A New Hybrid Traffic Generation Model for Tactical Internet Reliability Test

Weiqiang Wu, Beihang University
Ning Huang, Ph.D., Beihang University
Yue Zhang, Beihang University

Key Words: Reliability Test; Self-similarity; Tactical Internet; Traffic Generation.

SUMMARY & CONCLUSIONS

Tactical Internet (TI) is the communication infrastructure of tactical level maneuver warfare forces; its reliability directly affects the military combat. Therefore, in the TI reliability test, how to generate the appropriate network traffic and get the most accurate evaluation results should be an important part of the TI reliability test research.

This paper analyzes the characteristics of applications and traffic in TI, and proposes a new hybrid traffic model which can reflect TI mission profile, to generate traffic for TI reliability test. Firstly, we research the current popular traffic generation technologies of network reliability test area, and point out their advantages and disadvantages. Secondly, according to the research result of traffic generation technologies, we propose a method for application traffic generation and combine it with background traffic generation method. Then the completed hybrid traffic model which includes application traffic generation method and background traffic method is proposed. Based on this traffic model, application traffic and background traffic are generated for TI reliability test and can get the most accurate reliability evaluation result. Finally, all the theories and models are verified by a case study. In the same case, we get the reliability test results by using hybrid traffic generation method and reliability simulation results by using OPNET, according to comparing both results, the ranges of reliability curves are same and the effectiveness of the method is proven.

1 INTROUDUCTION

Tactical Internet (TI) is the tactical communication network under mobile communication environment, which is constituted by tactical radio stations, computer hardware and software. It is mainly used for achieving tactical edge's horizontal and vertical interconnection of wireless networks, combat forces' command and control, battlefield situational awareness and seam-less connectivity, etc.

TI is communication infrastructure of tactical level maneuver warfare forces, so the reliability of TI will directly affect the military combat. However, several factors: a variety of networks integration, the number of devices and equipment, dynamic running environments and WAN multicast transmission make the TI reliability problem become increasingly severe. TI is growing rapidly, but there's no typical and wildly recognized research on reliability evaluation of TI.

For the method of network reliability evaluation, simulation and test are important methods. During reliability experiment, the different combat missions will produce different reliability test profiles. It means that the different missions could lead different network running environments and timing relationships. It will make the traffic flow, which need to be loaded into network reliability test based on reliability test profile, whether from time traffic, spatial distribution, or flow duration and size perspective. Thus, in the TI reliability test, how to generate the appropriate network traffic and get the most accurate evaluation results should be an important part of the TI reliability test research.

About the methods of traffic generating, there are several concepts that have already proposed by researchers. For example: Botta et al [2] proposed the computer network reliability test correctness depends on traffic generating, and with the purpose of generating the most correct traffic, although they have proposed the concept of considering the different levels' traffic, they didn't consider the users' operation profile more for wireless network, especially for TI which has strong dynamic and moving properties. Qureshi J. H [4] has proposed another concept of network traffic generating and his research is based on the partition of different traffic levels and also is a common method. For generating the most correct traffic for network security test, he had proposed a background traffic generating method. Because this method is for network security test, it doesn't reflect the users' behavior as well. Therefore the demand of the design and evaluation for TI reliability is very urgent [10].

Therefore, we have to consider two important steps: task profile establishment and traffic generating method to deal with the TI reliability test:

1.1 The profile of network reliability test

The purpose of task profile researching is supposing to

978-1-4799-6703-2/15/$31.00©2015 IEEE

find a method of generating suitable traffic to carry out the network reliability test.

About the task profile of network, the reliability profile usually includes work stress and environment stress [9]. For network reliability test, the work stress is performed on network traffic [15], in other words, the network traffic can reflect the users' behavior. Thus, in order to implement TI reliability test, we have to establish the reliability test profile from TI, and then break down the profile to network traffic, establish the traffic model, the last step is generating the property network traffic for network reliability test.

