References

REFERENCES

[1] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[2] A. U. Khan, R. Puree, B. K. Mohanta and S. Chedup, "Detection and Prevention of Blackhole Attack in AODV of MANET," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021.

[3] Abu Zant M. and Yasin A., Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV), Security and Communication Networks, 2019.

[4] Aldana, J. A. A., Maag, S., &Zaïdi, F. MANETs interoperability: current trends and open research. In 32nd IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 481-487, 2018.

[5] Ali Zardari, Z.; He, J.; Zhu, N.; Mohammadani, K.H.; Pathan, M.S.; Hussain, M.I.; Memon, M.Q. A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs. Future Internet 2019, 11, 61. https://doi.org/10.3390/fi11030061

[6] Bai, Y., Mai, Y., & Wang, N. Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs. In *IEEE Wireless Telecommunications Symposium*, pp. 1-5, 2017.

[7] Balaji, S, Julie, EG, Robinson, YH, Kumar, R & Thong, PH 2019, ‘Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model’, Computer Standards & Interfaces, vol. 66, p. 103358, 2019.

[8] Bhola, J, Soni, S & Cheema, GK, ‘Genetic algorithm based optimized leach protocol for energy efficient wireless sensor networks’, Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 3, pp.1281-1288, 2020.

[9] Cai, RJ, Li, XJ & Chong, PHJ, ‘An evolutionary self-cooperative trust scheme against routing disruptions in MANETs’, IEEE Transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 2018.

[10] Chintalapalli, Ram Mohan and Venugopal Reddy Ananthula. "M-LionWhale: multi-objective optimisation model for secure routing in mobile ad-hoc network". IET Communications 12, no. 12, 1406-1415, 2018.

[11] D. Patel and K. Chawda, “Blackhole and gray hole attacks in MANET,” in Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES’14), pp. 1–6, Chennai, India, February 2014.

[12] D. Patel, R.H. Jhaveri, and S.N. Shah, “I-EDRI Scheme to Mitigate Grayhole Attack in MANETs,” Advances in Intelligent Systems and Computing, vol. 309, no. 2, pp. 39–43, 2015.

[13] Desai, A. M., &Jhaveri, R. H. Secure routing in mobile ad hoc networks: a predictive approach. International Journal of Information Technology, 11(2), 345-356, 2019.

[14] Dhanaraj, R. K., Krishnasamy, L., Geman, O., & Izdrui, D. R. Black hole and sink hole attack detection in wireless body area networks. *Computers, Materials & Continua*, *68*(2), 1949-1965, 2021.

[15] Dhand, G & Tyagi, SS, 'SMEER: Secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks', Wireless Personal Communications, vol. 105, no. 1, pp.17-35, 2019.

[16] Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. APD-JFAD: Accurate prevention and detection of jelly fish attack in MANET. *IEEE Access*, *6*, 56954-56965, 2018.

[17] Elwahsh, Haitham, Mona Gamal, A. A. Salama and Ibrahim M. El-Henawy. "A Novel Approach for Classifying MANETs Attacks with a Neutrosophic Intelligent System based on Genetic Algorithm". Security and Communication Networks, 2018.

[18] Fu, Yulong & Li, Guoquan & Atiquzzaman, Mohammed & Cao, Jin & Li, Hui. A Study and Enhancement to the Security of MANET AODV Protocol Against Black Hole Attacks. 1431-1436. 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00259, 2019.

[19] G. Singh Bindra, A.Kapoor, A.Narang, and A.Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in Proceedings of the International Conference on System Engineering and Technology (ICSET '12), pp. 1–5, Bangdung, Indonesia, September 2012.

[20] Gao, C. Z., Cheng, Q., He, P., Susilo, W., & Li, J. Privacy-preserving naive bayes classifiers secure against the substitution-then-comparison attack. Information Sciences, 444, 72-88, 2018.

[21] Ghonge Mangesh and S.U. Nimbhorkar, "Simulation of AODV under Black hole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering", 2012.

