International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Approach to Detect Wormhole Attack in Mobile Ad Hoc Networks Using Direct Trust Based Detection Approach

Shruti Thapar, Amol Purohit, Budesh Kanwer, Akash Jaiman, A. Mounika, V. S. Madhumala

Submitted: 09/02/2023 **Revised:** 13/04/2023 **Accepted:** 05/05/2023

Abstract: Mobile ad hoc organization is used in numerous applications climate strategic projects or standard gadget organization. The reason toward the rear of the developing acknowledgment of magnets is the simple accessibility of compact gadgets. The versatile Ad Hoc Network isn't simply smooth to introduce yet notes might be presented or eliminated powerfully shape it. Besides, the local area doesn't need a proper foundation. The above expressed make magnet exceptionally reasonable in various bundles however at the expense of raised weakness to Cyber-assaults. The greatest imperative attacks in Manet are wormhole attack and jellyfish assault. The writing needs inside the methods that could endless supply of these assaults simultaneously. In this examination we've proposed a coordinated strategy that is equipped for stagger on both wormhole and jellyfish assault the utilization of indistinguishable boundaries.

Keywords: *MANET, Wormhole Attacks, Jellyfish Attack, Routing Protocols, Performance Metric.*

1. Introduction

The mobile ad hoc organization can be portrayed as an arrangement of remote cell hubs which have the usefulness to set up themselves progressively in erratic and going organization geographies. As such magnet is an arrangement of monstrous wide assortment of portable hubs which could powerfully enter and disappear the organization. This sort of organization is profoundly decentralized one and does never again have a proper framework. The above noted features make MANET an especially reasonable organization anyway those qualities likewise are responsible for making MANET recognizably at risk to some of Cyber attacks. In pristine age of expanding realities move private is the guideline trouble in any organization and can't be compromised. In any case, with the appearance records Technology, assailants are really ready to set attacks each free from internal notwithstanding outside the local area. The conventional security highlights aren't enough for ensuring security in that frame of mind. Security in MANET depends intently upon the cooperation of the hubs [1].

Electronics and Communication, (Asst. Prof.), PIET, Jaipur, (RTU,KOTA), Jaipur, Rajasthan ,India, shruti.thapar@poornima.org
Electronics and Communication, (Asst. Prof.), Sree Dattha Institute of Engineering and Science, Hyderabad ,India, amolpurohit.sdes@gmail.com
Artificial Intelligence and Data Science, (Prof.), PIET, Jaipur, (RTU,KOTA), Jaipur,Rajasthan ,India, budesh82@gmail.com
Computer Science Engineering, (Asst. Prof.), PIET, Jaipur, (RTU,KOTA), Jaipur,Rajasthan ,India, akashjaiman@gmail.com
Computer Science Engineering, (Asst. Prof.), Sree Dattha Group of Institutions, Hyderabad ,India, gangimounika@gmail.com
Computer Science Engineering, (Asst. Prof.), Sree Dattha Group of Institutions, Hyderabad ,India, vmadhumalacse@sreedattha.ac.in

1.1 Wormhole Attack:

During a wormhole assault, aggressors make a topological trickiness within the community. Additionally, least malignant middle factors are speculated to bring this form of attack. The underlying step on this shape is the introduction of wormhole tunnel. Wormhole tunnel Represent the direction between the attackers. The Wormhole access can be made by means of modes, name d out of Band channel a advent invalid. The outer layer of channel comprise high strength connect among the pernicious hubs while in design channel the ordinary Tunnel is formed by means of utilizing various hubs inside the organization. The Wormhole misfortune deceives the victim notes in accepting that the objective hub can be arrived at in a considerably less significantly quicker through following a selective correspondence course. At the point when the victim hubs decide to take the above-alluded to verbal trade Path it transforms into a piece of wormhole burrow. The Wormhole assault is laid out in figure 1. It could be without trouble seen that the nodes N1 and N2, which aren't adjoining hubs seemed, by all accounts, to be essentially one portion of away because of the effect of wormhole attack. In various words, wormhole burrow causes extraordinary modes in organization to accept that there might be a more limited method for arriving at the surrender hub. Accordingly, the course among the inventory hub S and holiday destination hub D get empowered. The hubs select the course with fewer jumps. For example, in fig.1 the source word picks the

course made by Wormhole aggressors. The aggressors could similarly convey refusal of-organization (DOS) assault.

