Security Risks in Wireless Sensor Networks: Analyzing the Malicious Jellyfish Node Threat

Dr. Sarah Johnson
School of Computer Science, University of Toronto, Toronto, Canada

ABSTRACT

Custom remote control systems comprise of self-guided, self-guided hubs with zero structure. Along these lines, specifically equipped systems possess a powerful topology therefore the hubs can without very much of an extend sign up for or keep the program whenever. They possess many potential applications, especially in armed forces and repair areas, for example, interfacing troopers on the entrance series or producing another program rather than a program that crumbled after a calamity like the seismic tremor. Tweaked systems are acceptable for specific zones where a set base cannot be built up. Since hubs speak with one another without a fundamental foundation, they give availability by sending bundles over themselves. To help this association, the hubs utilize certain directing conventions, for example, AODV, DSR, and DSDV. Other than filling in as a host, every hub additionally goes about as a switch to find a way and divert bundles to the right hub in the system.

Keyword: *Wireless Ad Hoc Network, AODV, Jelly Fish, MATLA*

I. INTRODUCTION

As remote specially appointed systems come up short on a foundation, they are presented to a ton of assaults. One of these assaults is definitely the JellyFish assault. In the JellyFish assault, a pernicious hub ingests all information bundles in itself, like an opening which sucks in everything in. Along these lines, all bundles in the system are decreased. A pernicious hub shedding all the traffic in the system utilizes the vulnerabilities of the course disclosure bundles of the on interest conventions, for example, AODV. In course disclosure process of AODV conference, transitional hubs are capable to locate a fresh way to the goal, sending revelation bundles to the neighbor hubs. Vindictive hubs don't use this process and rather, they quickly react to the resource hub with false data as if it offers new plenty of way to the goal. Along these lines resource hub sends its info parcels by means of the malevolent hub to the goal anticipating it is definitely an authentic method. JellyFish strike may happen because of a vindictive centre which can be intentionally obtaining into mischief, simply as an injured hub user interface.

Irrespective, hubs in the program will continuously attempt to discover a program for the objective, which causes the centre to devour its electric battery notwithstanding shedding parcels.

1.1 Cellular Networks

Remote control correspondence is certainly used to move information among customers without a born framework. Making use of electromagnetic ocean, portable customers transmit and obtain details over the surroundings. Remote messages advances from house RF to satellites, from PDAs to walkie-talkies. Its versatility, effortlessness and price sparing restaurant factors of curiosity

make the remote correspondence progressively prominent, particularly in late decades Raising client versatility desires and improvements in the utilization of smart telephones PDA's is one of the principle factors of the ubiquity of remote systems.

II. LITERATURE SURVEY

[1] Sureka.D, Prof. T. Chandra Sekaran suggested asset tiredness approaches at the steerage convention level, which permanently cripple arranges by quickly depleting hubs' electric battery control. These "Vampire" approaches are not really direct to a particular lifestyle, yet rather rely on the properties of numerous famous classes of steering conventions. We talk about strategies to alleviate these kinds of assaults, including another confirmation of-idea convention that provably limits the harm brought about by Vampires during the parcel sending stage. The remote Adhoc sensor organize and directing information in them is vulnumarable to specific assaults. So we should guarantee a guarded and confirmed information transmission process. There are a great deal of conventions created to safeguard from DOS assault, yet it isn't totally conceivable. One such DOS assault is usually Vampire attack emptying of hub life out of remote adhoc sensor systems. Adhoc remote sensor systems (WSNs) assurance

energizing new applications sooner rather than later, for example, pervasive on-request signing up power, ceaseless network, and in a break up second deployable communication for armed service and people on call. Such systems as of right now screen natural conditions, processing plant performance, and troop business, to give some good examples applications.

[2] Harsha.In, Rashmi.H proposed a way to deal with distinguish and counteract the vampire attack in MANET. Impromptu low-control remote systems are the most motivating exploration proceeding in discovering and inevitable processing. Earlier security function around there offers concentrated essentially on disavowal of administration at the guiding or moderate gain access to control Figures. Prior, the asset usage approaches are seen as simply as a leading concern, all around as of past due these are purchased in to another gathering known as "vampire approaches". Vampire approaches are not really convention precise, in that they don't rely on strategy properties or utilization imperfections of particular leading conventions, but rather undertaking general properties of meeting classes, for example, user interface state, break up vector, supply guiding, and geographic and sign guiding .It is specific that all analyzed conventions are vulnerable to Vampire approaches, which are annihilating, hard to distinguish, and are anything but difficult to carry out utilizing seeing that few seeing that one particular malevolent insider mailing just lifestyle agreeable text messages. In the most depressed situation, an one Vampire can build organize wide energy usage by an aspect of O (D), where D in the volume of program hubs.

