Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021: 2448-2456

Research Article

Multidimensional Metric Model (MANET-SPR) for assessing the effectiveness of the MANET Configuration

[1]K. Purnima [2]Dr. M.N.Giriprasad

Abstract

In Mobile Ad Hoc Networks (MANETs) the mobile nodes are connected and associated usually on an ad-hoc basis. Due to the nature of the formation of the network and connectivity, it is important to assess all the packets and associated metrics in order to find the vulnerabilities and optimal configuration of the network. The multidimensional metrics and models are the ways and means through which the existing MANET network can be analyzed for its optimality. So, it is important to develop an appropriate multi-dimensional evaluation framework for assessing the optimal configuration of MANET. This paper aims to present the basic introduction about MANET, the metrics, exploratory and some of the key variables collected from the real time MANET data. This paper also proposes a novel three dimensional metric model which would be helpful for assessing the effectiveness of MANET networks.

***Index Terms*—**MANET, METRICS, MULTI-DIMENSIONAL MODEL, FRAMEWORKS, PERFORMANCE, SECURITY, RELIABILITY, MACHINE LEARNING, CONFIGURATION

I. INTRODUCTION

There are many types of network models such as Vehicle Ad hoc Network (VANET), Mobile Ad hoc Network (MANET), and Virtual Private Network (VPN). This article deals with MANET.MANET networks do not rely on pre-established infrastructure and they are dynamically self-organized. In MANET, Mobile nodes play a dual role. Nodes are not just hosts that send or receive data;, they act as routers, maintain routing information and also forward & receive packets. MANET provides faster convergence because these networks are in a mobile environment;, moreover, nodes are moving faster since nodes join and leave frequently. This characteristic demands high network convergence in order to respond faster to the topology changes. MANET poses a lot of challenges for the network and security administrators. The Security of MANET or

[1] Research Scholoar, Jawaharlal Nehru Technological University Anantapur
,[2] Professor, Department of ECE, Jawaharlal Nehru Technological University Anantapur

any network is very important because that is the only way to maintain confidentiality, information

integrity and node authenticity.There will be multiple independent control variables like bandwidth, no. of users, network throughput, no. of firewalls and up time etc., to be considered as part of building the framework. All these metrics are required to develop the correct regression to see what parameter change is going to improve or stabilize the environment. In addition to some of the metrics discussed earlier, there is a need to address how network merging cost and delay cost can be reduced so that addressing delays will be reduced.

LITERATURE REVIEW

The following section will provide a detailed review of some of the novel contributions done by many researchers related to the subject of study. Dhar et al, emphasized that there is no fixed infrastructure for MANET. Since nodes are moving around with certain mobility, a static configuration or parameters won't be sufficient. So it is evident that new research is required to see how the configuration parameters can be made more dynamic by arriving at an optimal configuration and developing a framework that supports the nature of the MANET [1]. Karen et al, focused on the local operating conditions to identify how the node can independently observe the local operating conditions and select the best parameter values. Some of the possible considerations are performance and learning speed are important while maintaining accuracy [2].
Nitin et al briefly discussed the various routing metrics in MANET environments, especially lifetime parameters for the nodes. Metrics like node lifetime and router lifetime are taken into consideration in the proposed multi-dimensional metric model [3]. Yanli proposes a methodology to address the configuration in MANETs like IP configuration and how to generate a unique ID for MANETs. The authors also discuss the address reconfiguration in MANETs in case of duplication. This research work highlighted that network merging cost and delays can be reduced as part of the address configuration and reconfiguration. This research work focused on efficient node addressing and auto configuration, which were also evaluated and tested [4].
Kurram Naim et al talks about how the IOT framework can incorporate the MANET technologies along with wireless sensor networks, near field communications and RFIDs. This framework also tells about the routing protocols that describe their applicability towards the IOT realization. There exists a scope to realize the IOT trends in the current research work. Since the MANETs are in IOT based environments, focus on the identification of suitable network simulation environments with IOT models can be considered for building the prototype and simulation [5]. Gondi Yasoda et al, highlighted the routing challenges, the obstacles in finding routing and how A* signaling algorithm can improve route search and minimize the path laying cost and penalty of node availability. A* signaling algorithm can be further applied and extended in future research works, as this is the best search algorithm used in artificial intelligence. Better than linear algorithm, binary algorithm, breadth first search and depth first search algorithms. A* algorithm will be adapted to look for the optimal loads [6].