1.2 Jellyfish Attack:

Recognizing jellyfish assault is a demanding task because of the reality this kind of attack consents to all the steering techniques. The Attack hubs at the hubs sending off jellyfish assault keep on being vivacious each in bundle sending and root Discovery that permits you to stay away from recognition. The jellyfish assault hubs can upset the normal working of the organization by utilizing bundle alteration, parcel losing for developing butterflies. Discovery of jellyfish assault in a TCP connection is bounty more confounded as the direct of jellyfish assault is regularly off-base for network clog. Numerous techniques were introduced in the previous years to recognize and moderate wormhole and jellyfish assaults. However, to the creator's mastery there are just not many examination, that have proposed a strategy that has detected both wormhole and jellyfish assault. The reason for this research is to exhibit an included methodology for recognizing the two harmful attacks ad hoc networking. The unwinding of the paper comprises of: Section II gives a fast understanding into present country of fine art, in fragment III the execution data are referenced, stage IV shows the outcome.

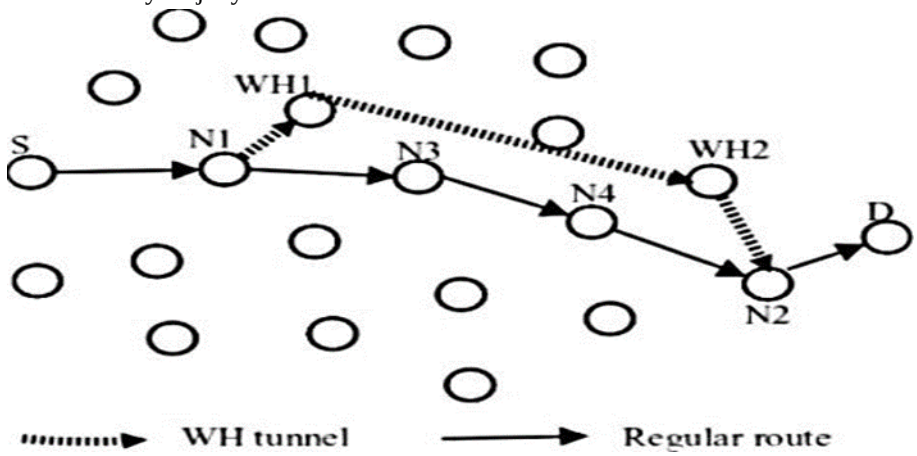

Fig. 1: Frame of Wormhole attack [5].

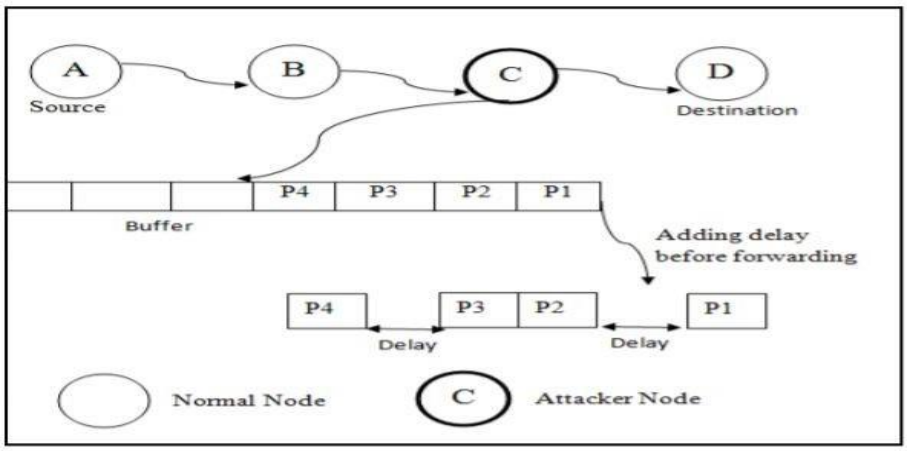

Fig. 2: Frame of Jellyfish delay variance attack [7].

