TABLE II
COMPARISON BETWEEN TESTING SCENARIO 1

Sigma	Traffic	Attack	μ(60)	Q1-μ	σ (60)	Result
Previous Method (3sigma)	20M	Yes	1.49	18.51	3.19	Detected
	6M	No	1.49	4.51	3.19	Detected
Proposed Method (6sigma)	20M	Yes	1.49	18.51	6.38	Detected
	6M	No	1.49	4.51	6.38	Not detected

TABLE III
COMPARISON BETWEEN TESTING SCENARIO 2

Sigma	Traffic	Traffic Type	μ(60)	Q1-M	σ (60)	Result
Previous Method (3sigma)	20M	Attack	3.51	16.49	5.19	Detected
	9M	Normal	3.51	5.49	5.19	Detected
Proposed Method (6sigma)	20M	Attack	3.51	16.49	10.38	Detected
	9M	Normal	3.51	5/49	10.38	Not Detected

F. Discussion and Summary Research Findings

In the aspect of simplicity, SDN controller can be programmed with a high-level programming language to implement low-level rules forwarding hardware, to implement the detection mechanism; we only use 2 functions, for the packet statistic pooling and the detection function. In the traditional network, it is tough to program high-level programming language; it only has to use the low-level rules.

For the detection accuracy, Table 2 and Table 3 present the result of a testing scenario. The result is that both three-sigma and Six-Sigma can detect the DDoS Attack. However, the three-sigma also detected the legitimate traffic as anomaly traffic, in that scenario the three-sigma have the false positive rate of 50%, in the Six-Sigma they have 0% of false positive. It is due to the threshold that shaped by three-sigma are too low. On the contrary, the improved Six-Sigma could detect the anomaly traffic and let the legitimate traffic not detected as an anomaly. It is due to the Six-Sigma shaping threshold above the three-sigma shaped threshold. The false positive value that we get shows an extreme percentage due to lack of traffic scenario; it is because the data traffic patterns that we get from the ISP only have 2 types.

IV. CONCLUSIONS

Based on several experiments have been performed, the results show that the use of Six-Sigma as threshold have better accuracy than using three-sigma. Six-Sigma has lower false positive than three-sigma. It is because the three-sigma threshold is too low and the gap of the routine traffic is too narrow, so when there is the high increase of traffic, it will be detected as an attack. The Six-Sigma otherwise, shows much of gap for the legitimate traffic to expand and not detected as an attack. The results show the proposed method could improve the accuracy of DDoS attack detection on SDN environment, either in constant or fluctuating traffic, by reducing the false positive. The performance is about 50% more accurate than the previous method.

ACKNOWLEDGMENT

Authors thank Telkom University under Research and Community Service Bureau (PPM) program for publication incentive. Also, thank Telkom Indonesia Corp. for financial support. Last but not least our colleague in the graduate program of Telkom University.

REFERENCES

[1] B. B. Gupta, Manoj Misra, R. C. Joshi, *An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach*, 2008.

[2] Mousavi, S.M *"Early Detection of DDoS Attacks in Software Defined Networks Controller."* Carleton University. Canada. https://curve.carleton.ca/system/files/etd/. 2014.

[3] Yadav, A., Radadiya, M., Tilva, M., Rohokale, V. *"SDN Control Plan Security in Cloud Computing Against DDOS Attack."* www.ijariie.com. 2016.

[4] C. Dillon, M. Berkelaar, "OpenFlow (D)DoS Mitigation," 2014

[5] S. Das, G. Parulkar, N. McKeown, "Unifying Packet and Circuit Networks," Below IP Networking (BIPN), November 2009. (S, G, & N, 2009)

[6] Alvaro Garcia de la Villa, Tuomas Aura, Aapo Kalliola, Distributed Denial of Service Attacks defenses and OpenFlow: Implementing denial-of-service defense mechanisms with software-defined networking, 2014.

[7] Saurav Das, Guru Parulkar, Nick McKeown. Unifying Packet and Circuit Switched Networks with OpenFlow. 2009

[8] Siamak Azodolmolky, software-defined network with OpenFlow, 2013

[9] Varun Tiwari, Rushit Parekh, and Vishal Patel. A Survey on Vulnerabilities of OpenFlow Network and its Impact on SDN/OpenFlow Controller. in World Academics Journal of Engineering Sciences 2014

[10] Wolfgang Braun, Michael Menth, Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices, 2014.

[11] Chun-Yu Hsu, Pang-Wei Tsai, Hou-Yi Chou, Mon-Yen Luo, Chu-Sing Yang, 1A Flow-based Method to Measure Traffic Statistics in Software Defined Network, 2014.

[12] S. Akbar Mehdi, J. Khalid, and S. Ali Khayam Revisiting Traffic Anomaly Detection using Software-Defined Networking, 2011

[13] Open Networking Foundation, OpenFlow Switch Speci_cation v1.0, 2009