[22] Ghugar, Umashankar, Jayaram Pradhan, Sourav Kumar Bhoi and Rashmi RanjanSahoo. "LB-IDS: 'Securing wireless sensor network using protocol layer trust-based intrusion detection system". Journal of Computer Networks and Communications 2019.

[23] Govindasamy, J & Punniakody, S, 'A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack', Journal of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 735-744, 2018.

[24] Gripsy, J. V., & Kanchana, K. R. Secure hybrid routing to thwart sequential attacks in mobile ad-hoc networks. *Journal of Advanced Research in Dynamical & Control Systems, 12*(4), 451-459, 2020.

[25] Gripsy, J. V., & Kanchana, K. R.. Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System, 2022.

[26] Guleria, K, Kumar, S & Verma, AK 2019, 'Energy aware location based routing protocols in wireless sensor networks', World Scientific News, vol. 124, no. 2, pp.326-333.

[27] Gurung, S. & Chauhan, S., "A Novel Approach for Mitigating Route Request Flooding Attack in MANET," Wireless Networks 2017, pp. 1–16, 2017.

[28] Gurung, S., & Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. *Wireless Networks*, *25*(3), 975-988, 2019.

[29] Gurung, S., & Chauhan, S. A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability. *Wireless Networks*, *26*(3), 1981-2011 2020.

[30] H. Shen, C. Gao, D. He, and L. Wu, "New biometrics-based authentication scheme for multi-server environment in critical systems," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 6, pp. 825–834, 2015.

[31] Hamdi, M.M.; Audah, L.; Abood, M.S.; Rashid, S.A.; Mustafa, A.S.; Mahdi, H.; Al-Hiti, A.S. A review on various security attacks in vehicular ad hoc networks. Bull. Electr. Eng. Inform., 10, 2627–2635, 2021.

[32] Islabudeen, M & Kavitha Devi, MK. 'A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks', Wireless Personal Communications, vol. 112, no. 1, pp. 193-224, 2020.

[33] J.M. Chang, P.C. Tsou, I. Woungang, H.C. Chao, and C.F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," IEEE Systems Journal, vol. 9, no. 1, pp. 65–75, 2015.

[34] J.P. Bhoiwala and R.H. Jhaveri, “Cooperation based defense mechanism against selfish nodes in DTNs,” in Proceedings of the 10th International Conference on Security of Information and Networks (SIN ’17), pp.268–273, October 2017.

[35] Jain M., Singh V., and Rani A., A Novel Nature-Inspired Algorithm for Optimization: Squirrel Search Algorithm, Swarm and Evolutionary Computation, 44, 148–175, 2019.

[36] Jhaveri, R. H., Desai, A., Patel, A., & Zhong, Y. A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs. Security and Communication Networks, 2018.

[37] K.V. Arya, Shyam Singh Rajput," Securing AODV Routing Protocol in MANET using NMAC with HBKS Technique", 2014 International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp-281-285, 2014.

[38] Kalidoss T, Rajasekaran L, Kanagasabai K, Sannasi G & Kannan A, ‘QoS aware trust based routing algorithm for wireless sensor networks’, Wireless Personal Communication, vol. 110, no. 4, pp. 1637-1658, 2019.

[39] Karthick K., & Asokan, R. Mobility Aware Quality Enhanced Cluster Based Routing Protocol for Mobile Ad-Hoc Networks Using Hybrid Optimization Algorithm Wireless Personal Communications, 2021 – Springer, 2021.

[40] Khan, A. U., Puree, R., Mohanta, B. K., & Chedup, S. Detection and prevention of blackhole attack in AODV of MANET. In *IEEE International IOT, Electronics and Mechatronics Conference*, pp. 1-7, 2021.

[41] Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., & Yaacob, M. A survey on MANETs: architecture, evolution, applications, security issues and solutions. *Indonesian Journal of Electrical Engineering and Computer Science, 12*(2), 832-842, 2018.

[42] Khanna, N & Sachdeva, M, 'Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation', International Journal of Communication Systems, vol. 32, no. 12, p. e4012, 2019.

