IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 1, May 2022

An Enhanced K Nearest Neighbor Classifier for Malicious Node Detection in VANET

Abhilash Sonker and R. K. Gupta

Department of Computer Science and Engineering and Information Technology
Madhav Institute of Technology and Science, Gwalior, Madhya Pradesh, India

Abstract: *Recently, wireless communication technologies have become a vital part of our lives. The advancements made in communication technology, VANET systems is been introduced. With the increase of vehicles, different sorts of traffic are created in realistic environment. In some cases, the traffic is created by anomalies. Henceforth, the security of VANET communication becomes an important entity. In this paper, we proposed an enhanced k-Nearest Neighbor classifier that detected the malicious node in VANET. Generally, the classifier suffers from high computational cost in distance estimation during malicious node detection. The efficiency of the proposed classifier is experimented and implemented by validating the throughput and packet delivery rate. Compared to the existing classifier, the proposed classifier achieves 20-25% improvement. By doing so, the communication overhead and delay metrics have been achieved and also helps to minimize the computational storage costs.*

Keywords: Communication System, VANET, Detection efficiency, Security, Malicious nodes and k- Nearest neighbor classifier.

References

[1]. A. M. Abdullah, M. B. Alsolami, and M. H. Alyahya ‘‘Intrusion, detection of DoS attacks in WSNs using classification techniques,’’ J. Fundam. Appl. Sciences., vol. 10, no. 4, pp. 298–303, 2018.

[2]. N. Savarimuthu, ‘‘An investigation on security attacks in wireless sensor network,’’ J. Pure Appl. Math., vol. 119, no. 15, pp. 925–927, 2018.

[3]. G. Kaur and P. Agrawal, ‘‘Detection of LDoS attacks using variants of CUSUM and Shiryaev—Roberts’s algorithm,’’ in Proc. 4th Int. Conf. Parallel, Distrib. Grid Comput., Dec. 2017, pp. 363–369.

[4]. S. Patel and A. Sharma, ‘‘The low-rate denial of service attack based comparative study of active queue management scheme,’’ in Proc. 10th Int. Conf. Contemp. Comput. IEEE Comput. Soc., Aug. 2017, pp. 1–3.

[5]. X. Yang et al., ‘‘A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems,’’ IEEE Trans. Comput., vol. 64, no. 1, pp. 4–18, Jan. 2015.

[6]. N. Singh et al., ‘‘Explicit query based detection and prevention techniques for DDOS in MANET,’’ Int. J. Comput. Appl., vol. 53, no. 2, pp. 19–24, 2013.

[7]. D. Yin, L. Zhang, and K. Yang, ‘‘A DDoS attack detection and mitigation with software-defined Internet of Things framework,’’ IEEE Access, vol. 6, pp. 24694–24705, 2018.

[8]. A. K. Nain et al., ‘‘A secure phase-encrypted IEEE 802.15.4 transceiver design,’’ IEEE Trans. Comput., vol. 66, no. 8, pp. 1421–1427, Aug. 2017.

[9]. J. Lin et al., ‘‘A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[10]. Samara G, Al-Salihy WAH, Sures R. Security issues and challenges of vehicular ad hoc networks (VANET). In: Proceedings of the second international conference on network applications, protocols and services; 2010.

[11]. Zhang Q, Almulla M, Ren Y, Boukerche A. An efficient certificate revocation validation scheme with k-means clustering for vehicular ad hoc networks. In: Proceedings of the IEEE symposium on computers and communications (ISCC); 2012.

[12]. Nowatkowski ME, Owen HL. Certificate revocation list distribution in VANETs using most pieces broadcast. In: Proceedings of the IEEE southeastCon; 2010. p. 238–41.

DOI: 10.48175/IJARSCT-3390

[13]. Papadimitratos P, Mezzour Gh, Hubaux J-P. Certificate revocation list distribution in vehicular communication systems. In: Proceedings of the 5th ACM international workshop on VehiculAr Inter-NETworking, VANET '08; 2008. p. 86–87.