[3] SumitAgrawal, ShilpaJaiswal proposed a Protected Ad-hoc On-Demand Length Vector leading convention (SAODV) to try our everything interests into an usual spot. So the accentuation is to build up a plan for the proportion of these system worms and blackhole assaults to take out events of correspondence risks from middle of the road and encompassing strings. the full investigation to dispense with string of dark gap assaults in MANET". We additionally address to the arrangement against the danger of dark gap assault in MANET. In Black Hole Attack a vindictive hub promotes itself as having the most limited way to the hub whose bundles it needs to block. So to redress the likelihood of event of dark opening attack we are proposing a process to identify attack and an solution for find a sheltered course for secure transmission. The need of remote system is definitely to implement taking an interest hubs to advance bundles to different hubs to cultivate secure and solid communication. In spite of the truth that there are nearness of defenseless hubs that can become related with pernicious hubs and can damage systems. The assortments of these noxious hubs are powerless against hubs which are either bargained or dishonestly led by weak hubs.

Vindictive hubs can without much of a stretch alter the taking an interest hubs in the systems. In portable specially appointed system these assaults proven their noteworthiness in the conditions of program earthworms which can strike, modify or change the basic symbolism of program over all managerial and acquiring an curiosity spaces.

[4] Saritha Reddy Venna1, Ramesh BabuInampudi proposed vulnerabilities and different types of protection assaults in MANETs The ongoing and quick progressions in the innovation and the particular highlights of MANETs possess used MANETs increasingly common. With the regularly growing applications, the shortcoming of these systems against an collection of approaches offers been revealed. MANETs doesn't possess very clear and proficient elements to understand or anticipate the approaches, so enemy centre can without very much of an extend hinder and obliterate the whole system or may suppose responsibility for the data getting sent in the program. Assailants present different kinds of approaches and each invasion provides its extremely very own level of impact on the program. Security is normally a remarkable get worried in MANETs in watch of its organic vulnerabilities. Every flexible centre can function either as a web host or as a switch. There is no need of fixed framework and these portable hubs arrange themselves in a discretionary manner to shape a transitory system with powerfully evolving topology. Hubs inside one another's remote transmission extents can convey straightforwardly however hubs outside one another's rangehave to rely upon neighboring hubs to transfer communications.

[5] GuozhuMeng, Yang Liu, Jie Zhang, Alexander Pokluda, RaoufBoutaba proposed various instruments of cooperation and guard in shared security. We deliberately examine numerous utilize instances of synergistic security by covering six types of security frameworks. Parts of these frameworks are completely contemplated, including their improvements, steps, systems, qualities and weaknesses.We then present a much reaching study regarding their exam target, practicality of investigation, design, organize foundation, activity, shared data and interoperability. We feature five significant styles in community oriented security, and distinguish troubles and potential bearings for long term study. Our work contributes the accompanying to the current study on synergistic security with the intent of producing communitarian protection frameworks more powerful and effective.

Security can be in many instances midway overseen. An optional design of making use of cooperation therefore as to improve protection has selected up energy in the program of latest years. Synergistic protection is an exclusive idea that applies to a wide collection of frameworks, and offers been used to fathom protection issues inbuilt in distributed conditions. Therefore significantly, joint work offers been used in several areas, for example, disruption area, spam going, botnet blockage, and powerlessness reputation.

III. PROBLEM FORMULATION

At initial, we should consider Ad-hoc On-Demand Length Vector (AODV) Routing Process and after that we will clarify JellyFish Strike.

3.1. Ad-hoc On Demand Distance Vector (AODV) Routing Protocol

Specifically appointed On-Demand Length Vector (AODV) Routing Protocol is utilized for finding a way to the goal in an impromptu system. To discover the method to the objective every one portable centre function in involvement making use of the guiding control text messages. On accounts of these control text messages, AODV Redirecting Protocol presents speedy modification to powerful system circumstances, low managing and storage over head, low program band width usage with little size control messages. The most distinctive element of AODV contrasted with the other steering conventions is usually that it utilizes a goal arrangement number for each course passage. The goal succession number is usually produced by the goal when an association is usually pointed out from it. Utilizing the goal grouping number guarantees circle opportunity. AODV ensures the course to the goal does not contain a circle and is usually the most brief way. Course Requests (RREQs), Route Replay (RREPs), Path Mistakes (RERRs) are controlmessages used for establishing up a method to the objective, sent making use of UDP/IP conventions. Header data of these control communications are clarified in [13].