[43] Khanna, N., & Sachdeva, M. A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. *Computer Science Review*, *32*, 24-44, 2019.

[44] Kukreja, D.; Dhurandher, S.K.; Reddy, B.V.R. Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. J. Ambient Intell. Humaniz. Comput. 9, 941–956, 2018.

[45] Kumar, R & Shekhar S., 'Trust-Based fuzzy bat optimization algorithm for attack detection in manet', Smart Innovations in Communication and Computational Sciences, vol. 1168, pp. 3-12, 2020.

[46] Kumar, S., 'Security Enhancement in Mobile Ad-Hoc Network Using Novel Data Integrity Based Hash Protection Process', Wireless Personal Communications, pp. 1-25, 2021.

[47] Liu, G.; Yan, Z.; Pedrycz, W. Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. J. Netw. Comput. Appl., 105, 105–122, 2018.

[48] Manoranjini, J., Chandrasekar, A., & Jothi, S., Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. Automatika, 60(3), 274-284, 2019.

[49] Md Ibrahim Talukdar, Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar, Amjed Sid Ahmed, "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature", Wireless Communications and Mobile Computing, vol. 2021, Article ID 6693316, 13 pages, 2021. https://doi.org/10.1155/2021/6693316

[50] Mirza S. and Bakshi S. Z., (2018), Introduction to MANET, International Research Journal of Engineering and Technology, 5(1), 17–20, 2018.

[51] N. Schweitzer, A. Stulman, R.D. Margalit, and A. Shabtai, “Contradiction based gray-hole attack minimization for ad-hoc networks,” IEEE Transactions on Mobile Computing, vol. 16, no. 8, pp. 2174–2183, 2017.

[52] Nabarun Chatterjeea, Jyotsna Kumar Mandalb, “Detection of Blackhole Behaviour using Triangular Encryption in NS2”, Elsevier, Procedia Technology 10, pp-524 – 529, 2013.

[53] Nabou, A., Laanaoui, M. D., & Ouzzif, M. Evaluation of MANET routing protocols under black hole attack using AODV and OLSR in NS3. In *6th IEEE International Conference on Wireless Networks and Mobile Communications*, pp. 1-6, 2018.

[54] Ndajah P., Matine A. O., and Hounkonnou M. N., Blackhole Attack Prevention in Wireless Peer-to-Peer Networks: A New Strategy, International Journal of Wireless Information Networks, 26(1), 48–60, 2019.

[55] Nguyen Duy Tan. Detection and Avoidance Mechanism of Black Hole Attack on AODV Routing Protocol in MANET using NS2. UTEHY Journal of Science and Technology, 27, 40-46, 2020.

[56] Nurcahyani, Ida, and Helmi Hartadi. "Performance Analysis of Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) Under Black Hole Attacks in Mobile Ad Hoc Network (MANET)." 2018 International Symposium on Electronics and Smart Devices (ISESD). IEEE, 2018.

[57] Pandey, Preeti and AtulBarve. "An Energy-Efficient Intrusion Detection System for MANET". In Data, Engineering and Applications, pp. 103-117.Springer, Singapore, 2019.

[58] Pathan, M.; Zhu, N.; He, J.; Zardari, Z.; Memon, M.; Hussain, M. An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. Future Internet, 10, 16, 2018.

[59] Payal N. Raj and Prashant B. Swadesh, "DPRAODV: A Dynamic Learning System against Blackhole attack in AODV based MANET", International Journal of Computer Science, Vol. 2, 2009.

[60] Pereira, EE & Leonardo, EJ, 'Performance evaluation of DSR for MANETs with channel fading', International Journal of Wireless Information Networks, pp. 494-502, 2020.

[61] Prachi D. Gawande, Yogesh Suryavanshi, member, IEEE, "Cryptography Based Secured Advanced on Demand Routing Protocol in MANET's", 978-1-4799-8081-9/15 IEEE, pp-1478-1481, 2015

[62] PremKumar, R., & Manikandan, R. Distributed hybrid sybil attack detection framework for mobile ad hoc networks. *Materials Today: Proceedings*, 1-4, 2021.