2. Background

Forestalling this kind of assaults has stayed an essential examinations issue over the course of the past years. Both equipment and programming based absolutely approaches not entirely set in stone inside the writing. Movement of the Watchdog show poisonous lead of center points is stated in [7]. In this, the nodes which denied sending the groups to the vacation spot center points are contemplated to be pernicious. Attestation and group drop extent are the overall show resting cushions used on this system. The use of a 1 digit to find wormhole nodes is given in [8]. In this show each time the notice x gets a sales to associate from a center point y. The creators have involved an extraordinary kind of equipment for computing the opportunity to reaction or the put off. If the defer is past an edge cost it could be deciphered that it the hub y is a malignant hub. One more utilization of the Watchdog convention for distinguishing pernicious hubs inside the organization can be found in [9]. In on this examination works of art the general presentation of the nodes buy delay in sending and dropping parcels is utilized in light of the fact that the

marker. Confirmation essentially based system that utilizes the area of hubs to recognize presence of malevolent hubs in the organization is presented in [10]. Convention dependent absolutely upon limited country gadget and notices model is given in [11]. Two domains acknowledgment for assurance of wormhole assault is given in [12]. In this method throughput and bundle transport extent are used for revelation and separation of the assault. A comfortable steering convention known as WARP is created in [13]. Twist gives multipath steering and might be viewed as an augmentation of AODV convention. In this convention in the event that the hyperlink between two notes surpasses an edge cost, search hubs are managed pernicious and are disposed of from the organization. Albeit many responses were proposed in setting of Jelly fish assaults, but by and by those techniques are not efficient and ideal in expressions of viability and proficiency. There isn't any such response found which fits pleasantly in each less and huge amount of hubs arrangement. The unfriendly outcome of jellyfish assault is endorsed in [14] with assistance of multiplication. It is changed, trying to break down as it enthusiastically follows the show lead; however the proliferation was accomplished on relatively few nodes. Two strategies for ID and balance of jellyfish attack are shown in [15]. The plans are known as bunch essentially based interruption location and anticipation strategy (CPIDT) and striking group based absolutely interruption recognition and avoidance procedure (SPIDT). As they consider shows those procedures uses the thoughts of grouping for following the organization. In this approach a mortar had video show units the assortment of bundles inside the cradle. CPIDT is utilized while a middle of the road hub is sending off jellyfish attack though SPIDT subtleties utilized while the bunch head itself acts perniciously. The writers in [16] laid out that perusing specific boundaries of Transmission oversee boundaries which incorporate crippling quick retransmission and permitting particular ACK can assist in discovery of jellyfish with going after. In such method a bunch head is doled out the test of sending charge computation in light of the time cost of the parcel. Hereditary arrangement of rules is utilized for forestalling jellyfish attack in [17]. A clever measurement to rearrange thickness is used in [18] to forestall jellyfish assault. Recipient record is utilized to compute the reorder thickness. In any case the investigation materials are restricted to area and no methodology is introduced for evasion of jellyfish assault. Changed SHA - 1 game plan of rules and time locale KEY cryptography is spread out in [19]. The arrangement is basically established on Hash Function in any case it causes above in transmission of faker groups.

3. Research Method

3.1 Parameter initialization:

The initial step is boundary introduction. In this stage a WSN of 100 hubs is made through setting essential qualities like Bandwidth, Frequency, getting limit. In the ensuing step of hub defining directions of nodes are unmistakable. In this exploration 2D people group is thought about, thus z direction of the hubs is all 0. Every hub is given a special locale in a 2D area of seven-hundred*seven-hundred. Locally 100 hubs are appropriate hubs and 10 hubs are assault hubs. The way float is demonstrated in Figure 3,

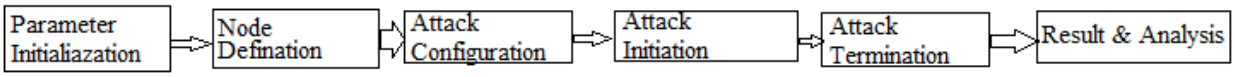

Fig. 3: Frame of Jellyfish delay variance attack [7].