The definition of "profile" is: a description of event, state, process function and the environment, so this kind of description is a timing description [1]. Hence, the task profile's definition in reliability area should be: A timing description of all necessary events and states that the products have to experience for completing the specify tasks. The task profile usually includes: the working status of products, maintenance program, working time and order of products, the environment time and order for products, the failure definition of the tasks.

Now the current profile modeling methods of reliability test are focus on temperature, pressure and voltage of system components. But for some complex systems, it is very difficult to establish the profiles [2]. About the researching on network profile, US Force's standard gives some rules and settings, and just includes two contents: the time of the task and the possible application types, such as voice, data and video. It is not enough for breaking down to support traffic generating and cannot meet the requirements of reliability test as well. Weiwei Chen had tried to describe the profile as a triple which includes task execution stages, types of applications for each stage and the relationship between applications [13]. Comparing with the US Force's standard, this description considers the relationship between different applications. However, the types of the supported applications are limited, and without considering the distribution of space and users' behaviors on application layer, so this method also is not fit for network reliability test. For reliability test of TI, the breaking down of task profiles is the breaking down of network usage requires. This process of breaking down reflecting to network system is network traffic generating.

1.2 The methods of traffic generating

The traffic generating model is most important to the methods of network traffic generating. The test results usually are different for the same network under the different traffic models. For traditional research of theory of telecommunications, the reach of network traffic is described by Poisson process and Markov process, both of these process models are short dependent model. However, with the progress of data communication network, the researchers find the data flow is not as stable as in telecommunications network, and has strong burst. Actually, in data communication network, the process of link establishment also can be modeled based on Poisson process, but the transmission process should be described by using Self-similar traffic model. However, the network traffic model only can reflect the whole status of network traffic from the statistics view and cannot from the combat missions to build the traffic model which specify the operational characteristics of TI. Hence we need to improve the network traffic model from the research of reliability view and consider the combination of task profile and traffic model.

There are a couple of software tools of network traffic generating and these tools can be divided into the following four categories [3-6] [8-10]:

Application-level traffic generators: this kind of tools can generate the data flow by simulating user behaviors, but cannot support concurrent multi-service.

Flow-level traffic generator: this kind of tools, such as Harpoon, can generate traffic according to source and target IP, port number. But it also cannot describe the applications' profiles.

Packet-level traffic generators: this kind of tools is based on IDT and PS, and the description parameters are limited, just can be used to do network performance test.

Closed-loop and multilevel traffic generators: this kind of tools is still in researching progress, for example, Swing, which is proposed by Kashi Vishwanath and Amin Vahdat [12]. It can describe users' behaviors and network behaviors, but it cannot input the parameter manually, only support traces files input.

In summary, how to generate the most appropriate traffic for TI reliability test is to resolve. This paper proposes a new method that based on hybrid traffic generating for TI reliability test. The rest of this paper is organized as follows. In section II, we propose the hybrid traffic generating model and generating method based it. In section III we verify the traffic generation method by a TI case study. From this case study, we discuss how to generate hybrid traffic during reliability test and reliability simulation, and according to comparing the reliability test result, the effectiveness of the method has been verified.

2 THEORIES AND MODELS

Because of the behaviors of Tactical Internet, the traditional reliability test profiles and the methods of network traffic generating do not fit in with Tactical Internet reliability evaluation test, hence we propose a model of Tactical Internet traffic generating based on hybrid traffic.

2.1 Network traffic generating method based on hybrid traffic

In this paper, we sum up the end-to-end traffic flows and link utilizations as background traffic flow and application packet traces is summed up as application traffic. There are several differences between application traffic and background traffic:

The application traffic is based on the model of application conduct description. It means that the differences are: application traffic generating is a process of business

behaviors imitation, and the background traffic is based on statistical of the traffic reproducibility process.