[63] R.H. Jhaveri and N.M. Patel, "Mobile ad-hoc networking with AODV: A review," International Journal of Next-Generation Computing, vol. 6, no. 3, pp. 165–191, 2015.

[64] R.H. Jhaveri, N.M. Patel, and D.C. Jinwala, "Acomposite trust model for secure routing in mobile ad-hoc networks," in Adhoc Networks, J.H. Ortiz, Ed., chapter 2, pp. 19–45, Intech, 2017.

[65] Rajendran, N., Jawahar, P. K., & Priyadarshini, R. Cross centric intrusion detection system for secure routing over black hole attacks in MANETs. *Computer Communications*, *148,* 129-135, 2019.

[66] Reza Amiri, Marjan Kuchaki Rafsanjani, and Ehsan Khosravi ,"Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks", Indian Journal of Science and Technology, Vol 7(4), pp.401–408, 2014.

[67] S. Khushbu, R. K. Bathla, An Approach of Detecting and Elimination of Black Hole Attack in AODV Based Mobile Ad-hoc Network (MANET) Based on MESS Network, International Journal of Scientific Research in Network Security and Communication, Vol.7, Issue.4, pp.21-25, 2019.

[68] Saudi, N. A. M., Arshad, M. A., Buja, A. G., Fadzil, A. F. A., & Saidi, R. M. Mobile ad-hoc network (MANET) routing protocols: a performance assessment. In *Proceedings of the Third International Conference on Computing, Mathematics and Statistics*, Springer, Singapore, pp. 53-59, 2019.

[69] Selvi, PT & Ghana Dhas, CS, ‘A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET’, Mobile Networks and Applications, vol. 24, no. 2, pp. 307-317, 2019.

[70] Shamsi, S, ‘Improving the effect of black hole attack on zone based energy efficient routing protocol in wireless sensors network’, Global Sci-Tech, vol. 11, no. 3, pp. 164-169, 2019

[71] Sumathi Ganesan and Manikandan. R, "Discuss the Prevention of Jelly Fish Attack by AODV and APD-JFAD in MANET", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.6, Issue 6, page no.167-176, 2019.

[72] Syed, S. A., A systematic comparison of mobile ad-hoc network security attacks. *Materials Today: Proceedings*, 1-6, 2021.

[73] Tahboush, M., & Agoyi, M. A hybrid wormhole attack detection in mobile ad-hoc network (MANET). *IEEE Access*, *9*, 11872-11883, 2021.

[74] Tarek M. Mahmoud, Abdelmgeid A. Aly, Omar Makram M, “A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 6, pp-27-33, 2015.

[75] Thapar, Shruti and Sharma, Sudhir Kumar, Detection and Prevention Policies of Jellyfish Attack in MANET (February 21, 2020). Proceedings of the 4th International Conference: Innovative Advancement in Engineering & Technology (IAET) 2020, http://dx.doi.org/10.2139/ssrn.3548382

[76] Vatchala B, G. Preethi, "Hybrid Optimization-Based Secure Routing Protocol for Cloud Computing", International Journal of Computer Networks and Applications (IJCNA), 9(2), PP: 229-239, 2022, DOI: 10.22247/ijcna/2022/212338.

[77] Vinayagam, J., Balaswamy, C. H., & Soundararajan, K. Certain investigation on MANET security with routing and blackhole attacks detection. *Procedia Computer Science*, *165*, 196-208, 2019.

[78] Wang, Y & Wang, Z, ‘Routing algorithm of energy efficient wireless sensor network based on partial energy level’, Cluster computing, vol. 22, no. 4, pp.8629-8638, 2019.

[79] Y. Liu and W. Trappe, “Topology adaptation for robust ad hoc cyberphysical networks under puncture -style attacks,” Tsinghua Science and Technology, vol. 20, no. 4, pp. 364–375, 2015.

