Acquiring Data Packets Commencing Predator Spells in WSN

[1]Rajesh Khanna.M, [2]Dr.A.Rengarajan
[1]Ph.D Scholar, Department of Computer science and Engineering, St.Peter's University, Avadi, Chennai, India.
[2]Professor, Department of Computer science and Engineering, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India.

Abstract: **Wireless Sensor Network is a rising stage in the field of remote sensing, information accumulation, examination, amendment of the issue and research in different studies. The goal of this paper is to investigate asset exhaustion assaults at the directing convention layer, which forever debilitate organizes by rapidly emptying the hubs' battery power. These "PREDATOR" assaults are not particular to any particular convention, but instead depend on the properties of numerous prominent classes of directing conventions. In the most detrimental possibility, a solitary Predator can expand system wide vitality utilization by a component of O(n), where N in the quantity of system hubs. We examine techniques to alleviate these sorts of assaults, which limits the harm brought on by Predators amid the bundle sending stage.**

KEYWORDS— Denial of service, routing, ad-hoc networks, sensor networks, wireless networks, routing.

I. INTRODUCTION

Wireless remote sensor systems (Wsns) gives persistent network, [21] and in a split second deployable correspondence. Such systems are equipped for checking natural conditions, plant execution, and troop's arrangement. As Wsns get to be more critical to regular working of people and associations, high accessibility of these systems is a basic property and ought to capacity without disappointment much under pernicious conditions. Since their correspondence system is impromptu in nature, remote specially appointed systems are especially defenseless against foreswearing of administration (Dos) assaults [2], and a lot of examination has been carried out to [3] improve survivability. The most perpetual disavowal of administration assault is to completely exhaust hubs' batteries. This is an example of an [4] asset consumption assault, with battery control as the asset of investment. In this paper, we examine the [5] different predator assaults. These assaults are not the same as at one time examined dissent of administration [6] (Dos), lessening of value (Roq), and steering base assaults, predators don't upset prompt accessibility of system hubs, but instead work about whether to completely handicap a system. [7] Predator assaults are not convention particular, as they don't depend on configuration properties or usage deficiencies of specific directing conventions. These assaults don't depend on flooding the system with a lot of information, yet rather attempt to transmit as meager information as could be expected under the circumstances to accomplish the biggest vitality channel.

This paper makes three essential commitments. To begin with, a careful assessment of the current directing conventions towards battery exhaustion assaults is carried out. We watch that current secure steering conventions, for example, Ariadne [10], SAODV [8], and SEAD [9] don't ensure against Predator assaults. Existing deal with secure steering endeavors to guarantee that enemies can't cause way disclosure to give back an invalid system way, yet Predators don't upset or modify found ways, rather utilize existing legitimate system ways to do the assault. Conventions that expand power proficiency are additionally wrong, since they depend on helpful hub conduct and can't streamline battery power use. Second, reproduction results measuring the execution of a few agent conventions in the vicinity of a solitary Predator insider enemy is demonstrated. Third, alteration of a current sensor system directing convention is made to keep the harm brought on by Predator assaults amid bundle sending stage.

A.Classification

Foreswearing of administration is an assault, where a victimized person can utilize 10 minutes of the CPU time to transmit an information parcel, yet while a legitimate hub utilizes 1 moment of its CPU time to transmit the same information bundle. In multihop steering system: a source forms the most limited way and transmits the information parcel to the following jump, which transmits it further, until the end of the line is arrived at; devouring assets at the source hub as well as at each hub the bundle travels through. Predator assault might be characterized as an intentional activity of forming and transmitting a vindictive message that picks the longest way which expends more vitality of the system than if a legitimate hub transmits a message of indistinguishable size to the same goal. The quality of an assault could be measured by the proportion of system vitality utilized as a part of the genuine case to the vitality utilized within the noxious case.

