The paper introduced a new application to monitor the current network traffic in the real-time version for High-Speed Network today, called “ntopng”.

First, ntopng read the JSON message by nPorbe, Who convert network flow to JSON file with standard of NetFlow, to achieve the goal of making network feature to be visible, which also reduce the complexity of flow standards at the same time. What’s more, ntopng instance can also provide data to one another, to create a centralized view of network without other application or tools (page 72).

Ntopng detect application protocol carried by the flow by inspecting the IP/ports it used, or analyses the payload of raw packets by nDPI. Encrypted traffic can also be handled by inspecting the SSL certificate information. Ntopng also be able to characterize traffic based on its nature with specific tag categorically, for instance: FaceBook for tag “social”, and traffic to CNN tagged as “News and Media”. Additionally, ntopng can also detect previously malicious hosts by accessing public services, and report to the web interface to response for malicious network activities. (page 74) Ntopng process traffic and strip data from it with the monitor engine, which core is coded in C++, and scripting engine using Lua API, and also could be configured for specific requirement by changing scripts easily(page 73,75).

After the data is captured and processed, ntopng provide multiple interface s to show the user its work. It could be web page, or JSON objects for other applications, or the log files of itself. These results are also associated with system information, establish connection between network traffic and specific process and reports system status for reference(page 76).

Ntopng, according to this paper, has following advantages: First one is real-time monitor, better than those old methods based on flow data that already captured. Second one is visibility, exhibited data directly and clearly. Next is compatibility for application layer, could be implemented in virtual and cloud environment.

Beside these features while being compared with same sort of products, in my opinion, ntopng may also have some shortcoming. First, the standard of classification is not specified in the paper, which means it could be possible for attackers to forge the feature of normal traffics to avoid being detected. Another vulnerable point is, as stated in the paper, for the corporation of different ntopng instances, it is necessary to consolidate all data in a certain location. Author says that it could be improved by using cloud-based storage system. But if attacker aware of the information are all concentrated at the same spot, it probably be hacked or sabotaged to disable the whole service.

After viewing this paper, I believe that robustness of this application should be further investigated. As a network flow monitor, the primary goal is to keep the object being monitored from threats on the Internet. So the application must have relevant security methods to prevent it from being deceived or sabotaged maliciously. This is also the shortcoming of most software based network traffic monitor applications. Comparing those implement mathematic methods to calculate the feature of network flow, the applications with specific standards defined by people could possibly be aimed at. So I may recommend to corporate with other group to increase the security level of this application to make it a more reliable and improve its robustness.