[80] Yadav, Neha and Urvashi Chug. "Secure Routing in MANET: A Review". In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 375-379. IEEE, 2019.

[81] Younas, S.; Rehman, F.; Maqsood, T.; Mustafa, S.; Akhunzada, A.; Gani, A. Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs. Appl. Sci., 12, 12448. https://doi.org/10.3390/ app122312448, 2022

[82] Yuan, YuHua, HuiMin Chen, and Min Jia. "An optimized ad-hoc on-demand multipath distance vector (AOMDV) routing protocol." 2005 Asia-Pacific Conference on Communications. IEEE, 2005.

[83] Zhang, Bing, Zhiyang Liu, Yanguo Jia, Jiadong Ren and Xiaolin Zhao. "Network Intrusion Detection Method Based on PCA and Bayes Algorithm". Security and Communication Networks 2018, 2018.

[84] Vatambeti, R. A Novel Wolf Based Trust Accumulation Approach for Preventing the Malicious Activities in Mobile Ad Hoc Network. Wireless Pers Commun 113, 2141–2166, 2020, https://doi.org/10.1007/s11277-020-07316-z

[85] Wadhwani, G. K., Khatri, S. K., and Mutto, S. K. Trust framework for attack resilience in MANET using AODV. Journal of Discrete Mathematical Sciences and Cryptography, 23(1), 209-220, 2020.

[86] M. Thebiga and Pramila, R. Suji. Reliable and Hybridized Trust Based Algorithm to Thwart Blackhole Attacks in MANETs using Network Preponderant Determinants. International Journal of Interactive Mobile Technologies (iJIM). 14. 42. 10.3991/ijim.v14i19.16391, 2020

[87] Sivanesh, S., Dhulipala, V.R.S. Accurate and Cognitive Intrusion Detection System (ACIDS): a Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks. Mobile Netw Appl 26, 1696–1704, 2021. https://doi.org/10.1007/s11036-019-01505-2

[88] Hassan Jari, Ali Alzahrani and Nigel Thomas. A Novel Indirect Trust Mechanism for Addressing Black hole Attacks in MANET. In Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '21). Association for Computing Machinery, New York, NY, USA, 27–34. https://doi.org/10.1145/3479243.3487296, 2021.

[89] Malik, A.; Khan, M.Z.; Faisal, M.; Khan, F.; Seo, J.-T. An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. Sensors, 22, 1897. https://doi.org/10.3390/s22051897, 2022

[90] Ebazadeh, Yaser & Fotohi, Reza. A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold. Security and Privacy. 5. 10.1002/spy2.183, 2021.

[91] Jamaesha, S. & Bhavani, S.. A secure and efficient cluster based location aware routing protocol in MANET. Cluster Computing. 22. 10.1007/s10586-018-1703-4, 2019.

Publications

PUBLICATIONS

1. K. R Kanchana and J. Viji Gripsy, **“A Survey on Recent Secure Routing Techniques in mobile ad hoc networks”**, International Journal of Future Generation Communication and Networking, Volume 13, Issue 3, pp. 594-602, April 2020 (Web of Science).
2. K. R Kanchana and J. Viji Gripsy, **“Secure Hybrid Routing to Thwart Sequential attacks in mobile ad hoc networks”**, Journal of Advanced Research in Dynamical and Control System, Volume 12, Issue 4, pp. 451-459, March 2020 (Scopus Indexed).
3. K. R Kanchana and J. Viji Gripsy, **“Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System”**, International Journal of Intelligent Engineering & System, Volume 15, Issue 6, pp. 237-236, August 2022 (Scopus Indexed).
4. K. R Kanchana and J. Viji Gripsy, **“Relaxed Hybrid Routing To Prevent Consecutive Attacks In Mobile Ad Hoc Network”,** International Journal of Internet Protocol Technology, Volume 16, Issue 2, pp. 92-98, June 2023 (Scopus Indexed, ESCI).
5. K. R Kanchana and J. Viji Gripsy, **“Protecting MANET from Distinct Attacks Using (SIIDAI) Protocol”,** Accepted Journal of Computer Science.
6. K. R Kanchana and J. Viji Gripsy, **“Improved network security by utilizing cloudy automated watermarking techniques”,** International conference on Computer Communication and Informatics, January 2023 – IEEE.