B. Protocols and Assumptions

In this paper, we consider the impact of Predator assaults on Destination grouping separation vector steering conventions, and a sensible ID-based sensor system directing convention proposed by Parno et al. [11]. These conventions are prone to avoid Predator assaults, so the secured conventions are a

vital subset of our directing result space. We separate on-interest steering conventions, where topology revelation is carried out at transmission time, and static conventions, where topology is found amid an introductory stage, with occasional rediscovery to handle uncommon topology changes. The foes are malevolent insiders and have the same assets and level of system get to as legit hubs. Sending malevolent parcel consequently permits few Predators to assault numerous fair hubs. We will indicate later that a solitary Predator may assault each system hub at the same time, implying that predators are to be disengaged from the genuine hubs. Predator assaults may be debilitated by utilizing gatherings of hubs with stunned cycles: just dynamic obligation hubs are helpless while the Predator is dynamic; hubs are sheltered while the Predator rests

C.Overview

In the rest of this paper, we show an arrangement of progressively harming Predator assaults, assess the defenselessness of a few illustration conventions, and propose how to enhance adaptability. In source steering conventions, we indicate how a pernicious bundle source, can detail ways through the system, which are far more than ideal, therefore squandering vitality at middle hubs that forward the parcel as proposed by the source. In steering plans, where sending choices are made freely by every hub instead of detailed by the source, we recommend how directional receiving wire and wormhole assaults [12] could be utilized to convey bundles to various remote system positions, compelling bundle preparing at hubs that would not regularly get that parcel whatsoever, and consequently expanding system wide vitality consumption. In conclusion, we indicate how an enemy can target bundle sending as well as course and topology disclosure stages if revelation messages are overwhelmed, a foe can, for the expense of a solitary parcel, devour vitality at each hub in the system.

In our first assault, an enemy forms bundles with deliberately presented steering circles. We call it the merry go round assault, since it sends parcels in rings as demonstrated. It targets source steering conventions by abusing the constrained check of message headers at sending hubs, permitting a solitary parcel to over and over cross the same set of hubs. Results demonstrate that in an arbitrarily produced topology, a solitary aggressor can utilize a merry go round assault to expand vitality utilization by to the extent that a variable of 4. Concise notice of this assault might be found in other writing [13] however no instinct for safeguard or any assessment is given. In our second assault, likewise focusing on source steering, a foe builds falsely long courses, possibly navigating each hub in the system. We call this the stretch assault, since it builds bundle way lengths, creating parcels to be transformed by various hubs that is free of bounce tally along the most limited way between the foe and parcel terminus. A sample is delineated Stretch assaults expand vitality utilization by up to a request of extent, contingent upon the position of the malevolent hub. The effect of these assaults might be further expanded by consolidating them, expanding the quantity of ill-disposed hubs in the system, or essentially sending more bundles. Albeit in systems that don't utilize confirmation or just utilize end-to-end verification, enemies are allowed to supplant courses in any caught parcels.

We investigate various relief routines to bound the harm from Predator assaults, and find that while the merry go round assault is easy to avert with immaterial overhead, the stretch assault is much all the more difficult. The principal foundation for predator assault is detached source steering, where any sending hub can reroute the parcel in the event that it knows a shorter way to the objective. In this manner, we adjust the convention created by Parno et al [11] to ensure that it mitigates all said Predator assaults. The topology disclosure system and restricted hashing method [bp] is utilized for beginning security stages. A portrayal of how to alter the convention to catch Predator hubs amid the bundle sending stage and along these lines to disengage the antagonistic hubs from the system is proposed [22].

II. CORRELATED WORKS

An early specify of force weariness could be found in [68], as "lack of sleep torment." according to the name, the proposed assault keeps hubs from entering a slumber cycle, and consequently drains their batteries speedier. More current research on "foreswearing of-slumber" just considers assaults at the MAC layer [14]. Noxious cycles steering circles have been quickly said [11] however no powerful protections are examined other than expanding proficiency of the underlying MAC and directing conventions or exchanging far from source steering. Predators don't drop parcels; the nature of the noxious way itself may stay high. Other take a shot at disavowal of administration in specially appointed remote systems has fundamentally managed enemies who avert course setup, upset correspondence, or specially secure courses through themselves to drop, control, or screen bundles [9]. The impact of disavowal or debasement of administration on battery life and other limited hub assets has not by and large been a security attention. Conventions that characterize [10] security regarding way disclosure achievement, guaranteeing that just legitimate system ways are found, can't ensure against Predator assaults, since Predators don't [15] utilize or return unlawful courses or counteract correspondence in the short term. Current work in insignificant vitality steering, which plans to build the lifetime of force compelled systems by utilizing less vitality to transmit and get packets[16] . Nonetheless, Predators will build vitality utilization even in negligible vitality steering situations. Aggressors will deliver bundles which navigate a bigger number of bounces than should be expected, so regardless of the fact that hubs use the base obliged vitality to transmit parcels, every parcel is still more lavish to transmit [17] in the vicinity of Predators. Our work might be considered assault safe insignificant vitality steering, where the foe's objective is to [18] diminish vitality reserve funds.