Manoranjani et al, highlighted three QoS parameters, including packet loss, network throughput and energy consumption. For arriving at optimal configuration parameters, incorporating QoS is very important. This proposed work considers QoS metrics like packet loss, network throughput and energy consumption and sees how this framework proactively monitors these variables and improves these parameters [7]. Baisakhi et al, discussed how we can train the parameters by expanding the acceptability Based Routing protocol and how different weighing parameters like battery power, security factor and degree of neighbor can be trained. In Machine learning, the primary focus is on how to train or improve the model, which is the important step towards deep

learning. There are two types of learnings, supervised and unsupervised. In supervised learning the variables and parameters are known and in unsupervised learning parameters are not known. So, giving more learning to understand parameters is necessary, so that the parameters can be learned & adjusted. A new algorithm can be proposed to predict the new parameter based on the existing training data set [8].

Rashiah et al, suggested to deploy cross-layer mechanisms to detect every possible attack targeting the data-link, network, transport, and application layers. This paper has also given us the directions to look at cross-layer mechanisms and see how configuration parameters can be seen as cross-layers with input sources, middle interfaces and system/network/output layers [9]. Husssain et al, reviewed and explained the importance of scalable and auto configurations of MANET. When the nodes are increasing and the environments are becoming dynamic, there is a need to look at the scalability factor as well as automatic adjustment of the configuration, so that the new users or connections can be accommodated. The proposed research work includes automatic forecast of scalable configuration parameters which can be forwarded to the right interfaces to make automatic correction and updates of the MANET configuration files and/or settings. The machine learning algorithms can be used to predict the future values based on the metrics collected in run time [10].

Nishani et al suggested that deploying machine learning algorithms plays a vital role in intrusion detection. Since the MANETs are ad-hoc and dynamic in nature with infrastructure less mode, there is a need to continuously monitor various attacks of intrusion to the network. The proposed framework should not only address scalability, auto configuration, reduction of error rate, and replay attacks but also consider the right mechanisms to handle the intrusion [11].

Purnima et al discussed the detailed literature review for predicting the optimal configuration. This review also confirms that ML based Intrusion detention systems can be considered in the proposed research works as there is an enhancement in technologies and security issues, in order to cope with the dynamic configuration to handle IDS effectively [12]. From the above literature review this work considered some of the following key metrics which are helpful for monitoring and supporting MANET network:

- Node Lifetime
- Route lifetime
- Accuracy
- Significance & sensitivity
- Learning speed
- Packet Loss
- Network Throughput
- Energy Consumption
- No. of Intrusions
- Path laying cost

The following section briefly discusses some of these metrics.

Node Lifetime is nothing but the duration of how long the node can participate in communication. The lifetime of a node begins when it first boots and ends when it is no longer able to communicate or perform any other basic task. Route lifetime is the link lifetime that is used to establish a route between the source and destination. It is defined as the time span at which the route is operational

and valid. Once the lifetime of the route expires it becomes invalid and is no longer operational. Accuracy represents how close a measurement comes to its true value. This is important because bad equipment, poor data processing or human error can lead to inaccurate results that are not very close to the truth or real value. Significance of the parameter is the importance of each parameter in the model used. Sensitivity of the parameter tells how sensitive the model is to fluctuations in the parameters and the data on which it is built.

Learning speed is the time taken by the system to learn or evaluate the result depending on the inputs provided. Sometimes packets don't make it to its destination. This loss in transit is referred to as packet loss. For most users, packet loss comes in the form of a slow document download, frozen video, or a gargled voice call. Network throughput is the actual capacity of a network that allows a certain amount of data to be passed from one point to another t within the specific amount of time. It is the rate of message delivery over a single channel. Energy Consumption aggregates based on the Power consumption of each node in the network. Path laying cost is the cost, i.e time taken and steps incurred in making path decisions by setting arbitrary metric values on the links along the path, end to end. Those values with lower numbers are indicated as better paths. Intrusions are malicious attacks, and suspicious or unauthorized activity. This is one of the important metrics which is considered as part of the proposed dimensional model.

MANET DATA ANALYSIS AND FEATURE SELECTION

Tables 1, 2 and 3 list the variables obtained by analyzing the real time data from a few popular web sites which contain the data sets related to MANET. A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. Each connection record consists of about 100 bytes. Attacks fall into four main categories – DOS, R2L, U2R, Probing.