3.2 Wormhole Attacks detection

DSR is an extensively elaborate open show in impromptu associations. These sorts of messages involved by DSR controlling show for turning out course, particularly, heading interest route request and course reply. The route request message is used best in the event that the course store. The technique for way Discovery starts when the RREQ package is dispatched. It is way, which takes region why broadcasting request message. After the previous center point has capably protected its ID to the demand. The reply message is transport by using the center centers. The execution of wormhole attack may be obvious in Fig. 3 and Fig 4. The Bogus request may be used to do the sinkhole assault. If the principal RREQ is extensively not exactly the fake request, the midway nodes will discard the primary RREQ and the conversation might be diverted to the poisonous nodes. It may be communicated that the Wormhole attack prompts break and thus removal of the way; here it tends to be observed that the centers are moving nearer or all things considered cutting down their verbal exchange arrangement.

3.2 Jellyfish Attack Detection

Distinguishing proof and avoidance of jellyfish assault is been discussed here, consequently immediate concur with based recognition (DTD) set of rules is utilized. The calculation is laid out in this sort of way that it could forestall every one of the three variations of jellyfish attack in particular occasional disposing of, parcel reordering and put off change. The proposed procedure is conveyed in ns2 test system on a TCP based absolutely

MANET. The arrangement of rules begins through growing a trust table with work area for all hubs inside the organization. In our model, every hub n makes entrust table with work area. Yn [k] is the trust an incentive for hub given by hub n. Just the adjustments in the end update are passed on the way on to limit the correspondence above. In the event that they consider expense doled out to a note through its partners is not exactly the foreordained limit cost then search a word is named as jellyfish word or malevolent hub. A clock is connected with dubious node. The clock increases at point when the hub is dubious by utilizing the adjoining hubs. Is the notification is Mark dubious for multiple occurrences then the important kind is block recorded from the organization for the total lifetime.

Parameter	Value
Area	700*700 m2
Bandwidth	512 KB
Frequency	2.4GHz
threshold	4.5KHz
Antenna.	Omni directional antenna.
Authentic Nodes	90
Attack Nodes	10

Table 1: Experimental Settings.

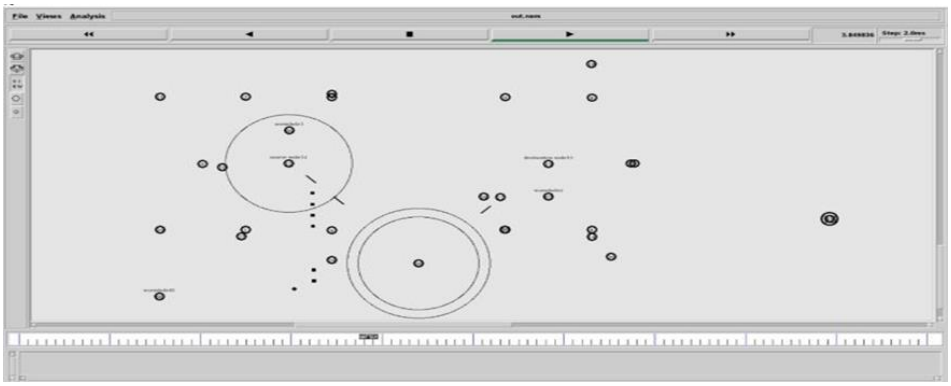

Fig..4: 100 nodes setup.

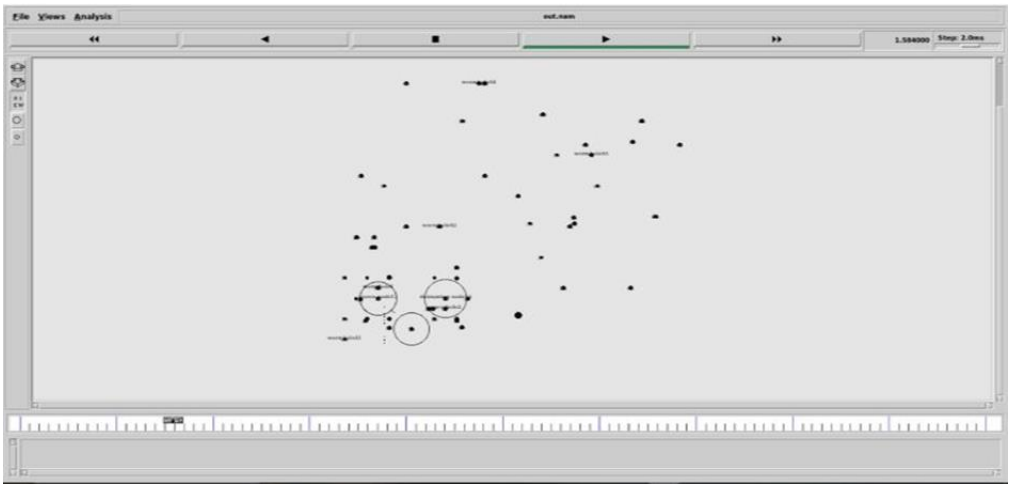

Fig. 5: Initiation of wormhole attack.