III. ATTACKS ON STATELESS PROTOCOLS

In these frameworks, the source hub determines the whole course to an objective inside the parcel header, so transitional hubs depend on the course detailed by the source. [19] The trouble is on the source to guarantee that the course is legitimate at the time of sending the

information bundle, and that each hub in the course is a physical neighbor of the past course bounce. This methodology has the preference that moderate hubs have less troubles while sending the information bundles towards the goal, furthermore takes into account whole courses to be sender validated utilizing computerized marks, as in Ariadne [10]. We assessed both the merry go round and stretch assaults in an arbitrarily created 30-hub topology and a solitary haphazardly chose noxious DSR executor, utilizing the ns-2 system test system [21]. Vitality utilization is measured for the base number of bundles needed to convey a solitary message. We autonomously processed asset use of fair and pernicious hubs and found that malevolent hubs did not utilize an equivalent measure of vitality as the genuine hubs while doing the assault.

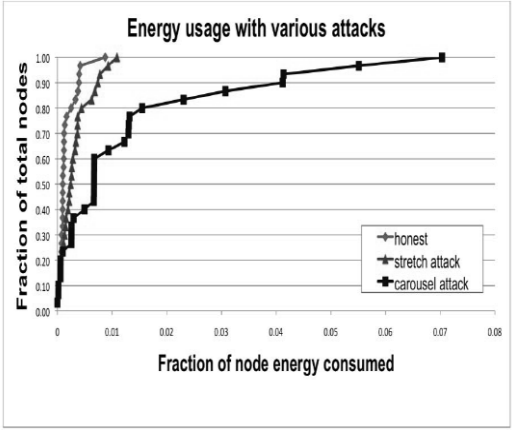

Fig 2. Results of a single malicious packet sent by the attacker is evaluated under both attacks is shown [22].

Obviously, the merry go round assault causes intemperate vitality utilization for a couple of hubs, since just hubs along a shorter way are influenced. Conversely, the stretch assault demonstrates more uniform vitality utilization for all hubs in the system, since it protracts the course, bringing on more hubs to process the bundle. While both assaults fundamentally utilize system vitality unnecessarily, singular hubs are influenced, by losing just about 10 percent of their aggregate vitality for every message. Fig. 3a outlines the vitality use when hub 0 sends a solitary bundle to hub 19 in an illustration system topology with just fair hubs. Dark bolts signify the way of the parcel.

A. Carousel attack

In this assault, a foe sends a parcel with a pernicious course made as an arrangement out of circles, such that the same hub shows up in the course ordinarily. This technique might be utilized to build the course length past the quantity of hubs in the system, just constrained by the quantity of permitted entrances in the source course. A case of this kind of course. In Fig. 3b, malignant hub 0 completes a merry go round assault, sending a solitary message to hub 19. The exceptional increment in vitality use along the first way is indicated. The hypothetical furthest reaches of this assault is the vitality use increment by an element of O(n), where N is the most extreme course length.

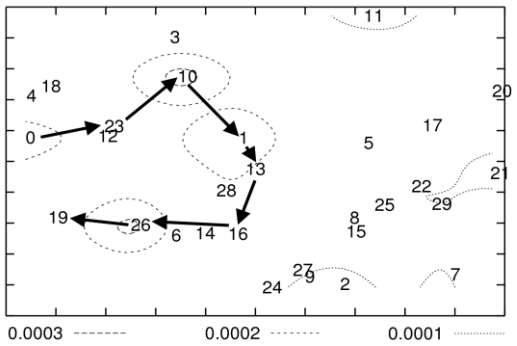

Fig.3a. : Honest Scenario: Node 0 Sends A Single Message To Node 19 [22]

General vitality utilization increments by up to a variable of 3.96 for every message. Generally speaking, an arbitrarily found merry go round assailant in our case topology can build system vitality utilization by an element of 1.48 +_ 0.99. The explanation behind this huge standard deviation is that the assault does not generally build vitality utilization the length of the antagonistic way is a different of the legit way, which is thus, influenced by the position of the enemy in connection to the terminus, so the foe's position is essential to the accomplishment of this assault.