feature name	description
duration	length (number of seconds) of the connection
protocol_type	type of the protocol, e.g. tcp, udp, etc.
service	network service on the destination, e.g., http, telnet, etc.
src_bytes	number of data bytes from source to destination
dst_bytes	number of data bytes from destination to source
flag	normal or error status of the connection
land	1 if connection is from/to the same host/port; 0 otherwise

wrong_fragment	number of ``wrong'' fragments
urgent	number of urgent packets

Table-1 : Basic MANET variables/features and the description

feature name	description
hot	number of ``hot'' indicators
num_failed_logins	number of failed login attempts
logged_in	1 if successfully logged in; 0 otherwise
num_compromised	number of ``compromised'' conditions
root_shell	1 if root shell is obtained; 0 otherwise
su_attempted	1 if ``su root'' command attempted; 0 otherwise
num_root	number of ``root'' accesses
num_file_creations	number of file creation operations
num_shells	number of shell prompts
num_access_files	number of operations on access control files
num_outbound_cmds	number of outbound commands in an ftp session
is_hot_login	1 if the login belongs to the ``hot'' list; 0 otherwise
is_guest_login	1 if the login is a ``guest''login; 0 otherwise

Table-2 : Second set of MANET variables/features and the description

Feature name	description	type
count	number of connections to the same host as the current connection in the past two seconds	continuous
serror_rate	% of connections that have ``SYN'' errors	continuous
rerror_rate	% of connections that have ``REJ'' errors	continuous
same_srv_rate	% of connections to the same service	continuous

diff_srv_rate	% of connections to different services	continuous
srv_count	number of connections to the same service as the current connection in the past two seconds	continuous
	Note: The following features refer to these same-service connections.	
srv_serror_rate	% of connections that have ``SYN'' errors	continuous
srv_rerror_rate	% of connections that have ``REJ'' errors	continuous
srv_diff_host_rate	% of connections to different hosts	continuous

Table-3 : Third set of MANET variables/features related to connections and the description

PROPOSED MANET MULTIDIMENSIONAL METRIC MODEL (MANET-SPR)

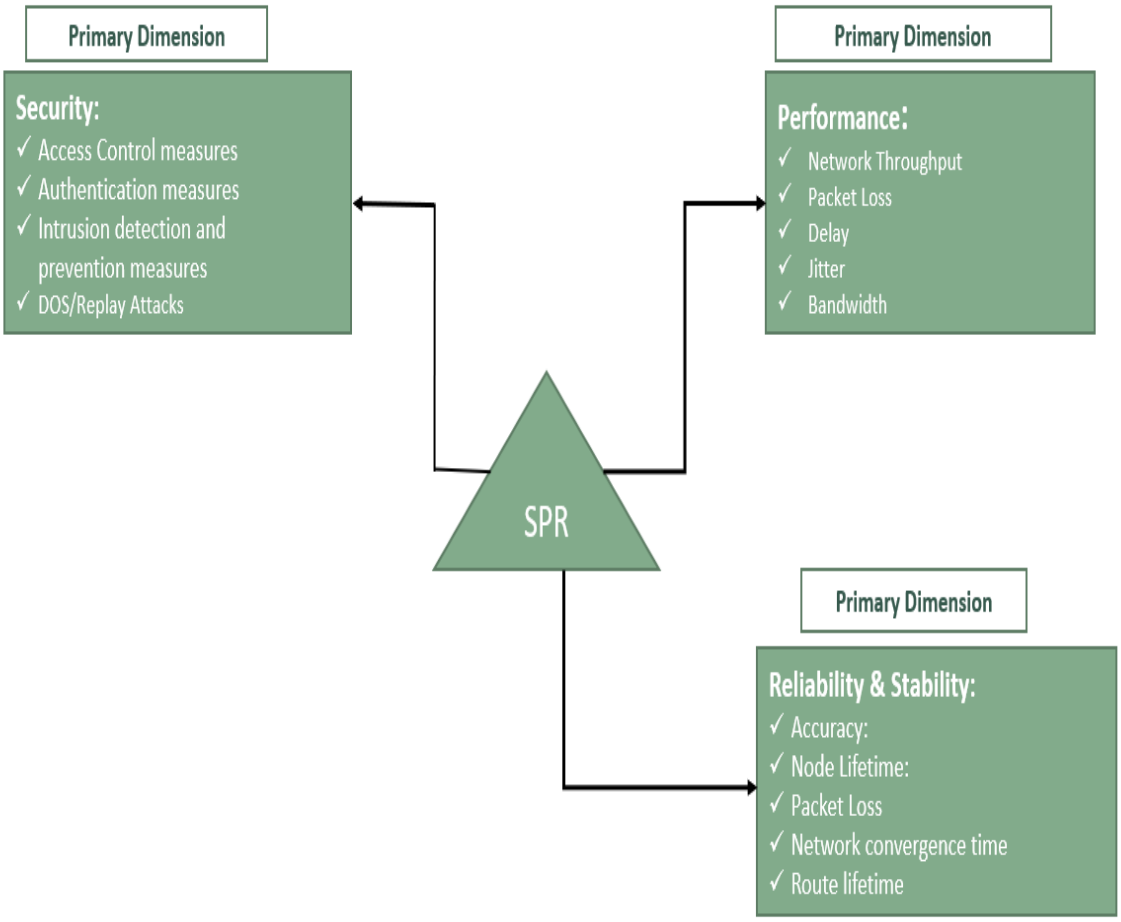

Figure-1 : MANET-SPR model

The above figure is the proposed MANET Multidimensional model which categorizes the assessment of MANET into three major dimensions or factors or views, namely, Security,