Fig. 5: Removal of wormhole attack.

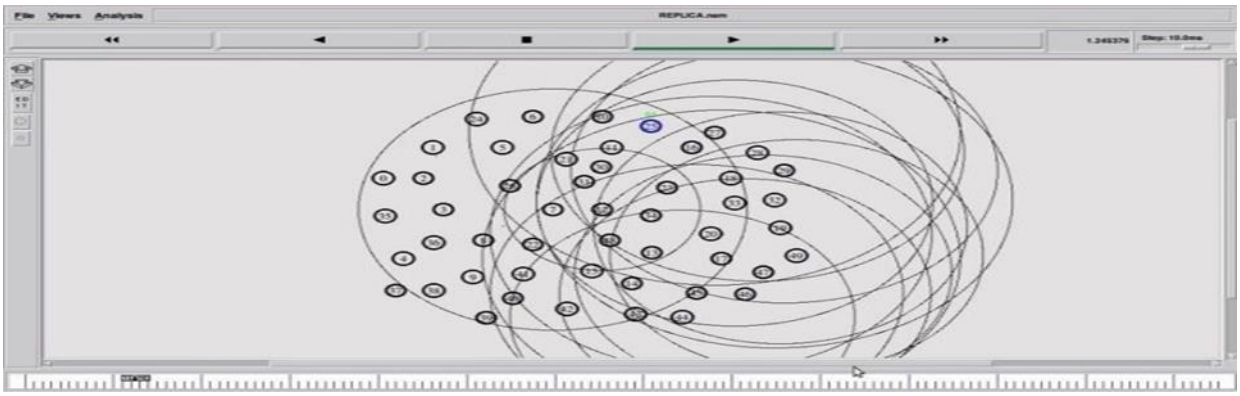

Fig. 6: Startup of Jellyfish attack.

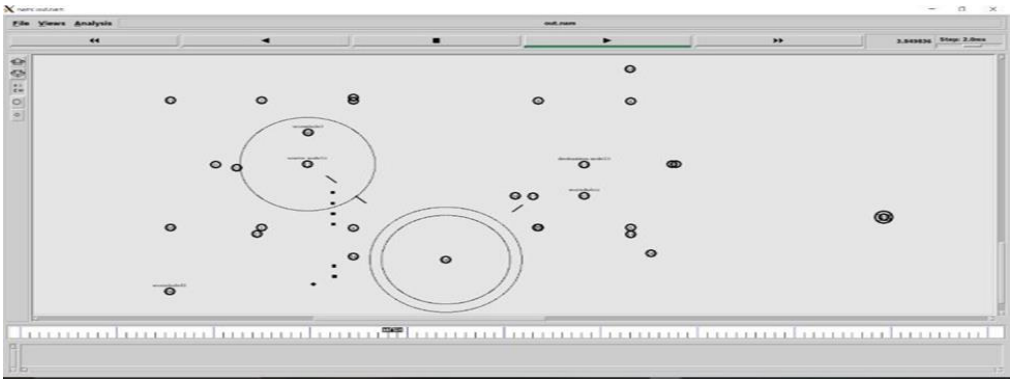

Fig. 7: Removal of jellyfish attack.

