Detection of Clone Attacks in Manets using Ant Colony Optimization

Anubha, R P S Bedi

Abstract: Wireless and mobile computing enables the spontaneous networking of a system with or without previous set-up. Mobile Ad Hoc Network (MANET) is a Wi-Fi grid that has already been developed and does not require an existing infrastructure for a specific extemporaneous operation. Any node can then connect or exit the network, which will permit the attacker to access the whole system. These networks are liable to various attacks. This paper directs detection of the clone attack from MANETs in which the attacker node steals the id of the closing node, twin it and attracts all the data towards it. ACO noticed the clone attack and measured performance based on the packet drops, packet delivery ratio and network throughput.

Keywords: Network Security, Ant Colony Optimization (ACO), Hybrid ACO, Clone attack, PDR

I. INTRODUCTION

In recent decades, the network sector has developed so enormously that it has paved the way for a wireless era. Cellular wireless systems have been in use since the 1980s and have increasingly developed into wireless systems of the first, second and third generations. These systems work with a central support structure like a point of access. By using these access points, wireless users can be connected to the wireless system when they go from one location to another. A new wireless network is a new technology which enables users, independently of their geographical location, to access services and information electronically.

Ad-hoc networks continue to change rapidly, contributing to network instability. A smooth communication is therefore important. Mobile ad hoc networks (MANETs) are one form of network in which autonomous control is fundamentally necessary. A decentralized independent wireless system consisting of free nodes and an independent organizing capability, MANET, has a strong role to play. At any time, nodes may join or leave. The network is not fixed. There's no central control or description and all nodes are the same. No routers are recognized, nodes are used and data packets are transferred from node to node multi hop. [1]. Nodes within the radio range of the other depend on their intermediary nodes to communicate directly through wireless linkages.

The capacity of MANETs to create networks anywhere without any existing infrastructure [2] can be used in various future applications. As the network topology is constant to alter, routing is a central issue because of a lack of centralized control.

To order to reduce the signal quantity of MANET due to the maintenance of valid routes, MANET requires efficient routing algorithms that improve overall MANET system performance. Not only should a MANET routing algorithm be able to find the shorter route between source and destination, it should also adapt to changing node conditions, changing network load conditions, and changing environmental conditions [2].

II. RELATED WORK

Several researchers have recently researched biological species ' collective behavior as an analogy that offers a natural model for the problems associated with combinatorial optimization. There have already been a variety of ants routing algorithms. Most of them are based on the ACO which is a meta-heuristic technique for the resolution of probability technology-based computational problems.

A. Hybridized Ant- Colony Optimization (ACO)

In order to resolve the salesman's problem, Mohsen proposed a hybrid algorithm for ACO, SA, mutation provider and local search. The ACO is the foundation of the algorithm. The SA and mutation operator have been used from time to time to increase the population diversity of the ants and to effectively leverage the current search area using local search.

The comparative experiments, which have been conducted on 24 of the TSPLIB TSP instances, show that the proposed algorithm surpassed some popular literature solution efficiency algorithms. Roy et al. have suggested a novel ad hoc mobile QoS algorithm. In the proposed algorithm, Ant Colony and OLSR are merged to spot stable paths between source and target nodes. One of the main problems in MANET is routing because of the versatility of nodes. When it's time-to-varying QoS, limited resources, and energy etc, complexity increases because of different characteristics including dynamic topology. QoS routing plays a main part in implementing QoS in ad hoc wireless networks. Zhang et al. recommend a systematic management plan for addressing the energy consumption issue in data centers. For a cloud data center is a resource planning system design and Stochastic Petri Net analyzes this system. A LET-ACO method is proposed; it can effectively reduce data center power consumption on the basis of a performance guarantee. The simulation tests on CloudSim [17] are performed to verify the efficiency of our proposed method. The future work deals with building an in-depth system prototype in particular to report the data center or design a new type of model which can be very useful for an analysis of certain issues in the cloud data center, like

Revised Manuscript Received on March 11, 2020.

Anubha, Research Scholar, I.K. Gujral Punjab Technical University, Kapurthala.

Dr. Ravneet Preet Singh Bedi, Research Scholar, I.K. Gujral Punjab Technical University, Kapurthala.

heterogeneous scheduling of tasks and failure detection and we will be able to take farther factors into consideration.

B. Clone Detection Techniques

Wireless sensor networks (WSNs) face clone attack threats that can initiate a range of additional attacks to monitor or harm the networks. A tale distributed clone detection [12- 16] protocol is proposed by Zhang et al. for randomly deployed networks with low resource expenditure. In the non-hotspot region of the network, it is implemented in a ring structure, which manages the use of resources throughout the system, the system consisting of the establishment of the Witness Chain and the production of clone detection track. The witness chains and detection paths are respectively in the centrifugal and circumferential direction that may confirm the meeting of watchers and detection paths of sensors with the alike identification but dissimilar locations to identify clone attacks.