Secure Hybrid Routing To Thwart Sequential Attacks in Mobile Ad-Hoc Networks

Dr.J. Viji Gripsy, Assistant Professor, Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, India. E-mail: vijigripsy@gmail.com

K.R. Kanchana, Research Scholar, Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, India. E-mail: kanchumsc@gmail.com

Abstract--- In the recent trends, wireless networks and Mobile Ad-hoc Network (MANET) have yielded tremendous opportunity and popularity. This opportunity and popularity insisted on many kinds of research to focus on it. This highly flexible nature of the MANET also creates many network performance-related and security related issues. Various security vulnerabilities threaten the process in MANET in various ways. Sequence number attacks such as grey hole and black hole attacks are such dangerous attacks that significantly weaken the functioning and performance of the network in different situations. The proposed approach generates a fusion outline and that organizes with the Ad hoc on-demand distance vector (AODV) routing protocol to moderate these attacks. The new and modified protocol is named as SRD-AODV (Secure Route Discovery-Adhoc On-Demand Distance Vector) protocol. This protocol contains different components and methods to provide both proactive and reactive solutions by deploying effective authentication using the Elliptic Curve Diffie-Hellman algorithm (ECDHA) methods. This also aims to secure the data packets and routing table information and finally the incursion detection and prevention from sequential attacks in MANET. The performance of this protocol is measured with the help of performance parameters such as packet delivery ratio, and delay. The SRD-AODV protocol also compares with attacked AODV and other existing protocols.

Keywords--- MANET, Sequential Routing Attacks, AODV, Cryptography, Black Hole Attack, Grey Hole Attack, Denial of Service.

I. Introduction

The wireless network is widely used in a variety of applications. This marvelous growth is achieved because of the MANET nature such as dynamic infrastructure, instant topology [1]. The network generation can be dynamic and can set up anytime and anywhere. This highly flexible nature also creates many networks performance-related and security related issues. Various security vulnerabilities threaten the process in MANET in various ways. Sequence number attacks such as grey hole and black hole attacks [2] are such hazardous attacks that greatly weaken the functioning and performance of the network in different situations. Sequence number attacks and black hole attacks destroy certain count of data packets and discard them by deploying false routes and modifying the routing information. In the past, many researchers offered different solutions for detecting the sequence number attacks. In this research, a new technique and routing protocol are developed to proactively identify those attacks in MANET. This also helps to eliminate the false nodes in the network who are frequently misbehaving. The proposed SRD-AODV (Secure Route Discovery-Adhoc On-Demand Distance Vector) protocol contains secure neighbor node discovery for secure route discovery by selecting trusted node detection, hybrid cryptographic methods to secure the data packets and routing table information's and finally the incursion detection and prevention from sequential attacks in MANET. The proposed secure routing protocol finds legitimate nodes, provides a cryptographic shield to data packets using hybrid cryptography. This protocol also detects attacks that are implemented by malicious nodes and prevents these malicious nodes from routing by isolating them from the network with many restrictions. The popular open-source Network Simulator is used in simulations. The SRD-AODV protocol also compares with attacked AODV and other existing MANET protocols [3]. The proposed SRD-AODV routing protocol can guarantee that data packets travel through the network with maximum security. It achieves all security primitives such as authentication, non-repudiation, confidentiality, and integrity in a malicious environment. This SRD- AODV protocol guarantees that only legitimate nodes can participate and also achieves access control over the participants by distributing authentication keys before the routing process begins.