4. Result

The commencement of jellyfish assault on an organization of hundred hubs is demonstrated in figure 5. It

could be resolved that at this degree limit of the hubs are kindled. The reaction of the designed estimation can be seen in fig. 6. Remote Mesh association of hundred notes is made in ns2 test framework. Nodes can send messages upto 250 meters. To ensure the center point flexibility sporadic waypoint structure is used. From the outset the association is inspected impact of warm void assault. Bundle movement extent and quit giving up put off are the overall show limits used in this investigation. The delay with and without wormhole attack can be measuredin Fig 8. It will in general be tracked down that End to stop put off impact upon the start of attack. The strong response of the association as opposed to wormhole assault should be visible in Fig 9. For this situation the blue line addresses the parcel move expense while there is no malignant hub, pink line addresses the attack and green line addresses the bundle move charge after the proposed set of rules takes out the malevolent hubs. The practically identical unique reaction might be found in the event of jellyfish assault in Figure7. The stop to stop put off with and without ID of jellyfish assault is spread out in Figure 10. The throughput got in the event of diminishing amount of jellyfish assailants can be apparent in Figure 11. It very well may be resolved that the proposed calculation supplements throughput of the gadget by putting off pernicious hubs.

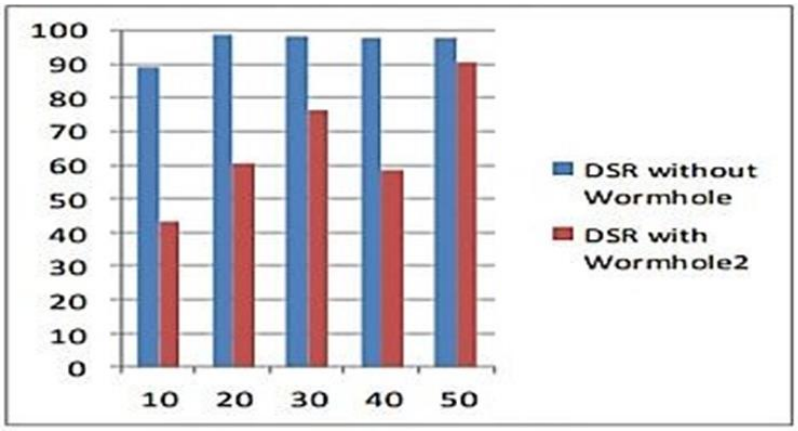

Fig. 8: Packet delivery ratio with and without wormhole attack.

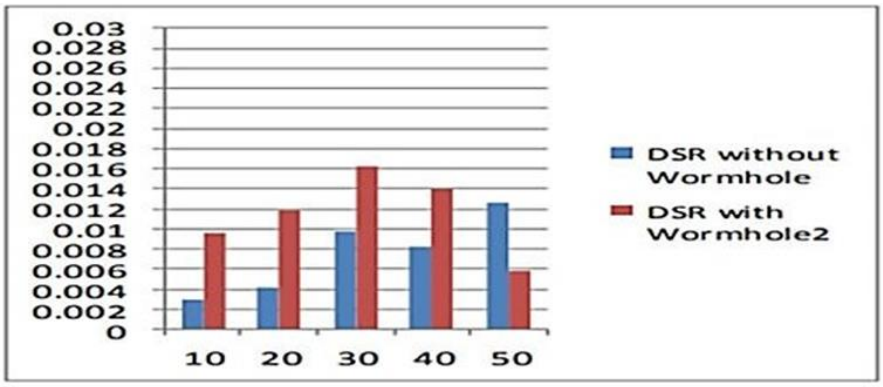

Fig. 9: End to end delay with and without wormhole Attack

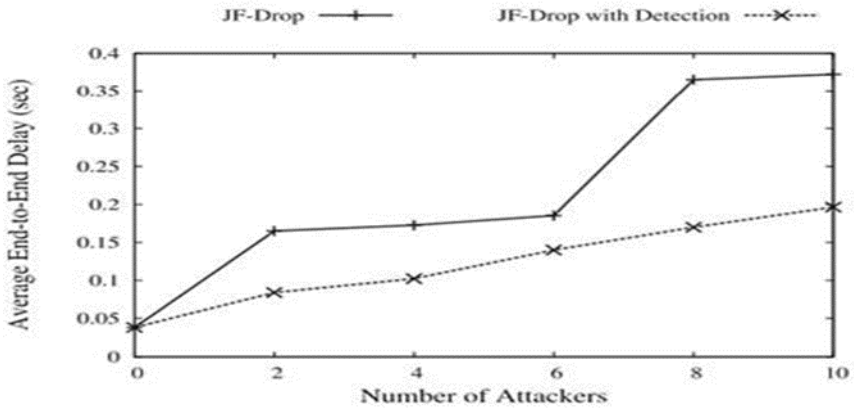

Fig. 10: End to end delay with increasing number of JF attackers.