Performance and Reliability, As depicted in the figure, every dimension has the associated metrics, for example, security can be viewed and evaluated in terms of access control measures, intrusion detection measures and others. Similarly, the performance of MANET can be meausred based on the network throughput from the network and other metrics like delay or jitter. The third dimension Reliability and Stabiltiy deals with the Accuracy of the MANET networks. The proposed dimension can be used as an input to evaluate the given MANET network and data sets using a Machine learning classifier. The possible steps in using the proposed model for evaluation using the machine learning based classifier are given below:

- Decide the size of the real time MANET data – Number of rows/columns using the three dimensions
- Load/Import data into ML system
- Perform exploratory data analysis [EDA] and Normalize the data using standard Scaler function and Visualize the data to find the correlation between the variables
- Apply the data transformation/mapping to make any updates to the variables
- Split the preprocessed source dataset into training and testing datasets (Data Preparation)
- Develop the model and fit the ML prediction model (Modeling) using the SECURITY and RELIABILITY dimensions
- Predict the outcomes using the test data (Evaluation) using SECURITY and RELIABLIITY dimensions and the associated measures
- Identify the underlying MANET configuration used in the training data and compare the days and respective MANET configurations and choose the optimal firewall configuration
- Deploy the model

CONCLUSION AND FUTURE STEPS

Based on the extended literature review, real time data analysis on the data sets from MANET networks, it has been identified that certain metrics are vital for choosing the right performance and configuration prediction. Based on further study, this work proposed a novel and comprehensive three dimensional metric model to be used for evaluating and/or assessing the performance of the MANET system. Further research works can be carried out in applying this metric model and choosing right machine classifier to assess each dimension. When compared with all other dimensions, the security dimension is very important and the associated metrics should be taken into consideration for monitoring the intrusions and anomalies and other issues in order to predict the optimal MANET configuration.

REFERENCES

[1] Dhar, Subhankar. (2005). MANET: Applications, Issues, and Challenges for the Future. International Journal of Business Data Communications and Networking,1,pp 66-92.

[2] Karen Zita Haigh, Srivatsan Varadarajan, Choon Yik Tang (2006), Automatic Learning-based MANET Cross-Layer Parameter Configuration, WWASN2006

[3] Nitin Goyal, Alka Gaba(2013), A review over MANET- Issues and Challenges,International Journal of Enhanced Research in Management & Computer Applications, 2, 5, pp 24-36

[4] Yanli Li Xiaonan Wang (2019), A novel and efficient address configuration for MANET, International Journal of Communication Systems, Volume 32, Issue 13, 2019

[5] KhurramNaim Shamsi, Dr.Mohammad Mazhar Afzal (2019), An IoT framework incorporating MANET, International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC) -2018
[6] Gondi Yasoda Devi, Gurrala Venkateswara Rao (2019), Artificial Intelligence Based A* Optimization Routing in Mobile Ad Hoc Networks, International Journal of Engineering and Advanced Technology.
[7] J. Manoranjini, A. Chandrasekar and S. Jothi (2019), Improved QoS and avoidance of black hole attacks in MANET using trust detection framework, Journal for Control, Measurement, Electronics, Computing and Communications, Automatika, 60:3, 274-284
[8] Baisakhi Chatterjee, Himadri Nath Saha(2019), Parameter Training in MANET using Artificial Neural Network, J. Computer Network and Information Security
[9] Rashidah F. Olanrewaju(2020), MANET Security Appraisal: Challenges, Essentials, Attacks, Countermeasures & Future Directions, International Journal of Recent Technology and Engineering, Volume 8, Issue 6
[10] Hussain, S.R., Saha, S. & Rahman, A. SAAMAN (2011), Scalable Address Auto Configuration in Mobile Ad Hoc Networks, Journal Of Network and Systems Management 19, 394–426 (2011).
[11] Nishani, Lediona & Biba, Marenglen. (2015). Machine learning for intrusion detection in MANET: a state-of-the-art survey. Journal of Intelligent Information Systems. 46. 10.1007/s10844-015-0387-y.
[12] K.Purnima & M.N. Giriprasad (2020). Review of Metrics and Frameworks for MANET Configuration Management. International Conference on Science, Technology and Management (ICSTM-20).