[14]. Studer A, Shi E, Bai F, Perrig A. TACKing together efficient authentication, revocation, and privacy in VANETs. In: Proceedings of the 6th Annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks, SECON'09; 2009. p. 484–92.

[15]. Nowatkowski ME, Wolfgang JE, McManus C, Owen HL. The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS. In: Proceedings of the IEEE southeastCon; 2010.

[16]. Haas JJ, Hu Y-C, Laberteaux KP. Efficient certificate revocation list organization and distribution. In: Proceedings of the IEEE journal on selected areas in communications, 29; Mar. 2011. p. 594–604

[17]. Samara G, Al-Salihy WAH, Sures R. Security issues and challenges of vehicular ad hoc networks (VANET). In: Proceedings of the second international conference on network applications, protocols and services; 2010

[18]. Mallissery S, Pai MM M, Ajam N, Pai RM, Mouzna J. Transport and traffic rule violation monitoring service in ITS : a secured VANET cloud application. In: Proceedings of the 12th annual IEEE consumer communications and networking conference (CCNC); 2015

[19]. [19] Rajput U, Abbas F, Eun H, Oh H. A hybrid approach for efficient privacy preserving authentication in VANET. IEEE Access published in 2017;5:12014–30.

[20]. Martín-Fernández F, Caballero-Gil P, Caballero-Gil C. Managing certificate revocation in VANETs using hash trees and query frequencies. In: Proceedings of the 15th international conference on computer aided systems theory – EUROCAST. Springer; 2015. p. 57–63

[21]. Wasef A, Lu R, Lin X, Shen X. Complementing public key infrastructure to secure vehicular ad hoc networks. IEEE Wirel Commun 2010;17(5):22–8

[22]. T. D. S. Keerthi and P. Venkataram, ''Confirmation of wormhole attack in MANETs using honeypot,'' Comput. Secur., no. 76, pp. 32–49, Jul. 2018.

[23]. P. Liu et al., ''Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET,'' IEEE Access, vol. 6, pp. 20795–20806, 2018.

[24]. H. Chen et al., ''Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol,'' J. Netw. Comput. Appl., vol. 30, no. 1, pp. 145–166, 2007.

[25]. J. Han et al., ''Do you feel what i hear-enabling autonomous IoT device pairing using different sensor types,'' in Proc. IEEE Symp. Secur. Privacy (SP). San Francisco, CA, USA, Sep. 2018, pp. 836–852.

[26]. Huda, S., Miah, S., Yearwood, J., & Alyahya, S. (2018). A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network. Journal of Parallel and Distributed Computing, 120, 23-31

[27]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[28]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[29]. Qu, F., Zhang, J., Shao, Z., & Qi, S. (2017). An intrusion detection model based on deep belief network. In Proc. of ICNCC, 97-101.

[30]. Alom, Z., Bontupalli, V., & Taha, T.M. (2015). Intrusion detection using deep belief networks. In Proc. of IEEE NAECON, 339-344

[31]. Ding, Y., Chen, S., & Xu, J. (2016). Application of Deep Belief Networks for opcode based malware detection. In Proc. of IJCNN, 3901-3908

[32]. Erfani, S. M, Rajasegarar, S., Karunasekera, S., & Leckie, C. (2016). High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recognition, 58, 121-134.

[33]. M. Hasan, M. M. Islam, M. I. I. Zarif, M. Hashem, Attack and anomaly detection in iot sensors in iot sites using machine learning approaches, Internet of Things 7 (2019) 100059.

[34]. Zhang, H., Li, Y., Lv, Z., Sangaiah, A. K. & Huang, T. (2020). A real-time and ubiquitous network attack detection based on deep belief networks and support vector machines. IEEE/CAA Journal of Automatica Sinica, 7, 790–799.

[35]. Chunhua Zhang et al, “Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs”, IEEE access, 2017.