The application traffic could collect all parameters for each layer, and the background traffic only could collect the parameters from the layers of Link Layer (TCP/IP Reference Model).

The application traffic generating either is corresponding to the network traffic according to the mission profile decomposition, or the object which need to be examined in the reliability test. And the background traffic generating is corresponding to statistical self-similarity characteristics of the whole network, it is also according to the actual tasks of network, just the model of background traffic is based on the long time statistics rather than for a particular combat mission. Background traffic is not the content of reliability test inspection, but as an environment factor of Tactical Internet system during the reliability test, it also should be included into the requirements of traffic generating for the reliability tests.

So when we try to simulate or test network traffic of Tactical Internet, we have to consider its application traffic and background traffic, and use hybrid traffic models.

2.2 The application traffic generating method based on multiport applications model

A significant difference for the application with others is the different information transmission structures. It is easy to model two-tier architect applications, and for the customized multiport applications, we need a multiport application traffic generating model that can describe their multiport behaviors better.

The characteristics of Tactical Internet application traffic are longitudinal, multiport and self-similar background traffic. Meanwhile, on the basis of the definition for network application meaning, if we want to generate traffic for reliability test, we have to consider factors on the application layer: application end IP, Service request type, the behavior of application process, multiport service/thinking time, cycles (Duration) and the background traffic of the links. Hence, we can simplify an analytical model of multiport network service to get a model of multiport application traffic generation process description:

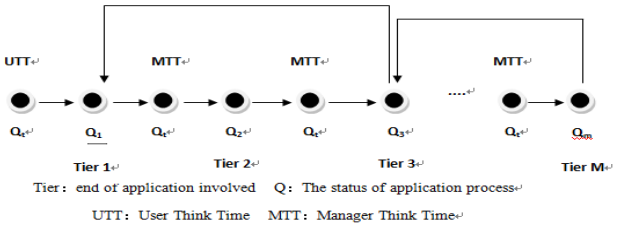

Figure 1-Multiport application traffic generating process

About the above figure, a Tier denotes an end, the corresponding statuses (1…m) are Q_1. . Q_m, and the arrows between the statuses (Q) denote the state transition. The user's behaviors are based on dialog, and every dialog may generate multiple requests. We define the time between the requests as MTT (Manager Think Time). For a given task, the probability of returning the queue and the probability of forwarding to next queue are fixed (or subject to a certain distribution). This data is obtained by the statistical. For a Tactical Internet multiport application, we could determine the metastatic behavior of the queue. For UTT(User Think Time), it exists before the first Tier 1, so other service time which occurs after Tier 1 can be seen as MTT of server side, and Q_t denotes the state of thinking time.

The transfer process between multiport actually is the process of information transfer between end to end, the process is corresponding with the calling different network protocols. The model clearly shows the data flow characteristics of the applications, and the required input parameters include the amount of data transference, transition probabilities and the distribution of thinking time. For the given tasks, the transition probabilities and the amount of data transference should be determined.

According to establish the application traffic model, we can get a parameter elements combination of this model:

$$AppTraffic_i = \begin{Bmatrix} TierAddr_j, AppType_j, Transfer_i, MTT_j, UTT_j, \\ Time_i, BackTraffic_j, j = 1,2,...m \end{Bmatrix} \quad (1)$$

AppTraffic_j denotes the number i multiport application, TierAddr_j denotes m number ends IP addresses, AppType_j denotes the application type of each end-to-end, Transfer_i denotes the information flow transition process of this multiport application. MTT and UTT are thinking time for each end, Time denotes the duration of this application (or cycles), BackTraffic denotes the background traffic of each end-to-end.

2.3 The self-similar background traffic model

This section we'd like to discuss about the background traffic generating based on ON/OFF source model.

2.3.1The model of background traffic generating

Since Will E.Leland [14] found the self-similar feature of the Ethernet traffic, it has been proved that the self-similar feature is widely spread in network traffic and has been the most important feature of the network traffic. So we have to find a method to generate traffic to fit the self-similar feature.