At the stage when the source hub needs to make an association with the goal hub, it communicate a RREQ note. This RREQ message can be pass on from the resource, received by neighbours (middle of the street hubs) of the supply centre.

The halfway hubs communicate the RREQ message to their neighbours. This method will go on until the package is received by objective centre or a middle centre that provides a brand-new enough training course section for the objective. Figure underneath displays how the RREQ message is normally pass on in an impromptu program.

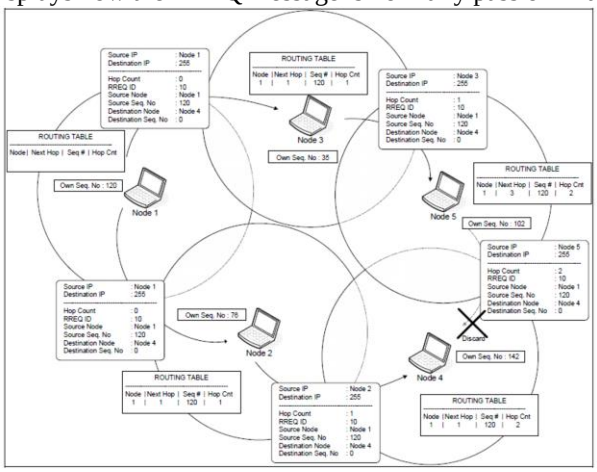

Fig 3.1 - Propagation of the RREQ message

Crisp enough implies that the middle of the street hub has a reputable training course to objective designed a timeframe back, lower than the edge. While the RREQ parcel goes through the system, each halfway hub builds the bounce check by one. In the event that a RREQ message with the equivalent RREQ ID is gotten, the hub quietly disposes of the recently got RREQs, controlling the ID field of the RREQ message. At the point when the goal hub or moderate hub that has crisp enough course to the goal get the RREQ message they make a RREP message and upgrade their directing furniture with aggregated jump tally and the set up quantity of the goal hub.

A while later on the RREP message is unicasted to the resource hub. The contrast between the phone system a RREQ and unicasting RREP can become seen from Numbers 9 and 10. While the RREQ and the RREP communications are sent by middle of the road hubs, halfway hubs upgrade their steerage desks and extra this training course section for 3 secs, which is normally the Energetic_Path_TIMEOUT constant appraisal of AODV lifestyle. The default continuous estimations of the AODV lifestyle are documented. In this method the centre understands over which neighbors to reach at the objective. In phrasing, the neighbors list for objective is ski slopes as "Forerunner List". Fig 3.1 displays how the RREP message is unicasted and how the training course areas in the middle of the street hubs are refreshed.

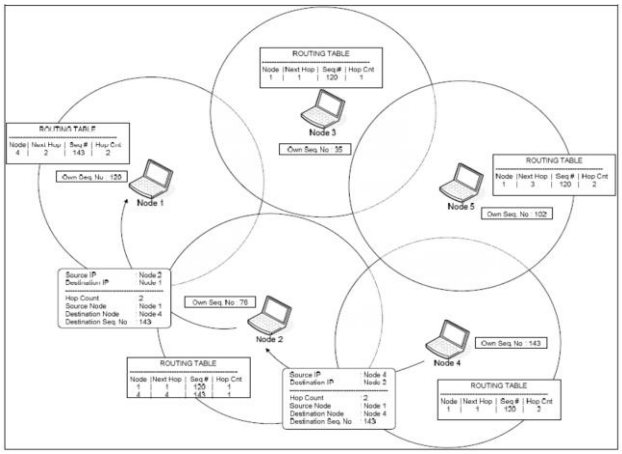

Fig 3.2 - Unicasting the RREP message

3.2. Sequence Numbers

Grouping Quantities fill up in as period stamps and allow hubs to appear at how crisp their data on the other hub is normally. In any case when a centre transmits any kind of steerage control message, RREQ, RREP, RERR and therefore on., it expands it is very very own grouping number. Higher succession number is increasingly exact data and whichever hub sends the most astounding grouping number, its data is considered and course is built up over this hub by different hubs.

The grouping number is a 32-bit unsigned whole number worth (i.e., 4294967295). In the event that the arrangement number of the hub achieves the conceivable most elevated succession number, 4294967295, at that point it will be reset to zero (0). In the event that the aftereffects of subtraction of the right now put away grouping number in a hub and the succession number of approaching AODV course control message is usually under zero, the put away arrangement number is usually changed with the succession number of the approaching control message.

