Accompanying Document: Early Characterization of Distributed Network Trust Attacks using a Support Vector Machine

Tanmayee Deshprabhu and Justin P. Coon
Department of Engineering Science, University of Oxford, OX1 3PJ, United Kingdom.
Email: justin.coon@eng.ox.ac.uk

August 2022

Abstract

This is an accompanying document to the paper entitled "Early Characterization of Distributed Network Trust Attacks using a Support Vector Machine" by the same authors. The full paper will be made available upon publication.

1 Unified Framework of Trust Attacks

Tab. 1 shows our proposed unified trust attack framework based on a survey of trust inference literature since 2017.

Table 1: Unified framework of trust attacks.

Attack type	**Attack name**	**Protocol**	**Minor variations and alternative names**	**Citation no. in references document [6]**
False identity *(early-stage)*	White-washing	Having committed a malicious action resulting in low trust, the node leaves and re-joins the network with a new identity to reset its reputation.	Newcomer, node replication	[1, 8, 9, 17, 24, 25, 26, 27, 28, 29, 30, 31, 32]
	Sybil	A node joins the network under a false identity to evade detection.	False identity	[11, 14, 17, 29, 30, 31, 32, 47, 51]
Collusion *(early-stage)*		Two or more nodes work in collaboration to achieve a high trust for at least one of the nodes.	Ballot-stuffing, orchestrated, time-varying attack, wormhole attack	[2, 7, 15, 24, 29, 31, 32, 33, 34, 35, 36, 37, 46]
On-off *(early-stage)*		The node behaves normally in the network for a period of time to achieve a high trust ('on' phase) and then executes a malicious action ('off' phase), thereby maximising the effect of that action on the network.	Conflicting behavior, garnishing, sleeper, camouflage	[1, 2, 6, 7, 8, 11, 28, 29, 36, 39, 40, 41, 42, 43, 44, 45, 48, 49, 52]
False trust reporting *(early-stage)*	Slandering	The node C consistently relays bad observations about another node in the network D, resulting in D having a significantly lower trust.	Bad-mouthing, time-varying attack, ballot-stuffing, false validation, defamation	[2, 6, 7, 11, 15, 24, 27, 32, 33, 34, 36, 46, 47, 48, 49, 50, 51]
	Self-promotion	The node relays positive observations about itself to other nodes in the network to improve its own reputation.	Selfish attack	[11, 15, 24, 27, 32, 33, 41, 47]
Resource-limiting *(leveraged)*	Denial of service	The node creates a high demand on the network resources such that they become unavailable to other nodes and the network function is disrupted.		[11, 19, 44]
	SSDF Attack	The node sends false information to the channel regulator / base station about whether the channel is in use.		[4, 5, 21]
False data reporting *(leveraged)*	Black hole	The node drops all (black hole) or some (grey hole) packets that it receives	Sinkhole, concealment, selective forwarding	[13, 16, 17, 18, 23, 34, 38, 45, 48, 49, 51]
	Tampering	The node changes existing data without permission.		[3, 11, 13, 17, 27, 34, 35, 36, 37, 51]
	Forgery	The node creates new, falsified data.		[11, 17, 27]
	Replay	The node repeats an out-of-date or invalidated packet		[13, 17]
Recruiting other nodes *(leveraged)*	Man-in-the-middle	The node compromises another node and uses its resources or reputation to carry out a malicious action	Eavesdropping	[10, 20, 21]
	Discrimination	Any attack in which the malicious node takes advantage of another node's bad reputation or low trust rating		[27, 29]

References

[1] J. Zhang, K. Zheng, D. Zhang and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," in IEEE Access, vol. 8, pp. 21077-21090, 2020.

[2] H. Xia, S. Zhang, Y. Li, Z. Pan, X. Peng and X. Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 7108-7120, July 2019.

[3] H. Alhumud, M. Zohdy, D. Debnath, and R. Olawoyin, "Cooperative Spectrum Sensing for Cognitive Radio-Wireless Sensors Network Based on OR Rule Decision to Enhance Energy Consumption in Greenhouses", Wireless Sensor Network, 2019.

[4] Y. Fu and Z. He, "Bayesian-Inference-Based Sliding Window Trust Model Against Probabilistic SSDF Attack in Cognitive Radio Networks," in IEEE Systems Journal, vol. 14, no. 2, pp. 1764-1775, June 2020.

[5] W. Fang, C. Zhu, W. Chen, W. Zhang and J. J. P. C. Rodrigues, "BDTMS: Binomial Distribution-based Trust Management Scheme for Healthcare-oriented Wireless Sensor Network," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), pp. 382-387, 2018.