DOI: 10.5373/JARDCS/V12I4/20201458
ISSN 1943-023X

Received: 18 Feb 2020/Accepted: 25 Mar 2020

A Survey on Recent Secure Routing Techniques in Mobile Ad-Hoc Networks

Dr. J. Viji Gripsy[1] K. R. Kanchana[2]

Assistant Professor, Department of Computer Science,PSGR Krishnammal College forWomen, Coimbatore,India.
Research Scholar,Department of Computer Science,PSGR Krishnammal College for Women,Coimbatore, India.
vijigripsy@gmail.com[1],kanchumsc@gmail.com[2]

Abstract

In the current scenario, wireless technologies have attained massive popularity. This wireless technology is used in many applications. In wireless technology, Mobile Ad-hoc Networks (MANETs) are a part and it doesn't require any pre-established infrastructure. The dynamic character of those networks makes them more functional and it is suitable for many applications. MANET has high mobility and doesn't rely on centralized authority. This nature of MANET is more vulnerable to many security attacks and threats. When comparing to the traditional networks, ad-hoc networks are having higher chances for many routing attacks. Securing MANET is a challenging issue, which need more analysis. In past few years, numerous researchers proposed different solutions for detecting the routing attacks in MANET. In this survey, recent approaches and techniques done for MANET routing attacks is discussed. The review thoroughly presents the problems and merits of those existing approaches.

Keywords: *Mobile Ad-hoc networks, Secure routing, Security issues, Sequence number attacks, Proactive scheme*

1. Introduction

Mobile Ad-hoc Network (MANET) is a kind of wireless mobile devices together which communicates with each other. This type of network is infrastructure less based [1]. So the routing packets can be transmitted to any node without any infrastructure. Mobile Ad-hoc networks are battle field and natural disasters. For remote and rural areas long haul MANETs can also be useful where no communication and infrastructure exists. Nodes forming MANETs follow MANET routing protocols, which can be categorized into Proactive and Reactive. Proactive protocols consider the changes of topology at all times, and in Reactive protocols discover the necessary information only when they need it. Some principles of MANET routing protocols are similar to the traditional wired networks. When comparing to the traditional wired network, wireless networks are energy limited and the resources are challenged. The network topology is dynamic and the routes, links are not static. Mobile nodes are too vulnerable for several types of attacks. Secure routing Protocols are the best resolution to get rid of the routing vulnerability in MANET. Even in the presence of malicious routers, the Secure MANET routing protocols function effectively. This routing protocol provides assurance for security. However, the security protocols are affected by network overhead, Because MANET device are battery operated, and they cannot tolerate excessive overheads. With minimal overhead proactive safety functions are critical for proper functioning of Ad hoc networks. So, the designs of secure routing protocols are more challenging. The main aim of Secure MANET Protocols [2] is to achieve high security with less overhead. The routing protocols perform topology information exchange and the topology information can be used to find the optimal route. These MANET protocols include some features to mitigate attackers in MANET. In this paper, we first review different predictive techniques and recent approaches which address different routing security issues in wireless ad-hoc networks. Based on the analysis and summary, different types of future works can be established.

Received: July 8, 2022. Revised: August 25, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Protecting MANETs from Black and Gray Hole Attacks Through a Detailed Detection System

Vijigripsy Jebaseelan[1] **Kanchana Kavartty Raju**[1]*

[1]*Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, India*
* Corresponding author's Email: *kanchuphd22@gmail.com*

Abstract: In mobile ad-hoc network (MANET), identification and mitigation of black and gray-hole attacks is a challenging task compared to the detection of other attacks. To solve this issue, a secure route discovery ad-hoc on-demand distance vector (SRD-AODV) protocol has been suggested, which verifies the nodes only during the path discovery. But, it is necessary to authenticate the nodes during data transmission since the gray-hole nodes broadcast an accurate target sequence number (TSN) during the route discovery, whereas it becomes malicious and drops the packets during the data forwarding. Hence in this article, a secure route maintenance and attack detection AODV (SRMAD-AODV) protocol is proposed for identifying and defending the black and gray-hole attacks in the data transfer stage. Initially, an attack discovery system (ADS) node is decided from the connected dominating set (CDS) method based on energy and confidence score. The CDS is a robust, distinct and localized method to identify nearby linked dominating sets of nodes in a limited range in MANETs. The selected ADS nodes forward a status packet within the size of the dominating set to retrieve the entire behavioral data. ADS nodes examine gathered behavioral data and create a blacklist in which the suspected black and gray-hole nodes are added. Then, the blacklist is forwarded to the origin node to confirm the susceptibility of nodes present in the blacklist. Once the origin node authenticates the blacklist, it broadcasts a block message to all other nodes in a path for discarding blacklist nodes from the routing path. Further, this SRMAD-AODV protocol is simulated and the findings exhibit that it realizes 5.2sec of end-to-end delay (EED) and 86 % of packet delivery ratio (PDR) in contrast to the SRD-AODV protocol.