2.3.2 Heavy-tailed distribution

For ON / OFF source model, the length of time ON and OFF is generally subject to heavy-tailed distribution. This is a widely distribution, the main features are attenuation presented in a long-tail phenomenon. The intuitive explanation for heavy-tailed distribution is random variables with non-negligible probability to take very large values, it means large number of small sampling values and small number of large sampling values are coexist. Heavy-tailed importance lies in it is the reason which cause long dependent phenomena. Heavy-tailed distribution phenomena has been detected in Ethernet LAN, besides that, the time of web file transmission and the size of transmission file also obey heavy-

tailed distribution. Common heavy-tailed distributions include Pareto distribution, lognormal, etc.

Pareto distribution is a continuous distribution, its probability density function is:

$$f(x;\alpha,\beta) = \alpha\beta^{\alpha} / x^{\alpha+1} \quad (2)$$

Among the formulas, α is shape parameter, β is location parameter, and $\alpha>0$, $\beta>0$. Pareto distribution is used to describe the phenomenon that larger compared to the Smaller.

2.3.3 ON/OFF model

ON / OFF data source superposition model: the model is with N independent data sources, each data source is a renewal process. They are independent and identically distributed with ON / OFF cycle. $X_i(t)$ alternately generated 1 or 0, corresponding to the state of ON or OFF. Such a superposition of packets generated by N different sources, its synthesis flow can be expressed as:

$$S_N(t) = \sum_{i=1}^{N} X_i(t) \quad (3)$$

Let $stream_{i,j}$ denote the traffic flow, in which packets are sent from the node i to the node j. The aggregate traffic superposed by a lot of streams generated by Pareto ON / OFF traffic model appears the self-similar feature over a range of time scales. Let T denote the rescaling time factor and N_i denote the number of the different streams passed through node i. Then if $N_i \to \infty$ and $T \to \infty$ the aggregate traffic in [0, T_t] could be described as follow:

$$A(T_t) = N_i v\mu_1 T_t / (\mu_1+\mu_2) + v\sigma_{\lim} B_H(T_t)\sqrt{N_j} \quad (4)$$

where $B_H(Tt)$ is a fractional Brownian motion and $B_H(0)=0$, $\sigma_{\lim}$ is a finite positive constant. H is the Hurst parameter which is widely used to measure the self-similar feature.

In this model, we set the data transmission of network source is two-state: ON and OFF. During ON period, the transmission rate is constant, the distribution of ON time length obey Pareto distribution; during OFF period, the source is idle state and without data transmission, the distribution of OFF time length obey Pareto distribution as well, but the parameters or distribution function may be different.

3 CASE STUDY

3.1 Case designing

This paragraph we would verify the traffic generation method by an actual TI case.

There are 4 kinds of TI equipment: terminal, broadcasting station, INC (InterNet Controller) and TMG (Tactical Multiple Gateway).

According to the network hierarchy, the terrestrial TI can be divided into 3 levels: Terrestrial Tactical Network, Terrestrial Tactical Subnet and Individual Ad Hoc Network. Individual Ad Hoc network is a flat network which is combined by individual soldiers in one same combat unit. All the nodes of Individual Ad Hoc Network constitute the underlying layer of terrestrial tactical network. Upper Individual Ad Hoc network contains the cluster head nodes of Individual Ad Hoc Network and other ordinary nodes, all these nodes and Individual Ad Hoc Network constitute the Terrestrial Tactical Subnet. Upper Terrestrial Tactical Subnet contains the cluster head nodes of Terrestrial Tactical Ad Hoc Networks, and all the nodes construct the whole terrestrial tactical network.