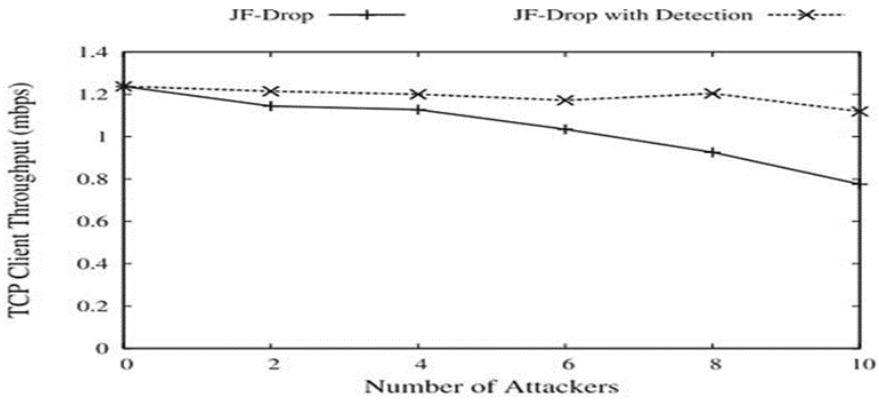

Fig. 11: TCP throughput with lesser number of JF attackers.

5. Conclusion

In this study an organized strategy is introduced for distinguishing and hindering wormhole and jellyfish attack in MANET. The exceptional features of MANET make it helpless to remove an attack. However in writing numerous procedures are proposed to stagger on and save you the equivalent, but the examinations needs expressions of calculations which could forestall both of these simultaneously. A fundamental explanation for this is that the counteraction procedures for every one of these assaults work on various boundaries and organization design. In this paper the creators have offered a consolidated procedure for recognizing and forestalling both wormhole and jellyfish assault. The proposed calculation is reenacted on NS2 test system and the general presentation is assessed with 100 hubs based on End to stop defer and throughput. It may be contemplated that the proposed approach major areas of strength for is perceiving and ending both the above alluded to assaults and works adequately with extending extent of centers.

References

[1] International conference on recent cognizance in wireless communication & image processing "A Review on Performance Evaluation of Routing

Protocols in MANET" (December'2014), *PUBLISHED IN SPRINGER 2015 EDITION*.

[2] Ahmed, Diaa Eldein & Khalifa, Othman, "An Overview of MANETs: Applications, Characteristics, Challenges, and Recent Issues," International Journal of Engineering and Advanced Technology (IJEAT) ISSN, pp. 2249 – 8958, 2017.

[3] Shruti Thapar and Sudhir Kumar Sharma, "Analysis of Isolation access of Wormhole Attack in Mobile Ad hoc Network using Delay Prediction Technique", International journal of Advanced Science and Technology (IJAST), ISSN: 2005-4238 IJAST, volume-29 issue-6, 2020, page no.-9401-9411.

[4] W. A. Aliady and S. A. Al-Ahmadi, "Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 84132-84141, 2019.

[5] Shruti Thapar and Sudhir Kumar Sharma, "Study of Direct Trust Based Detection Algorithm for Prohibiting Jellyfish Attack in MANET", ILKOGRETIM Online, doi: 10.17051/ ilkoline.2021.04.234, volume 20 issue 4, 2021, page no. -2052-2057.

[6] Azer, M. & El-Kassas, Sherif & El-Soudani, Magdy, "A Full Image of the Wormhole Attacks - Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks," 2009.

[7] Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rajkumar Kaushik, "A Secure Routing for MANET using Internet of Things", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp. 2957-2965.

[8] V. Krundyshev, M. Kalinin and P. Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks," 2018 IEEE Industrial Cyber- Physical Systems (ICPS), pp. 795-800, 2018.

[9] Shruti Thapar, M Venu Gopala Rao, Babita Jain, Rohan Sharma , "Research Article on Routing Protocols for MANET: A Review", International Journal of Early Childhood Special Education (INT-JECSE)DOI:10.9756/INTJECSE/V14I5.305 ISSN: 1308-5581 Vol 14, Issue 05 2022, pp 2939-2949.