B. Stretch Assault

An alternate assault in the same vein is the stretch assault, where a pernicious hub develops falsely long source courses, creating parcels to navigate a bigger number of hubs than picking an ideal way. A fair source would choose the course Sourcefesink, influencing four hubs including it, however the malignant hub chooses a more extended course, influencing all hubs in the system. These courses energy hubs that don't lie along the legitimate course to cast out vitality by sending malevolent parcels.

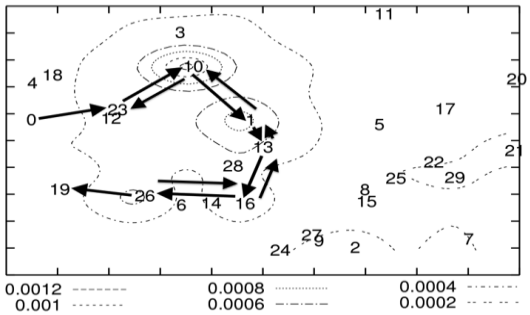

Fig 3b. Caption Missing [22]

A case of this kind of course. The conclusion gets to be clearer when we inspect Fig. 3c and contrast with the merry go round assault. While the merry go round assault utilizes vitality at the hubs that were at that point in the legitimate way; however the stretch assault amplifies the steering way to a more extensive segment of the system, and expends vitality from bigger number of nodes.

The hypothetical furthest reaches of the stretch assault is a bundle that navigates each system hub, creating a vitality utilization increment by a variable of O (min(n, lamda)), where N is the quantity of hubs in the system and lamda is the most extreme way length permitted. This assault is

possibly less harming for every bundle than the merry go round assault, as the quantity of bounces for every parcel is limited by the quantity of system hubs. In any case, foes can join merry go round and stretch assaults to keep the bundles inside the system longer time of time. Accordingly, extend assault and directing circle issues ought to be located and uprooted to keep the joined assault.

In our sample topology, we see an increment in vitality utilization by to the extent that a variable of 10.5 for every message over the legitimate situation, with a normal increment in vitality utilization of 2.67 +_ 2.49. Likewise with the merry go round assault, the purpose behind the vast standard deviation is that the position of the ill-disposed hub influences the quality of the assault. Anyway, the stretch assault can attain the same adequacy and does not rely on upon the assailant's system position in respect to the objective.

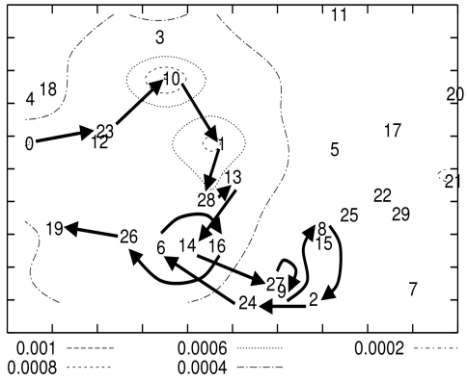

Fig.3c. caption missing [22]

C. Mitigation Methods

The carousel attack might be forestalled totally by having, sending hubs to check the source courses for circles. At the point when a circle is identified, it is better to just drop the parcel, particularly considering that the sending hub is likely malignant (legitimate hubs ought not present circles). The stretch assault is additionally difficult to forestall. Its achievement rests on the sending hub not checking for optimality of the course, yet essentially takes after the course precisely as tagged in the header, this assault might be anticipated by utilizing detached source directing, where middle of the road hubs may supplant part or the majority of the course in the parcel header in the event that they know of a superior course to the objective.

IV ATTACKS ON STATEFUL PROTOCOLS

Two critical classes of stateful conventions are connection state and separation vector steering conventions. In connection state and separation vector system hubs are mindful of the system topology, state and settle on autonomous sending choices, so enemies have restricted force to influence parcel sending, making these conventions invulnerable to merry go round and stretch assaults. Anyway these conventions devour overabundance vitality control as contrasted and the stateless conventions, since each hub in the system as often as possible redesigns its steering table to stay informed concerning the system hubs.