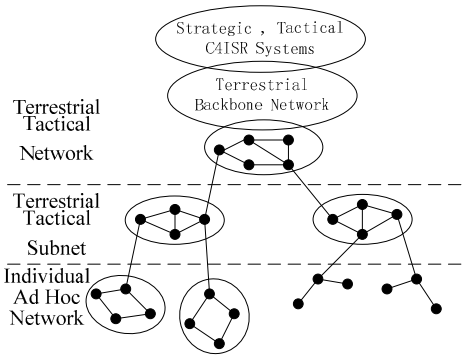

Figure 2-The TI structure graph

Here we break down a tactical mission, and can get several task profiles for TI reliability test. From the profiles, we can also get the application traffic and background traffic parameters and apply them to traffic generation tools.

3.2 Experiment design

With the purpose of analysis and verification of TI reliability test method, we use enterprise equipment based on real TI functionally similar and the network protocol consists with TI.

The designed test platform is as same as the actual TI network: using wireless cards to simulate the link function of the broadcasting station; the Windows OS supports INC route controlling and packets forwarding; the multi-level network is simulated by using wired and wireless network cards.

For this case, Node 1 is outside communication radius of other nodes ; Node 2, Node 3 are in the communication radius of node 4 , and outside communication radius of node 5 ; node 4 is a head cluster of individual Ad Hoc Network , it is within the communication range of node 5; node 5 is the second level of network nodes , and it is connected to node 6 by wire.

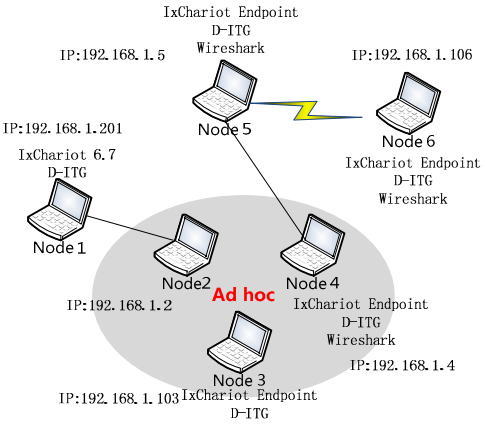

Figure 3-Test equipment connection graph

3.3 Hybrid traffic generation in test

From the designed case, the node 1 related to single-ended SA application (uplink and downlink) is selected as application traffic, and the rest is background traffic.

In this task, the SA includes 2 kinds of application: uplink information and downlink information.

The application traffic ensures the network application, and the background traffic determines network size, mobility and traffic type. In this case, we set the size of the network: link 3->4: 3 individual soldiers; link 4->5: 4 individual soldiers; link 5->6: 4 individual soldiers. About the mobility setting, as we introduced above, the mobility are reflected by the parameters of self- similarity coefficient, so we can set it according to setting Pareto distribution shape parameter by using ON/OFF model to generate background traffic. For the traffic type, we can mimic different types of traffic by traffic size.

3.4 Simulation design

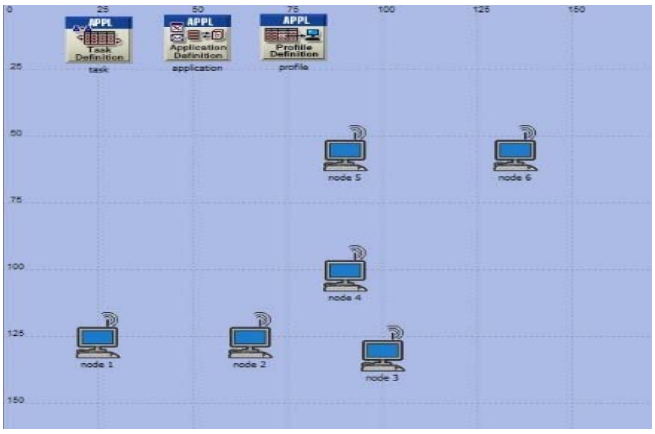

Figure 4- The topology of simulation

As the test designing, we use the same network topology map: node 1, 2, 3, 4, 5, 6 are wireless nodes, and node 6 is Command Center node. As Figure 4 shows.