[10] S. Sachdeva and P. Kaur, "Detection and analysis of Jellyfish attack in MANETs," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, pp. 1-5, 2016.

[11] S. Doss et al., "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," in IEEE Access, vol. 6, pp. 56954-56965, 2018.

[12] J.Dromard, R. Khatoun, L.Khoukhi, "A watchdog extension scheme considering packet loss for a reputation system in wireless mesh network," In: 20th International Conference on Telecommunications (ICT 2013). Casablanca, Morocco, pp 1–5, 2013.

[13] Capkun S, Buttyán L, and Hubaux JP SECTOR "secure tracking of node encounters in multi-hop wireless networks" In: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks

[14] (in association with 10th ACM conference on computer and communications security) Fairfax, VA, United States, 2003.

[15] Dias JA, Rodrigues JJ, Xia F, Mavromoustakis CX, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks" IEEE Trans Ind Electron, pp. 7929–7937,

[16] 2015.

[17] Biswas J, Gupta A, and Singh D WADP, "a wormhole attack detection and prevention technique

[18] in MANET using modified AODV routing protocol" In: Arya KV, Sunil Kumar (Eds) 9th international conference on industrial and information systems (ICIIS2014) IEEE, Piscataway, New Jersey, 2014.

[19] Liu X, Chen S, Song W, "A design and implementation of watchdog based on observer pattern and finite state machine," In: Proceedings of the 10th IEEE International Conference on

[20] Reliability, Maintainability and Safety (ICRMS '14), pp 407–411, 2014.

[21] Patel MM, Aggarwal A, "Two phase wormhole detection approach for dynamic wireless sensor networks," In Proceedings of the IEEE international conference on wireless communications, signal processing and networking (WiSPNET '16) IEEE,Chennai, India, 2016.

[22] Su MY WARP, "A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks". Comput Secur, pp. 208–224, 2010.

[23] Aad and J.P. Hubaux, E.W. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks,"

[24] IEEE/ACM Transactions on Networking, vol.16, pp.791- 802, Aug.2008.

[25] Wazid, Mohammad & Katal, Avita & Goudar, R.H., "Cluster and super cluster based intrusion

detection and prevention techniques for JellyFish Reorder Attack," Proceedings of 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing. Pp. 435-440, 2012

[26] Wazid, M., Katal, A. Goudar, R. H., "Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack," in Proceedings of 2nd IEEE international conference on parallel, distributed and grid computing , pp. 435– 440, 2012.

[27] M. Kaur, M. Rani and A. Nayyar, "A novel defense mechanism via Genetic Algorithm for counterfeiting and combating Jelly Fish attack in Mobile Ad-Hoc Networks," 5th International Conference -Confluence The Next Generation Information Technology Summit (Confluence), Noida, pp.359-364, 2014.

[28] Jayasingh, Bipin & Swathi, "Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network," BVICAM's International Journal of Information Technology, 2010.

[29] Ramesh, A. &Suruliandi, "A Performance analysis of encryption algorithms for Information Security," pp. 840-844, 2013.

[30] S. K. A. and Abha Jadaun. "Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT", Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.

[31] Pratiksha Mishra and S. K. A. "Design & Performance Assessment of Energy Efficient Routing Protocol Using Improved LEACH", International Journal of Wireless Network Security, 2021, Vol-7, Issue-1, PP: 17-33.

[32] S. K. A., Prakash Dangi and Pratiksha Mishra. Design and Comparison of LEACH and Improved Centralized LEACH in Wireless Sensor Network. *IJRITCC* 2021, *9*, 34-39.

[33] S. K. A., M. K. M, and P. Singh "A Security Approach to Manage a Smart City's Image Data on Cloud," AI-Centric Smart City Ecosystems: Technologies, Design and Implementation (1st ed.), PP: 68-82, (2022). CRC Press. https://doi.org/10.1201/9781003252542.

[34] S. K. A. "A. Raj, V. Sharma, and V. Kumar."Simulation and Analysis of Hand Gesture Recognition for Indian Sign Language Using CNN"." *International Journal on Recent and Innovation Trends in Computing and Communication* 10, no. 4 (2022): 10-14.