A. Directional Reception Apparatus Assault

Utilizing directional reception apparatus enemies can store a parcel in discretionary parts of the system, while likewise sending the bundle by regional standards. This devours the vitality of hubs that would not have needed to process the first bundle, with the normal extra legit vitality use of O (d), where d is the system measurement. This assault could be viewed as a half-wormhole assault [12], since a directional radio wire constitutes a private correspondence channel, yet the hub on the flip side is not so much pernicious. It could be performed more than once, saving the bundle at different inaccessible focuses in the system, at the extra cost to the enemy for each one utilization of the directional radio wire.

B. Malevolent Disclosure Assault

An alternate assault on all at one time specified directing conventions (counting stateful and stateless) is spurious course disclosure. A noxious hub has various approaches to affect an apparent topology transform: it might essentially dishonestly guarantee that a connection is down, or claim another connection to a nonexistent hub. Two chipping in malignant hubs may guarantee the connection between them is down. On the other hand, close-by hubs may have the capacity to screen correspondence to locate join disappointment. A solitary hub can imitate various hubs in neighbor connections [20], or erroneously guarantee hubs as neighbor's countermeasure is to utilize confirmation. To do this, two participating enemies conveying through a wormhole could over and over affirm and withdraw courses that utilize this wormhole, bringing on a hypothetical vitality use increment of an element of O (N) for every parcel.

C. Arrange and Signal Based Conventions

These conventions likewise succumb to directional receiving wire assaults in the same path as connection state and separation vector conventions.

V M-DSDV NETWORK ROUTING

In this segment, we demonstrate that end of the line arrangement removed vector a proactive system steering convention [DSDV] could be altered to provably oppose Predator assaults amid the bundle sending stage. Since the first form of the convention is proactive, and albeit intended to overcome steering circle issue, is powerless against Predator assaults. M-DSDV comprises of a topology revelation stage, took after by a topology support stage. Authentic system hub has an one of a kind endorsement of participation, which incorporates its open key and code word doled out by a trusted disconnected from the net power before system arrangement.

A. Topology Revelation

Disclosure of the neighboring hubs starts, when there is a need to transmit the information bundle. Every hub has a restricted perspective of the system the hub knows just itself. Hubs utilize the neighborhood TV plan to find their neighbors, where the declaration character confirmation is carried out to segregate the outer unapproved hubs from the system. Consequently, every fair hub takes in its dynamic neighbor hub's location and open key.

At the point when a source S, which needs to send an information parcel to end D, first builds and shows a course ask for bundle comprising of source location, terminus location, grouping number, next jump, metric, record number and time to live fields. The source location and end of the line location are the web convention addresses, the succession number is utilized to separate new courses from stale courses, the following jump and metric is a neighborhood counter kept up independently by every hub and increased each one time a Rreq is telecasted, the file number is introduced to zero, is utilized to stay informed regarding the circles the bundle has set aside a few minutes to live field is utilized as a clock which increases at whatever point a Rreq parcel is sent.

On receipt of Rreq, moderate hubs investigate it to check whether it is a copy, in which case it is rejected. If not the source address, next bounce, metric pair is entered into the nearby history table. The terminus location is turned toward the directing table, if a new course to it is known a Rrep a course answer bundle is sent once more to S. If not, it increases the list number and rebroadcasts the Rreq. This additionally makes a retrograde course towards S and exists has an advancement strategy. At the point when objective gets Rreq, it sends back a Rrep bundle to the hub from which it got the first Rreq parcel. The organization of the course answer bundle incorporates source address, terminus address, objective grouping, list number, life time. Here, the source address, goal address and record number are replicated from the approaching Rreq bundle; however the terminus grouping number is taken from its counter in memory. The life time field demonstrates to what extent the course is legitimate. On receipt of Rrep, transitional hubs on the path back, examine the bundle to checks the whether the arrangement number is more prominent than the worth in the directing table and contrasts the metric quality and the file number, whether the list number is littler than the metric check. Thusly, all hubs on the converse course make a retrogressive course towards S. Middle of the road hubs that got the first Rreq bundle however were not on the converse way dispose of the opposite course table entrance when the related clock lapses.