[6] San-shun Zhang, Shi-wen Wang, Hui Xia, Xiang-guo Cheng, "An attack-Resistant Reputation Management System For Mobile Ad Hoc Networks," in Procedia Computer Science, vol. 147, pp. 473-479, 2019.

[7] K. A. Awan, I. U. Din, A. Almogren, H. Almajed, I. Mohiuddin and M. Guizani, "NeuroTrust -Artificial Neural Network-based Intelligent Trust Management Mechanism for Large-Scale Internet of Medical Things," in IEEE Internet of Things Journal, 2020.

[8] I. T. Javed, K. Toumi, F. Alharbi, T. Margaria, and N. Crespi, "Detecting Nuisance Calls over Internet Telephony Using Caller Reputation," Electronics, vol. 10, no. 3, p. 353, Feb. 2021.

[9] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, "MARINE: Man-in-the-Middle Attack Resistant Trust Model in Connected Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3310-3322, April 2020.

[10] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni and Yinxuan Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey," in Wireless Communications and Mobile Computing, 2020.

[11] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on beta distribution," in Science China: Information Sciences, April 2017.

[12] L. Liu, Z. Ma, W. Meng, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks," in Future Generation Computer Systems, vol. 101, pp. 865-879, Dec. 2019.

[13] J. Jia and Y. Li, "A trust attack detection algorithm based on improved K-means clustering," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), pp. 1996-2004, 2020.

[14] R. Casadeia, A. Aldinib and M. Virolia, "Towards attack-resistant Aggregate Computing using trust mechanisms," in Science of Computer Programming, vol. 167, Aug. 2018.

[15] D. Mehetre, E. Roslin and S. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," in Cluster Computing, vol. 22, Jan. 2019.

[16] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali and Shabana Begum, "VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead," in Cost-Effective Techniques for Sensors Technology, 2018.

[17] G. Arulkumaran, R. K. Gnanamurthy, "Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Adhoc Network," in Mobile Network Applications, vol. 24, pp. 386–393, 2019.

[18] S. G. Fatima, S. K. Fatima, S. I. A. Sattar, "A Security Scheme based on Trust Attack in MANET", in International Journal of Advanced Research in Engineering and Technology, vol. 10, April 2019.

[19] R. E. Navas, H. L. Boulder, N. Cuppens, F. Cuppens, G. Z. Papadopoulos, "Demo: Do Not Trust Your Neighbors! A Small IoT Platform Illustrating a Man-in-the-Middle Attack," in International Conference on Ad-Hoc Networks and Wireless, vol. 11104, Aug. 2018.

[20] M. H. Junejo, A. Rahman, R. Shaikh, K. M. Yusof, I. Memon, H. Fazal, D. Kumar, "A Privacy-Preserving Attack-Resistant Trust Model for Internet of Vehicles Ad Hoc Networks," in Sci. Program, 2020.

[21] F. Zhao, S. Li, J. Feng, "Securing Cooperative Spectrum Sensing against DC-SSDF Attack Using Trust Fluctuation Clustering Analysis in Cognitive Radio Networks," in Wireless Communications and Mobile Computing, 2019.

[22] N. J. Patel and K. Tripathi, "Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method," in International journal of scientific research in science, engineering and technology, vol. 4, pp. 281-287, 2018.

[23] S. Xie, Z. Zheng, W. Chen, J. Wu, H. Dai, M. Imran, "Blockchain for cloud exchange: A survey," in Computers and Electrical Engineering, vol. 81, 2020.

[24] A. Gruner, A. Muhle, T. Gayvoronskaya, C. Meinel, "A Quantifiable Trust Model for Blockchain-based Identity Management," IEEE International Conference on Internet of Things (iThings), 2018.

[25] K. A. Awan, I. Ud Din, A. Almogren, and H. Almajed, "AgriTrust—A Trust Management Approach for Smart Agriculture in Cloud-based Internet of Agriculture Things," Sensors, vol. 20, no. 21, p. 6174, Oct. 2020.

[26] K. Rabadiya, A. Makwana, S. Jardosh, "Revolution in networks of smart objects: Social Internet of Things," in Conference: 2017 International Conference on Soft Computing and its Engineering Applications, Dec. 2017.

[27] O. A. Wahab, R. Cohen, J. Bentahar, H. Otrok, A. Mourad, G. Rjoub, "An endorsement-based trust bootstrapping approach for newcomer cloud services," in Information Sciences, vol. 527, pp. 159-175, 2020.

[28] S. Ji, H. Ma, Y. Liang, H. Leung, Chunjin Zhang, "A whitelist and blacklist-based co-evolutionary strategy for defensing against multifarious trust attacks," in Applied Intelligence, vol. 47, pp. 1115–1131, 2017.