In Fig 3.1, while Node 2 improvements the RREP message originating from Node 3, it appears in its very personal recently place away sequence quantity with that of Node 3. On the off opportunity that it views that the sequence number can be even more up to day than its personal, at that stage it adjustments its program desk section as essential.

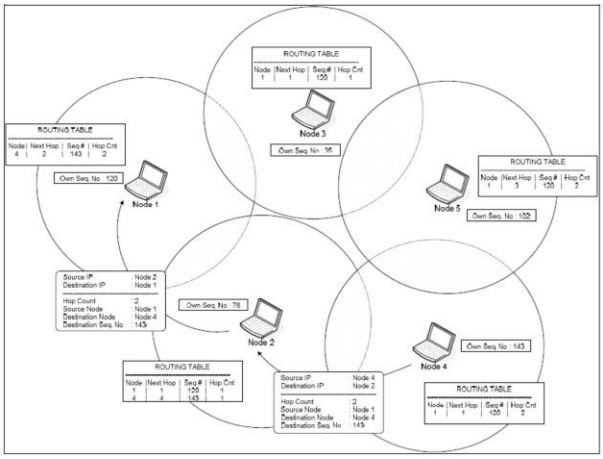

Fig 3.3 - Updating the String Number with fresh one

3.3. JellyFish Assault

JellyFish Assault is certainly quickly clarified in the previous Section. In this Section we will clarify it in even more fine detail as we possess simply clarified the AODV tradition. In an impromptu program that uses the AODV tradition, a JellyFishcentre ingests the program visitors and drops all packages. To clarify the JellyFish Assault we included a malignant centre that shows JellyFish carry out in the circumstance of the statistics of the previous area.

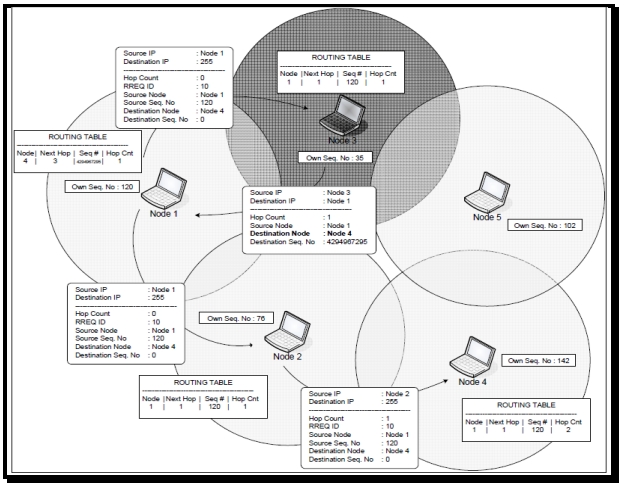

Fig 3.4-Representation of JellyFish Strike

In this situation appeared in Figure 3.4, we expect that Node 3 is the pernicious centre. At the point when Node 1 communicates the RREQ message for Node 4, Node 3 promptly reacts to Node 1 with a

RREP message that incorporates the most elevated grouping number of Node 4, as though it is originating from Node 4. Hub 1 expect that Node 4 is behind Node 3 with 1 bounce and disposes of the recently got RREP package originate from Node 2. A short time later Node 1 begins to convey its information parcel to the hub 3 believing that these bundles will achieve Node 4 yet Node 3 will drop all information bundles. In a JellyFish Attack, sooner or later, the sending hub comprehends that there is usually a connection blunder in light of the fact that the taking hub does not send TCP ACK bundles. In the event that it conveys new TCP info bundles and finds another program for the goal, the pernicious hub still numbers out how to mislead the sending hub. In the event that the sending hub conveys UDP info parcels the concern isn't determined in light of the truth that the UDP info organizations don't sit down limited for the ACK packets.In our situations we use UDP information packages and we will clarify our situations and their outcomes below.Before we will portray how JellyFish conduct is executed in the test system program, MATLAB-13.

IV. METHODOLOGY

In this function, we have attempted to assess the impacts of the JellyFish assaults in the remote control Ad-hoc Networks. To accomplish this we possess recreated the remote specifically appointed program circumstances which includes Jellyfish centre making use of MATLAB-13[14] plan. To recreate the JellyFishcentre in a remote control impromptu program we possess actualized another meeting that drops details parcels in the wake up of tugging in them to itself. In this section we present MATLAB-13and our dedication to this item.