Li et al. proposed a detection based method that is simultaneously API-equivalent. For a particular method, the author automatically generate the test cases and search by running the created test cases to semantically equivalent API methods. In each case, when two procedures generate the same output, they are considered as semantically comparable approaches. One of the drawbacks of clone detection based on tests is that it frequently takes longer.

Wireless (WSN) sensor networks typically comprise of a huge quantity of random, less-price sensor nodes in the deployed region with limited resources. The networks were commonly used in a range of arenas for incident surveillance and information collection, comprising environmental monitoring, jungle fire observing, information gathering for traffic and information collection for battlefields [9-11]. Numerous WSNs are however positioned in tough or unfriendly surroundings that are a challenge for their safe working. Numerous sensor nodes are cooperated or targeted by the attackers because the wireless communication is open and the security is insufficient [8]. A clone attack which applies to several nodes with the similar identity, is one of the toughest attacks.

Cloning the code guides to multiplying the source code. For software development it is the technique to reuse source code. If the code section has a flaw, all relevant parts should be tested for the identical virus. This cloning procedure will therefore cause virus circulation, which will have a significant impact on maintenance costs. Code clone detection (CCD) looks as a dynamic region of investigation by looking at this problem. Consequently, in this study, Ain et al. systematically examine the newest tools and methods used for the finding of code clones.

III. PROPOSED WORK

When the source node has data to forward to destination node, it broadcasts forward ants in the network to find a route to final node. During their journey to destination node, the nodes deposit pheromone value over the links. When the destination node is find, it creates the backward ants which trace the route back to the source node. However, there may be a node present in the system which has copied the id of the original destination node. In such case, the malicious clone node will send backward agents to the source node. If the packets are dispatched to the clone of the destination, it will lead to packet loss in the network.

In the proposed scheme, when the source node receives backward ants from the clone of the destination node, the source node will take help from the one its immediate one hop neighbors. The source node will send the route request packet again over the path from which backward ants have been received. This time the route request packet will have the id of the destination set as the id of one of the immediate neighbors of the source node.The malicious clone node will again assume the id of the new destination and address back the backward ants to the source node. Now, the source node would own same pheromone value for two different destinations which will allow the starting node to notice the malicious clone node which starts the backward ants for the route request made second time by the starting node.

IV. RESULTS AND DISCUSSION

The framework suggested has been implemented using NS2. Network Simulator (Version 2), commonly called NS2, is simply an open-source simulation event-driven instrument which has been shown to be useful to study the dynamic nature of communication systems. NS2 (e.g. routing algorithms, TCP, UDP) is used to simulate wired and wireless network functions and protocols. It has various levels and features including multi-layer set of different protocols-Ad-hoc Routing (DSDV, DSR, AODV), MAC (802.11, 802.3, TDMA) and Visualization (NAM), Tracing etc.

A. Simulation Parameters

Throughput: It is known as the total number of packets delivered over the whole time of simulation. That can be described mathematically as:

$$\text{Throughput}= N/1000 \qquad (1)$$

Where N is the number of bits received successfully by destination.

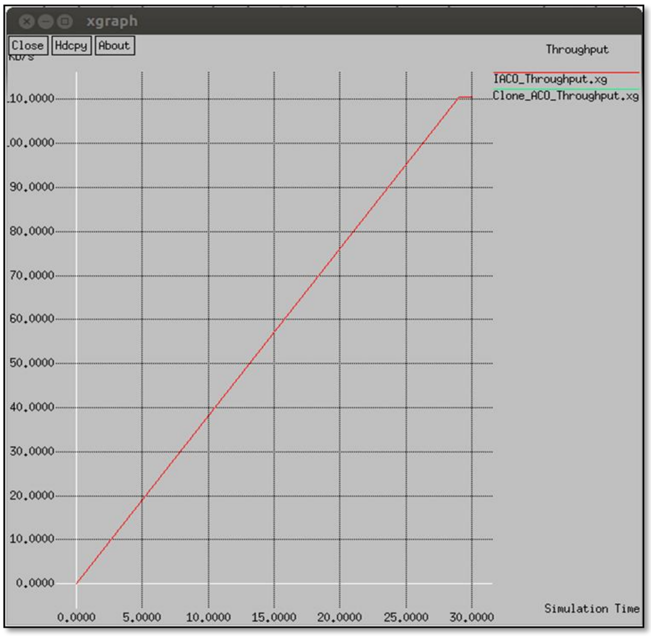

Figure 1. Throughput of the network under attack and after detection

DOI: 10.35940/ijeat.C6297.049420

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Figure 1 depicts the association of the procedure proposed to network under the clone attack on the basis of throughput generated. Under the clone attack, the destination node does not receives any packet since the packets are sent to the clone node. Therefore the value of throughout becomes zero. However, when the attack gets detected using ACO, the value of throughput was 110 Kbps in view of the original destination receives the packets from the source node.