B. Topology Support Stage

At the point when the following jump connect in the directing table passage breaks, all dynamic neighbors are educated by method for RERR bundles which overhauls the succession number. RERR bundles are additionally produced when a hub X is not able to forward bundle P from hub S to hub on connection (X, Y). The augmented grouping number N is incorporated in the RERR. At the point when hub S gets the RERR, it launchs another course disclosure for D utilizing the arrangement number that is at any rate as vast as N.

C. M-DSDV In The Vicinity Of Predators

In the vicinity of predators, merry go round assault and stretch assault could be forestalled by utilizing the list number. If there should be an occurrence of, merry go round assault, where a bundle which crossed through the most brief way of the system, returns back again to the same hub, that could be killed by checking the file number put away on the parcel header and the record number put away in the nearby steering table of the hub.

We can keep the stretch assault by freely scouting the bundle advance: the hubs stay informed concerning course "metric" and, when acknowledgement returns back, the course metric worth and the file number, which demonstrates the bounce tally might be checked. In the event that the record worth is more prominent than the metric esteem the source infers that the stretch assault as happened. Therefore, if pernicious mediation has been suspected the parcel is dropped from further sending system. Subsequently, the harm from an assailant is limited as a capacity of system size.

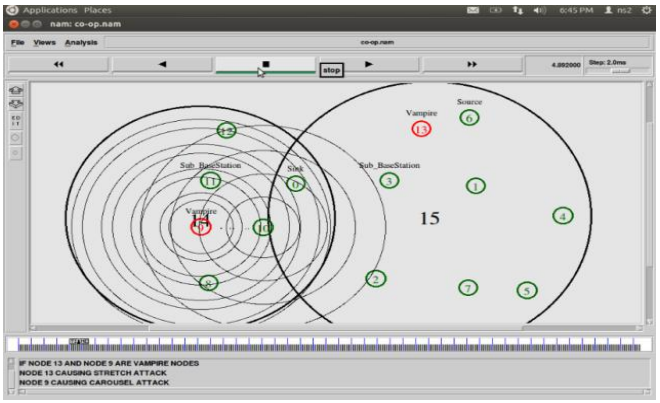

Fig 6a. Node 9 causing Carousel attack

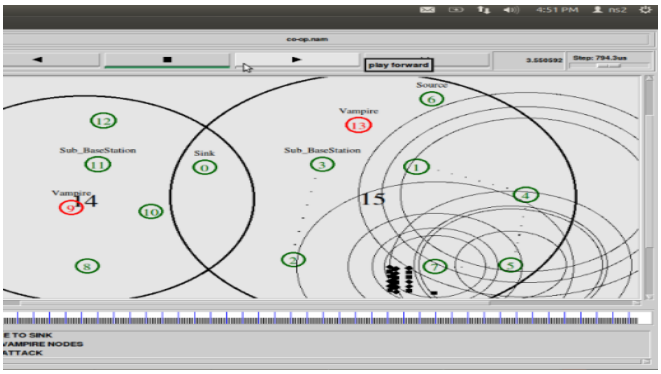

Fig 6b. Node 13 causing stretch attack

We assessed the merry go round assault, stretch assault and the ideal way for the hubs in an arbitrarily produced 14-hub topology and two haphazardly chose noxious DSR operator, utilizing the ns-2 system test system [1]. Vitality utilization is measured with the base number of bundles needed to convey a solitary message.

Fig.6c. Optimal path from Source to Sink

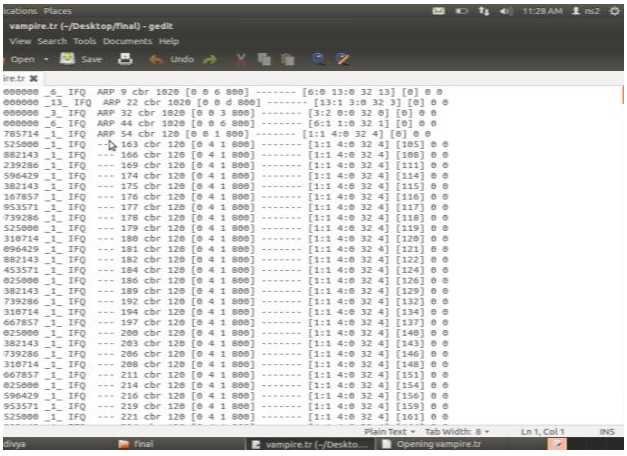

Fig 6d. Measurement of energy usage for the nodes with the minimum number of packets required to deliver a single message