4.1. MATLAB-13

MATLAB-13 is an event driven MATLAB-13 plan, created in the School of California Berkley, which incorporates many program products, for example, conventions, applications and visitors source carry out. The MATLAB-13 is normally a piece of encoding of the VINT opportunity [15] that is definitely bolstered by DARPA since 1995.

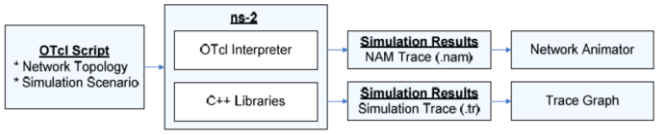

Fig 4.1 - MATLAB-13 pattern

At the reproduction coating MATLAB-13 utilizes OTcl (Object situated Tool Command Language) programming language to translate client reenactment contents. OTcl language is certainly in assurance an article arranged growth of the Tcl Language. The Tcl language is completely good with the C++ encoding language. At the top coating, MATLAB-13 is definitely a translator of Tcl material of the clients, they cooperate with C++ rules. In Section 5 the use of the Tcl Language will become clarified in fine detail.

While appeared in Number 4.1, an OTcl content material composed by a client is translated by MATLAB-13. While OTcl content material is becoming deciphered, MATLAB-13 makes two fundamental investigation reports at the same time. One of them is definitely NAM (Network Animator) object that demonstrates the visual liveliness of the reproduction. The additional is definitely the adhere to object that comprises of the ehavior of all items in the reenactment. Them two are made as a document by MATLAB-13. Earlier is definitely .nam record utilized by NAM programming that ties MATLAB-13. Last can be a ".tr" record that incorporates almost all duplication follows in the content material organization.

MATLAB-13 task is definitely regularly disseminated alongside different bundles (MATLAB-13, nam, tcl, otcl and so forth.) called as "across the panel package deal", nevertheless they can likewise become found out and downloaded individually. In this analysis we possess utilized performance 2.29 of MATLAB-13 across the board package deal and introduced the package deal in the Home windows condition utilizing Cygwin. After version 2, MATLAB-13it normally making use of a MATLAB-13 and in our theory we layer allude to it as MATLAB-13. We possess constructed the ".tcl" records in content material tool and shattered straight down the aftereffects of the ".tr" record using"cat", "awk", and "wc" and "grep" directions of Unix Operating System.

4.2 Simulation OF JellyFish attack and its effects

We clarified JellyFish Strike in AODV Routing Process and in Part 4 we depicted how this invasion is executed into the MATLAB-13. In this Part, initial, we will quickly disclose the Tcl Vocabulary to comprehend the duplication circumstances.

Having indicated how we attempted the JellyFish setup, we will screen the reproductions of JellyFish Strike to display its belongings. At that stage we will assess the has an effect on of JellyFish Strike in an Ad-Hoc Systems.

V. RESULTS

5.1 Implementation practice under MATLAB Taking into consideration AODV, DSR and DSDV Modification:

The idea of remote system is that any hub can join unreservedly the system and can keep it. Hubs which want to assault join the system. The noxious hub then later endeavors the abnormalities in the system among the hubs. It partakes in the transmission procedure and later on some stage dispatches the message adjustment assault

Pantomime: In remote systems a hub is allowed to move all through the system. There is usually no safe validation process so as to make the system secure from noxious hubs. The assailant use MAC and IP ridiculing so as to get personality of another hub and cover up into the system. This sort of attack is normally called parodying attack.

Man in middle Attack: An aggressor destinations between the sender and recipient and sniffs any data being sent between two hubs. Now and again, assailant may imitate the sender to speak with beneficiary or mimic the recipient to solution to the sender. Particular Forwarding: In such assaults, noxious hubs may decline to advance certain bundles and just drop them, ensuring that they are not really engendered any additional. A enemy won't, in any case, drop each bunch. To abstain from increasing uncertainties, the enemy rather particularly drops packages beginning from a few of selected hubs and advancements the rest of the Visitors .

Fake Node: A fake hub includes the expansion of a hub by a foe and causes the infusion of poisonous information. An interloper may add a centre to the system that bottles false.

Passive Traffic Monitoring: It can easily be made to acknowledge the correspondence gatherings and usefulness which could provide data to dispatch additional assaults.

Spying: The term listens in suggests catching without using any using any additional exercise.

In this recording and checking out and debate of message by unintentional collector take place. Versatile web host in portable specifically appointed program stocks a remote control medium. Principal parts of remote control correspondence make use of RF range and communicated essentially. Message sent can end up being took in stealthily and fake message can end up being infused into program.