Keywords: MANET, Routing, Black-hole, Gray-hole, SRD-AODV, Connected dominated set, Attack discovery system, Status packet.

1. Introduction

MANETs are usually dynamic self-organizing platforms, with no centralized controller or resources for connectivity. If the mobile node is not under the other's coverage area, then each other nodes are decided to act as intermediate nodes for information transfer between those nodes. Also, each node travels individually and coordinates via fluctuating networks [1]. Thus, rapid fluctuations in network structure may cause many problems in routing protocol including robustness and tolerance to efficiency loss. The routing protocols are mainly split into two major types such as proactive and reactive protocols. Proactive protocols enable nodes to send packets periodically and to constantly decide the routes between any network nodes, independent of whether the routes are being used or not [2-4]. This relates to the capability that diffuses a huge amount of resources including power and throughput which is not ideal in MANET. In contrast, reactive protocols like AODV routing protocols need not require constant data transmission and only realize the route while two nodes are interacting [5].

Conversely, the routing protocols are influenced via collaborating with the suspected nodes in the system. An inadequate dynamic structure of MANET is highly susceptible to the different routing attacks [6] including black-hole, gray-hole, etc. Black-hole attacks are suspected nodes that appeared in the system in which the data forwarded or accepted are secretly rejected without notifying

Login Help Sitemap

INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Internet Protocol Technology > 2023 Vol.16 No.2

Title: Relaxed hybrid routing to prevent consecutive attacks in mobile ad-hoc networks

Authors: J. Viji Gripsy; K.R. Kanchana

Addresses: Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, Tamil Nadu, India ' Department of Computer Science, PSGR Krishnammal College for Women, Coimbatore, Tamil Nadu, India

Abstract: In the current trends, Wi-Fi networks and cellular ad-hoc community (MANET) have yielded incredible opportunity and recognition. This opportunity and popularity insisted on many forms of studies to recognition on it. This enormously bendy nature of the MANET additionally creates many community performance associated and protection associated problems. Numerous security vulnerabilities threaten the technique in MANET in diverse ways. The new and changed protocol is called Secure Route Discovery-Ad-hoc On-demand Distance Vector (SRD-AODV) protocol. This protocol includes one-of-a-kind additives and techniques to offer each proactive and reactive answers through deploying powerful authentication the use of the Modified Elliptic Curve Diffie-Hellman Algorithm (MECDHA) techniques. This additionally aims to comfort the records packets and routing desk records and subsequently the incursion detection and prevention from sequential attacks in MANET.

Keywords: MANET; sequential routing attacks; AODV; cryptography; black hole attack; grey hole attack; denial of service.

DOI: 10.1504/IJIPT.2023.131292

International Journal of Internet Protocol Technology, 2023 Vol.16 No.2, pp.92 - 98

Accepted: 15 Jun 2021
Published online: 06 Jun 2023 *

Full-text access for editors Access for subscribers Purchase this article

Comment on this article

Keep up-to-date

- Our Blog
- Follow us on Twitter
- Visit us on Facebook
- Our Newsletter (subscribe for free)
- RSS Feeds
- New issue alerts

Return to top

Contact us About Inderscience OAI Repository Privacy and Cookies Statement Terms and Conditions Help Sitemap