We freely processed asset use of fair and pernicious hubs and found that vindictive hubs did not utilize an equivalent measure of vitality as the legit hubs while doing the assault. According to the dissection, a solitary assailant can utilize a Carousel assault to build vitality utilization by to the extent that an element of 4. Additionally, the Stretch assault builds the vitality utilization by up to a request of greatness, contingent upon the position of the vindictive hub. The effect of these assaults might be further expanded by joining them, expanding the quantity of antagonistic hubs in the system, or basically sending more bundles.

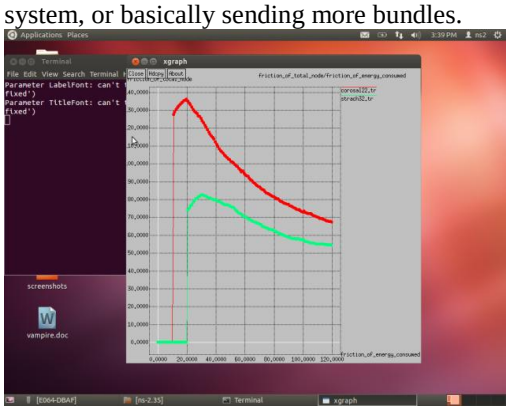

Fig.6e. Carousel attack Vs. Stretch Attack

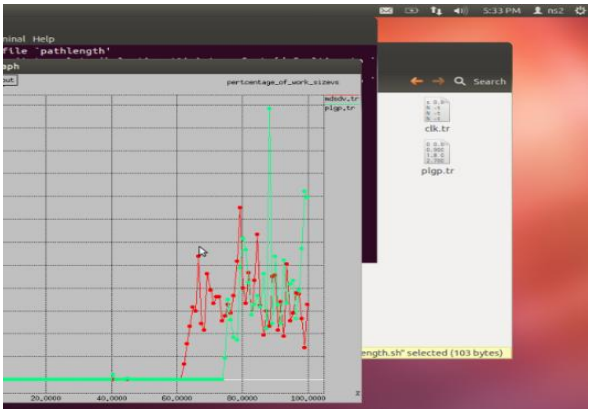

Fig.6f. PLGP Vs. M-DSDV

VII CONCLUSION

In this paper, we characterized Predator assaults, another class of asset utilization assaults that utilize directing conventions to forever impair impromptu remote sensor organizes by exhausting hubs' battery power. These assaults don't rely on upon specific conventions or executions, yet rather uncover vulnerabilities in various prevalent convention classes. We demonstrated various confirmation of-idea assaults against delegate samples of existing directing conventions utilizing a little number of feeble foes, and measured their assault accomplishment on a haphazardly produced topology of 30 hubs. Reproduction results demonstrate that relying upon the area of the enemy, system vitality consumption amid the sending stage increments. Hypothetical most pessimistic scenario vitality use can increment by to the extent that an element of O (n) for every enemy for every parcel, where N is the system size. We proposed guards against a percentage of the sending stage assaults and depicted M-DSDV, the limits harm brought about from Predator assaults by checking the bundle history reliably, which makes advance to their objectives.

REFERENCES

1. "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns,2012.
2. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
3. I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
4. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
5. J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
6. J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29,no. 2, pp. 216-230, 2006.
7. A. Nasipuri and S.R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Networks," Proc. Int'l Conf. Computer Comm. And Networks, 1999.
8. M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security (WiSE),2002.
9. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.

10. Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.
11. B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.
12. Y.-C. Hu, D.B. Johnson, and A. Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc.IEEE INFOCOM, 2003.
13. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
14. D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.
15. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.
16. J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12,no. 4, pp. 609-619, Aug. 2004.
17. S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev.,vol. 6, no. 3, pp. 50-66, 2002.
18. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks,"Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.
19. V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp. 1333-1344, Aug. 1999.
20. J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.
21. International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014 Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14) by author Mr.M.Rajesh Khanna 2014.
22. Predator attacks: Draining life from wireless ad-hoc sensor networks by Eugene Y. Vasserman from Kansas State University.