Traffic Evaluation: Visitors evaluation is a latent invasion used to find up data on which hubs speak with one another and how much information is handled.

Syn flooding: This assault is forswearing of administration assault. An aggressor may more than once make new association demand until the property required by every association are depleted or accomplish a best breaking point. It produces extreme asset imperatives for actual hubs.

The organization of sensor hubs in an unattended situation makes the systems powerless. Remote sensor systems are gradually being utilized in military, ecological, wellbeing and business applications. In this theory, we have examined security assaults its essential and powerlessness for handling and gathering the data in WSN and exhibited the security target that should become accomplished.

5.2. Integrated Proposed Model

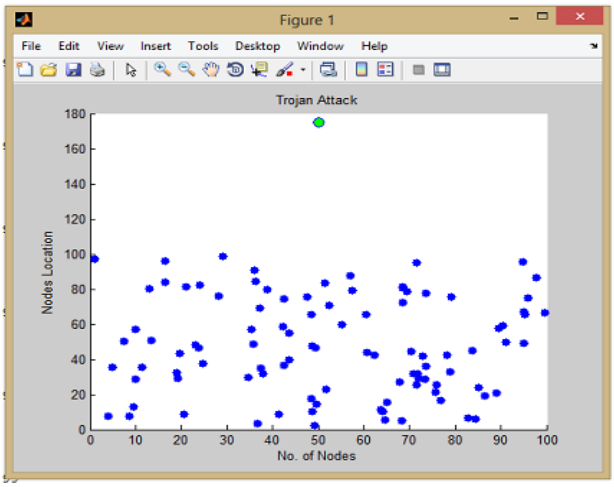

Fig 5.1 - No. of hubs 100 for JellyFish Assault Using AODV conference

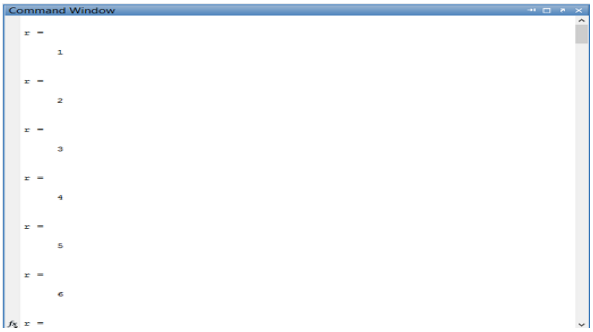

Fig 5.2-No. of Rounds from 1 to 6 which is definitely appeared here for JellyFish Assault Using AODV Protocol

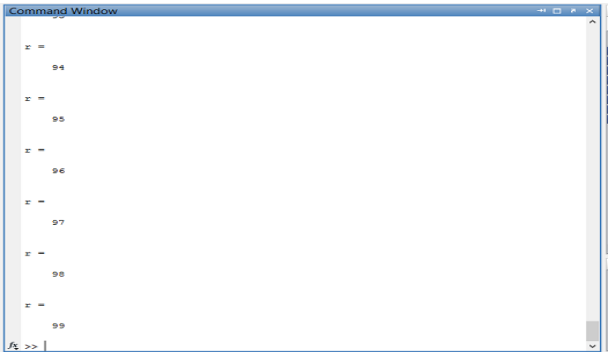

Fig 5.3 - No. of Rounds from 94 to 99 which is definitely appeared here for JellyFish Assault Using AODV (Total No. of Rounds 99)

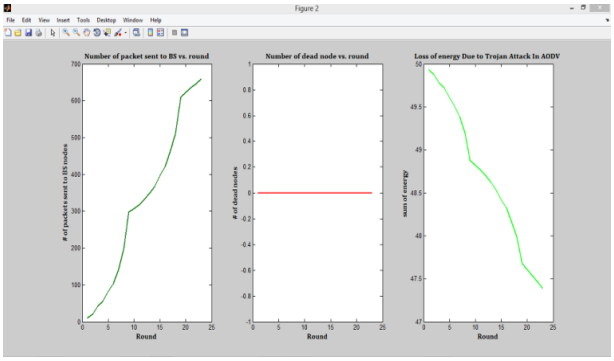

Fig 5.4: (1)- Quantity of Packets Sends To BS Vs Rounds (2) Quantity of Dead Nodes versus Cycle (3) Loss of Energy Due to JellyFish Assault in AODV in Different Rounds