Packet Delivery Ratio (PDR): Packet Delivery Ratio [18-20] is interpreted as the ratio of packets successfully received to the total sent packets.

The figure2 shows the comparison by packet delivery ratio of the proposed technique and network under the clone attack. The graph shows that under the clone attack, the value of PDR would as low as 0.21. Nevertheless, after the detection of the clone attack, the value of PDR was 0.44.

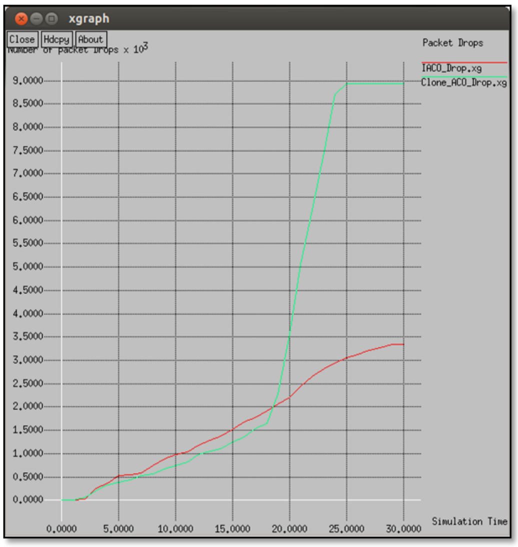

Figure 2. Packet Delivery Ratio Comparison

Packet Drop: It is the number of packets dropped in the grid

The figure 3 graph shows that when the clone attack happens, the number of packet drops were very high because the clone node dropped the packets. Under the proposed technique, less number of packets were dropped in the network.

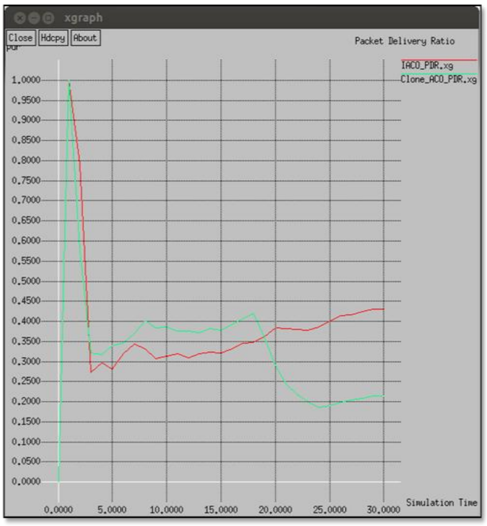

Figure 3. Packet Drop Comparison

V. CONCLUSION

Routing in a MANET has become a demanding task because of the complex topology and lack of an existing fixed infrastructure. These networks are susceptible to number of attacks because of decentralized environment. This paper focuses on detecting the clone attack using ant colony optimization. Network efficiency was compared based on the performance, packet distribution and packet drops. Under the clone attack, the network experienced extra packet drops in the network which reduced the packet delivery ratio and throughput as well. However, after detection the values showed an improvement which justifies the proposed technique.