In this case, about the communication functionality, the network which is constructed by OPNET is as same as the real TI network case that we have designed. About the communication protocol, the protocol is also as same as the real TI network.

This model contains all levels of the node model, here we refer OSI 7 levels: On physical layer, the physical channels are consisted by using wireless transceiver; On data link layer, use DCF based IEEE 802.11; On router layer, according to address resolution, use TORA protocol and AODV protocol which is supported by OPNET. On the top layer, use typical TCP protocol and the configuration of application/service layer.

3.5 Reliability test result analysis

We used software tool to capture the traffic from node 4 and node 5. From the traffic on node 5:

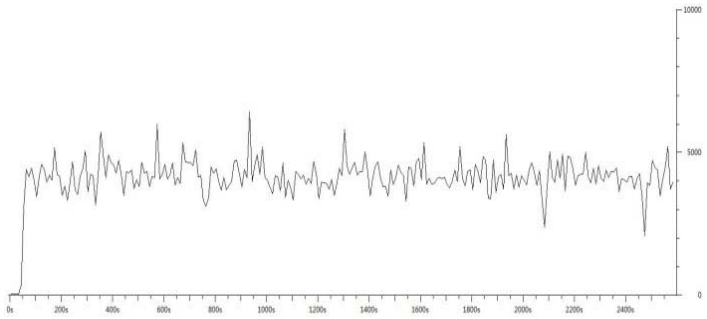

Figure 5-Test traffic on node 5

In figure 5, the x-axis denotes the time scale (3600s) and the y-axis denotes the traffic size (0~10000 byte), we can observe the self-similar feature of the traffic. We count the data per 10 second, and can obtain H （Hurst parameter）value by using R/S algorithm is:

$H = 0.72284$

And the Theoretical value should be:

$H = 0.7$

So from the analysis of Hurst value for the test result, the test hybrid traffic generation method is valuable.

3.6 Reliability comparing between test and simulation results

From the designed case, based on the results of reliability test and simulation, we can calculate the reliability value of the network of the case. Here we observe the packet loss rate on node 4 while SA application is applying. The time of the test is 3600 seconds, 10 trials. The rule is:

Packet loss rate per unit time than 0.5% is considered to be one fault. Here is the reliability curve of reliability test and reliability simulation (Figure 6, 7):

Figure 6-The reliability curve of reliability test result

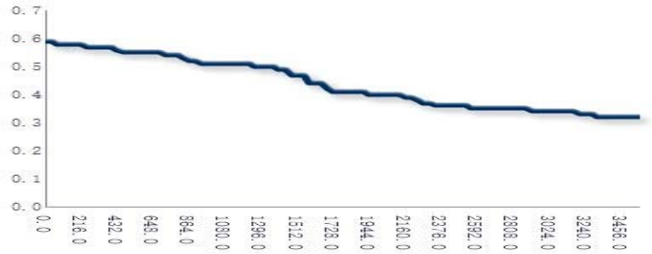

Figure 7-The reliability curve of reliability simulation result

From the comparing of above simulation results and experimental results, for a single node and single application, the result reflects the complete reliability is reducing with the

time's increasing. It means that the packet loss rate increases with time.

From these 2 curves, we observe a couple of differences for the shape and fitting. The reasons are:

- The environment for TI reliability test is not exact the same with the actual TI environment because of the laboratory limitation of equipment and condition. The simulation setting is more exact. Because we use a series of OPNET settings which are special for Ad Hoc.
- Some services of OS may also generate traffic and it will affect the test result.

Besides that, the range of two curves is substantial in the same interval and reflect the network reliability, it can prove that the hybrid traffic that we discussed in this paper is valid.