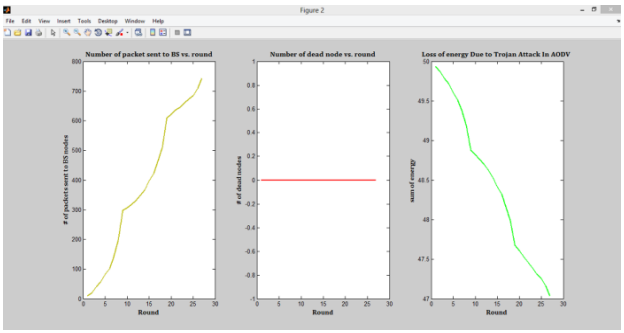

Fig 5.5 : (1)- Quantity of Packets Sends To BS Vs Rounds (2) Quantity of Dead Nodes versus Routine (3) Reduction of Energy Due to JellyFish Assault in AODV in Different Rounds

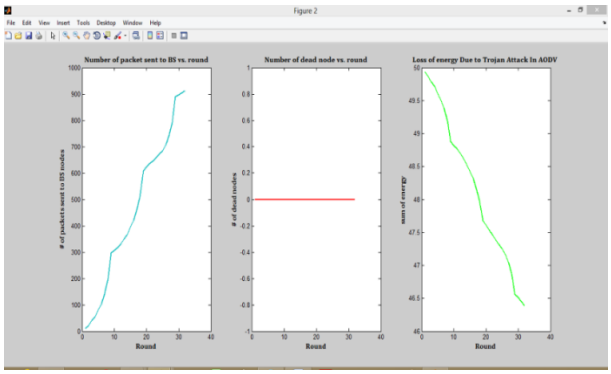

Fig 5.6 : (1)- Quantity of Packets Sends To BS Vs Rounds (2) Quantity of Deceased Nodes versus Routine (3) Reduction of Energy Due to JellyFish Strike in AODV in Different Rounds

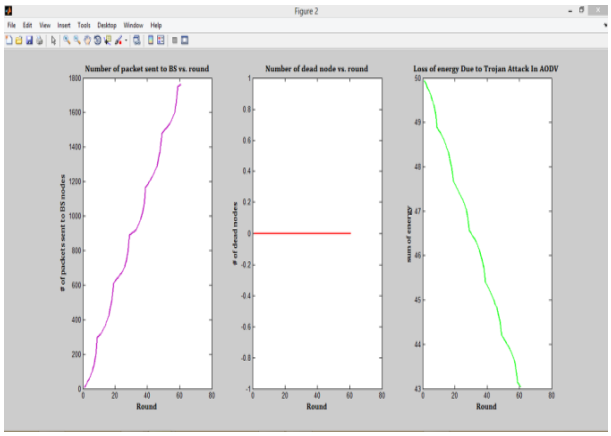

Fig 5.7 : (1)- Figure of Packets Sends To BS Vs Rounds (2) Figure of Dead Nodes versus Routine (3) Reduction of Energy Due to JellyFish Strike in AODV in Different Rounds

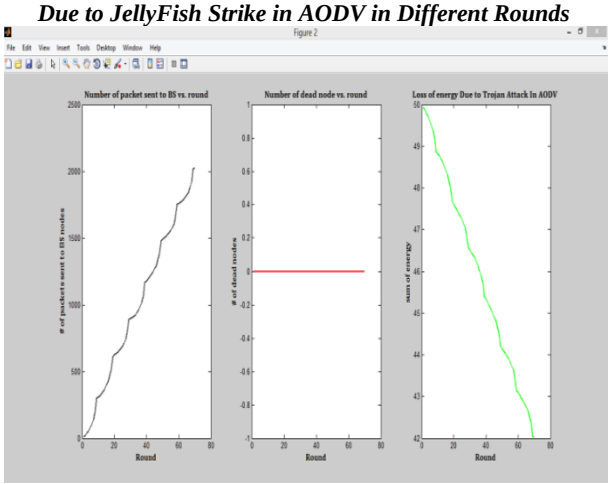

Fig 5.8 : (1)- Figure of Packets Sends To BS Vs Rounds (2) Figure of Dead Nodes versus Routine (3) Reduction of Energy Due to JellyFish Strike inAODV in Different Rounds