[29] M. Faisal, S. Abbas, H. U. Rahman, "Identity attack detection system for 802.11- based ad hoc networks," in EURASIP Journal on Wireless Communications and Networking, 2018.

[30] X. Meng, "speedTrust: a super peer-guaranteed trust model in hybrid P2P networks," in The Journal of Supercomputing, vol. 74, pp. 2553–2580, June 2018.

[31] M. Wang, C. Qian, X. Li and S. Shi, "Collaborative Validation of Public-Key Certificates for IoT by Distributed Caching," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pp. 847-855, 2019.

[32] A. Ugur, "Manipulator: A Novel Collusion Attack on Trust Management Systems in Social IoT," in Proceedings of 10th Computer Science On-line Conference, Vol. 1, pp.578-592, 2021.

[33] V. Busi Reddy, S. Venkataraman and A. Negi, "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory," in IEEE Sensors Journal, vol. 17, no. 12, pp. 3921-3929, June 2017.

[34] W. Yong-hao, "A Trust Management Model for Internet of Vehicles," in Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, pp. 136-140, January 2020.

[35] W. Fang, N. Cui, W. Chen, W. Zhang and Y. Chen, "A Trust-Based Security System for Data Collection in Smart City," in IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4131-4140, June 2021.

[36] J. You, J. Shangguan, L. Zhuang, N. Li, "An Autonomous Dynamic Trust Management System with Uncertainty Analysis," in An Autonomous Dynamic Trust Management System with Uncertainty Analysis: Knowledge-Based Systems, vol. 161, 2018.

[37] S. Nie, "A novel trust model of dynamic optimization based on entropy method in wireless sensor networks," in Cluster Computing, vol. 22, pp. 11153–11162, 2019.

[38] X. Liu, Y. Liu, A. Liu and L. T. Yang, "Defending ON–OFF Attacks Using Light Probing Messages in Smart Sensors for Industrial Communication Systems," in IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 3801-3811, Sept. 2018.

[39] W. Li, W. Meng, L. Kwok, "SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks," in the 12th International Conference on Green, Pervasive and Cloud Computing, vol. 10232, pp. 402-415, May 2017.

[40] J. Caminha, A. Perkusich and M. Perkusich, "A smart middleware to detect on-off trust attacks in the Internet of Things," IEEE International Conference on Consumer Electronics (ICCE), pp. 1-2, 2018.

[41] J. Caminha, A. Perkusich, M. Perkusich, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things", in Security and Communication Networks, vol. 2018.

[42] J. Fan, Q. Li and G. Cao, "Privacy Disclosure through Smart Meters: Reactive Power Based Attack and Defense," 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 13-24, 2017.

[43] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang and J. J. P. C. Rodrigues, "FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things," in IEEE Access, vol. 7, pp. 13476-13485, 2019.

[44] A. Meena Kowshalya, M. L. Valarmathi, "Trust Management in the Social Internet of Things," in Wireless Personal Communications: An International Journal, vol. 96, pp. 2681–2691, Sept. 2017.

[45] F. Khedima, N. Labraouia, A. A. A. Ari, "A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks," in Journal of Network and Computer Applications, vol. 123, pp. 42-56, Dec. 2018.

[46] V. Suryani, V. Sulistyo, W. Widyawan, "Two-phase security protection for the Internet of Things object," in Journal of Information Processing Systems Vol. 14, No. 6, pp. 1431-1437, Dec. 2018.

[47] D. Velusamy, G. K. Pugalendhi, "Fuzzy integrated Bayesian Dempster–Shafer theory to defend cross-layer heterogeneity attacks," in Information Sciences, vol. 479, pp. 542-566, 2019.

[48] C. V. Mendoza, J. H. Kleinschmidt, "A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach," in Wireless Personal Communications: An International Journal, vol. 103, pp. 2501–2513, Dec. 2018.

[49] M. D. Alshehri, F. K. Hussain, O. K. Hussain, "Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)," in Mobile Network Applications, vol. 23, pp. 419–431, June 2018.

[50] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh, M. Lydia "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," in Computers & Electrical Engineering, vol. 72, pp. 894-909, Nov. 2018

[51] A. Amouri, V. T. Alaparthy, S. D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things," in Sensors, vol. 20, Jan. 2020.

[52] X. Liu, Y. Liu, A. Liu and L. T. Yang, "Defending ON–OFF Attacks Using Light Probing Messages in Smart Sensors for Industrial Communication Systems," in IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 3801-3811, Sept. 2018.