REFERENCES

1. ZENG Shengkui, ZHAO,Tingdi, ZHANG Jianguo. "System Reliability Analysis Tutorial," Beijing: Beijing University of Aeronautics and Astronautics Press, 2001: 9-15 (in Chinese).
2. Botta A., Dainotti A., Pescapé A, "Do You Trust Your Software-Based Traffic Generator," IEEE Communications Magazine, 2010, 48(9):158-165.
3. SONG Yingdong, GAO, "Deping Principal component clustering method for engine mission profile," Journal of Aerospace Power, 2002, 17(2):196-200.
4. Qureshi J. H, "Generating background network traffic for network security test beds," Ames: Iowa State University, 2006.
5. Avallone S, et al., "D-ITG Distributed Internet Traffic Generator," USA:Proceedings of the First International Conference on the Quantitative Evaluation of Systems (QEST'04), 2004:316-317.
6. Philippe Bogaerts, HPING tutorial[R], 2003.
7. P. Barford, M. Crovella, "Generating representative Web workloads for network and server performance evaluation," *Proceedings of ACM SIGMETRICS 1998*, Madison, WI, June 1998:151-160.
8. Varet A, Larrieu N, "Realistic network traffic profile generation: theory and practice," *Global Journal of Health Science*, 2014, 7(2).
9. Chakraborty A., et al, "On Network Lifetime Expectancy With Realistic Sensing and Traffic Generation Model in Wireless Sensor Networks," *IEEE Sensors Journal*, 2013, 13(7): 2771-2779.
10. Botta A., Dainotti A., Pescapé A, "A tool for the generation of realistic network workload for emerging networking scenarios," *Computer Networks,* 2012, 56(15): 3531-3547.
11. Han Y, et al., "Flow-level traffic matrix generation for various data center networks," *Network Operations and Management Symposium (NOMS)*, 2014 IEEE, 2014: 1-6.
12. Tiemeni G L N, et al., "A mobile platform traffic generator for network performance evaluation," 2013.
13. Weiwei Chen, "Sectional System Study Based on Application," Beijing: Beijing University of Aeronautics and Astronautics, 2011.
14. Leland, W. E., Taqqu, M. S., Willinger, W., and Wilson, D. V, "On the self-similar nature of Ethernet traffic (extended version)," *IEEE/ACM Transactions on Networking*, 1994, 2(1): 1-15.
15. Li, Ruiying, Ning Huang, and Haitao Liao, "Test profile design for avionics Full-Duplex Switched Ethernet," *Reliability and Maintainability Symposium (RAMS)*, 2014 Annual, IEEE, 2014.

BIOGRAPHIES

Weiqiang Wu, Ph.D.Candidate
School of Reliability and System Engineering
Beihang University
37#Xueyuan Road
Haidian District, Beijing, 100191, China

Email: supernbman@gmail.com

Weiqiang Wu received the MSE degree in the School of Software at Beihang University in 2011 and had been an Oracle employee as software engineer for 2 years. Now he is pursuing a Ph.D. in Beihang University since 2013, China. His current research interests include network reliability and network failure diagnostic.

Ning Huang, Professor
School of Reliability and System Engineering
Beihang University
37#Xueyuan Road
Haidian District, Beijing, 100191, China

E-mail: hn@buaa.edu.cn

Ning Huang was born in Simao, Yunnan, China. She earned her Ph.D. in 1997 at computer software in the School of Computer Science and Engineering in Beihang University. Currently, she is a professor at School of Reliability and System Engineering of Beihang University and her research interests are network reliability, software test and software reliability.

Yue Zhang, Ph.D.Candidate
School of Reliability and System Engineering
Beihang University
37#Xueyuan Road
Haidian District, Beijing, 100191, China

E-mail: zybuaa2013@163.com

Yue Zhang received the BS degree in the School of Mathematics and Systems Science at Beihang University in 2012. Now he is pursuing a Ph.D in Beihang University since 2013, China. His current research interests include network reliability and network traffic.