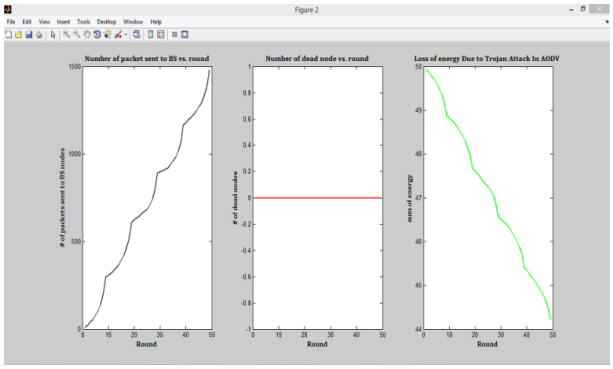

Fig 5.9: (1)- Figure of Packets Sends To BS Vs Rounds (2) Figure of Dead Nodes versus Routine (3) Reduction of Energy Due to JellyFish Strike in AODVafter99 Rounds

VI. CONCLUSION AND FUTURE WORK

6.1. Conclusion

In this evaluation, we dissected impact of the JellyFish in an AODV Network. For this cause, we performed an AODV lifestyle that bears on as JellyFish in MATLAB-13. We reproduced five situations where every one offers 20 hubs that utilization AODV tradition and furthermore reenacted related situations subsequent to bringing one JellyFish Node into the system. In addition, we similarly carried out an solution that endeavored to diminish theJellyFish influences in MATLAB-13 and reenacted the set up utilizing related situations.

6.2. Future Work

Our answer attempts to destroy the JellyFish impact at the program assurance instrument of the AODV convention that is done before the hubs begin the bundles. Also, we utilized UDP association with have the option to check the parcels at sending and receiving hubs. On the off opportunity that we got used the TCP association between hubs, the sending centre would become the end of the association, since ACK parcels don't attain the sending centre. This would become another response for locating the JellyFish Node. This occurs after the program guarantee component of the ADOV tradition and discovers the program in an any much longer period. Our response discovers the method in the AODV level. Locating the JellyFishcentre with association located conventions could become another function as a potential report.

REFERENCES

1. *Sureka.N1, Prof. S. Chandra Sekaran "Securable Routing And Elimination Of Adversary Attack From Manet" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 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) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014 Copyright @ IJIRCCE www.ijircce.com 4068.*
2. *Harsha.N1, Rashmi.S "Detection of Vampire Attack and Prevention in MANET" ISSN (Online) 2278-1021 ISSN (Print) 2319 5940 International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015. Copyright to IJARCCE DOI 10.17148/IJARCCE.2015.4872 340.*
3. *SumitAgrawal, ShilpaJaiswal "Study to Eliminate Threat of Black Hole of Network Worms in MANET" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153*
4. *Saritha Reddy Venna1, Ramesh BabuInampudi "Security Attacks in Mobile Ad Hoc Networks" Saritha Reddy Venna et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1), 2016, 135-140.*
5. *GuozhuMeng, Yang Liu, Jie Zhang, Alexander Pokluda, RaoufBoutaba "Collaborative Security: A Survey and Taxonomy" USA, fax +1 (212) 869-0481, or ACM 0360-0300/YYYY/01-ARTA $15.00 DOI:http://dx.doi.org/10.1145/0000000.0000000 ACM Computing Surveys, Vol. V, No. N, Article A, Publication date: January YYYY.*

6. *K.Sivakumar1, P.Murugapriya "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 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) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014. Copyright @ IJIRCCE www.ijircce.com 596.*
7. *Manju.V.C. "Wireless Sensor Network Attacks" ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 2, August 2012.*
8. *Ambili M A1, BijuBalakrishnan "A Security Approach For Detection And Elimination Of Resource Depletion Attack In Wireless Sensor Network" ISSN(Online): 2320-9801 ISSN (Print): 2320-9798 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) Organized by Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014.*
9. *Varalatchoumy.M, Sowmya H.K. Kohilambal R "Security Attacks and Defensive Technologies in MANETs" Proc. of the Intl. Conf. on Computer Applications – Volume 1. Copyright © 2012 Techno Forum Group, India. ISBN: XXXXXXX :: doi: 10.XXXXX/ISBN_0768 ACM #: dber.imera.10.XXXXX*
10. *Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002, 3–13.*
11. *X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.*
12. *J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.*
13. *S. Kurosawa, H. Nakayama, and N. Kato, "DetectingJellyFishattackon AODV based mobile ad-hoc networks by dynamic learning method, "International Journal of Network Security, pp. 338–346, 2007.*
14. *K. Makki, N. Pissinou, and H. Huang, "Solutions to the JellyFishproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.*
15. *S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand JellyFish Attack.," International Conference on Computational Intelligence and Security, 2009.*
16. *Chang Wu Yu, Wu T-K, Cheng RH, Shun chaochang, "A Distributed and Cooperative JellyFish Node Detection. And Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549, 2007.*