Electronics and communication Engineering programme in Saveetha School of Engineering, SIMATS, Chennai, India. His area of interest is wireless communication.