REFERENCES

1. Ducatelle, F., Di Caro, G., & Gambardella, L. M., “Ant Agents for Hybrid Multipath Routing in Mobile Ad Hoc Networks,” *Second Annual Conference on Wireless On-Demand Network Systems and Services*, Jan. 2005.
2. Batth K. K., & Singh R., “Performance Evaluation of Ant Colony Optimization based Routing Algorithms for Mobile Ad Hoc Networks,” International Journal of Advancements in Computing, vol. 8, no. 2, pp. 1-7, March 2017.
3. Mohsen A. M., “Annealing Ant Colony Optimization with Mutation Operator for Solving TSP,” *Computational Intelligence and Neuroscience*, vol. 2016, Nov. 2016.
4. Roy B., Banik S., Dey P., Sanyal S., & Chaki N., “Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services,” *Networking and Internet Architecture*, vol. v1, Dec. 2013.
5. Zhang W., Ma T., & Gao Q., “Ant Colony Optimization Algorithm to Dynamic Energy Management in Cloud Data Center” *Mathematical Problems in Engineering*, vol. 2017, pp. 1-10, Dec. 2017.
6. Ain, Q. U., Butt, W. H., Anwar, M. W., Azam, F., & Maqbool, B., “Recent Advancements in Code Clone Detection – Techniques and Tools,” *IEEE Access*, vol. 7, pp. 86121- 86144, May 2019.
7. Zhang Z., Luo S., Zhu H., & Xin Y., “A Clone Detection Algorithm with Low Resource Expenditure for Wireless Sensor Networks,” *Journal of Sensors*, vol. 2018, pp. 1-16, Mar. 2018.
8. Butun, S. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” in *2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, vol. 16, no. 1, pp. 266–282, Istanbul, Turkey, May 2014.
9. Y. Zhang, S. He, and J. Chen, “Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks,” in *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, vol. 24, no. 3, pp. 273–281, New Orleans, LA, USA, June 2013.
10. Y. Hu and A. Liu, “An efficient heuristic subtraction deployment strategy to guarantee quality of event detection for WSNs,” *The Computer Journal*, vol. 58, no. 8, pp. 1747–1762, 2015.
11. L. Jiang, A. Liu, Y. Hu, and Z. Chen, “Lifetime maximization through dynamic ring-based routing scheme for correlated data collecting in WSNs,” *Computers and Electrical Engineering*, vol. 41, pp. 191–215, 2015.
12. Li, G., Liu, H., Jiang, Y., & Jin, J., “Test-based Clone Detection: An Initial Try on Semantically Equivalent Methods,” *IEEE Access*, vol. 7, pp. 77643- 77655, Nov. 2018.
13. Dong, M., Ota, K., Yang, L. T., Liu, A., & Guo, M., “LSCD: A Low-Storage Clone Detection Protocol for Cyber-Physical Systems,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 5, pp. 712–723, May 2016.
14. Shi, H., Wang, R., Fu, Y., Jiang, Y., Dong, J., Tang, K., & Sun, J., “Vulnerable Code Clone Detection for Operating System through Correlation Induced Learning,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, Dec. 2019.
15. Cho, K., Jo, M., Kwon, T., Chen, H.-H., & Lee, D. H., “Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks,” *IEEE Systems Journal*, vol. 7, no. 1, pp. 26–35, Mar. 2013.

16. Liu, J., Wang, T., Feng, C., Wang, H., & Li, D., “A Large-Gap Clone Detection Approach Using Sequence Alignment via Dynamic Parameter Optimization,” *IEEE Access*, vol. 7, pp. 131270–131281, Sept. 2019.
17. Jammal, M., Hawilo, H., Kanso, A., & Shami, A., “ACE: Availability-aware CloudSim Extension,” *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1586- 1599, Dec. 2018.
18. Yang, B., Chen, Y., Cai, Y., & Jiang, X., “Packet Delivery Ratio/Cost in MANETs With Erasure Coding and Packet Replication,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 2062–2070, May 2015.
19. Jacobsson, M., & Rohner, C., “Estimating Packet Delivery Ratio for Arbitrary Packet Sizes Over Wireless Links,” *IEEE Communications Letters*, vol. 19, no. 4, pp. 609–612, April 2015.
20. Zhu, Y.-H., Chi, K., Tian, X., & Leung, V. C. M., “Network Coding-Based Reliable IPv6 Packet Delivery Over IEEE 802.15.4 Wireless Personal Area Networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2219–2230, April 2016.
21. Madhavan, P., “Framework for QOS Optimization in MANET using GA-ACO Techniques,” *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Mar. 2019.
22. Siemiński, A., “Ant Colony Optimization Parameter Evaluation,” *Multimedia and Internet Systems: Theory and Practice*, vol. 183, pp. 143–153, 2013.
23. Li, P., & Zhu, H., “Parameter Selection for Ant Colony Algorithm Based on Bacterial Foraging Algorithm,” *Mathematical Problems in Engineering*, pp. 1–12, Dec. 2016.
24. Shu, T., & Krunz, M., “Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks,” *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813–828, April 2015.
25. Mahmoud, M. E., & Xuemin Shen., “An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks,” *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3947–3962, Oct. 2011.
26. Chang, B., Zhao, G., Chen, Z., Li, L., & Imran, M. A., “Packet-Drop Design in URLLC for Real-Time Wireless Control Systems,” *IEEE Access*, vol. 7, pp. 183081- 183090, July 2019.

AUTHORS PROFILE

Anubha, Research Scholar at I.K. Gujral Punjab Technical University, Kapurthala. She has done MCA and currently pursuing Ph.D in in I.K. Gujral Punjab Technical University.

Dr. Ravneet Preet Singh Bedi, is presently serving as Joint Registrar in I.K. Gujral Punjab Technical University, Kapurthala. He is the head of department of Student Affairs. He has done his M.C.A. and Ph.D in Computer Science & Engineering. He also holds the prestigious certification such as Microsoft Certified Systems Engineer (MCSE). He has also completed another Ph.D. in Computer Science & Engineering from the Faculty of Engineering, Punjabi University, and Patiala. Dr. Bedi has published research papers in reputed International Journals and articles in Computer science and education in National journals and magazines. He has also chaired a session on networking at an international conference, “WORLDCOMP'10,” the world Congress on Computer Science, Computer Engineering and Applied computing held at Las Vegas in the USA. He has also participated in an International conference on Skill development organized by Indian High Commission, UK at London.