ANALYSIS OF MALACIOUS JELLY FISH NODES ON WIRELESS SENSOR NETWORK THROUGH MATLAB

Shayma Nand Kumar[1], Debprasad Sinha[2]
[1]M.Tech(ECE), [2]Assistant Professor(ECE)
Bengal Institute Of Technology & Management, Santiniketan

Abstract: Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of a network which collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.
Key Word: Wireless Ad Hoc Network, AODV, JellyFish, MATLAB

I. INTRODUCTION

As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the JellyFish attack. In the JellyFish attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. JellyFish attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets.

1.1 Wireless Networks

Wireless communication is used to transfer data among users without a wired infrastructure. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication spreads from home RF to satellites, from cellular phones to walkie-talkies. Its mobility, simplicity and cost saving installation advantages make the wireless communication more popular, especially in recent decades Increasing user mobility needs and developments in the use of laptop computers and PDA's is one of the main reasons of the popularity of wireless networks.

II. LITERATURE SURVEY

Sureka.N1, Prof. S. Chandra Sekaran proposed resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase. The wireless Adhoc sensor network and routing data in them is vulnumarable to certain attacks. So we must ensure a secure and authenticated data transmission process. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack draining of node life from wireless adhoc sensor networks. Adhoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications.

Harsha.N1, Rashmi.S proposed an approach to detect and prevent the vampire attack in MANET. Ad-hoc low-power wireless networks are the most promising research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of service at the routing or medium access control levels. Earlier, the resource depletion attacks are considered only as a routing problem, very recently these are classified in to a new group called "vampire attacks". Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing .It is clear that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In the worst case, a single Vampire can increase

network-wide energy usage by a factor of O (N), where N in the number of network nodes.

Sumit Agrawal, Shilpa Jaiswal proposed a Secure Ad-hoc On-Demand Distance Vector routing protocol (SAODV) to endeavor our all efforts into a common place. So the emphasis is to develop a scheme for the measure of these network worms and blackhole attacks to eliminate occurrences of communication hazards from intermediate and surrounding threads. the full study to eliminate thread of black hole attacks in MANET". We also address to the solution against the threat of black hole attack in MANET. In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. So to rectify the possibility of occurrence of black hole attack we are proposing a technique to identify attack and a solution to discover a safe route for secure transmission. The need of wireless network is to enforce participating nodes to forward packets to other nodes to foster secure and reliable communication. Although there are presence of vulnerable nodes that can be associated with malicious nodes and can harm networks. The varieties of these malicious nodes are vulnerable to nodes which are either compromised or falsely guided by vulnerable nodes. Malicious nodes can easily tamper the participating nodes in the networks. In mobile ad hoc network these attacks shown their significance in the terms of network worms which can attack, alter or modify the root definitions of network across all administrative and participating domains.

Saritha Reddy Venna1, Ramesh Babu Inampudi proposed vulnerabilities and various kinds of security attacks in MANETs The recent and rapid advancements in the technology and the distinct features of MANETs have made the use of MANETs more prevalent. With the ever increasing applications, the weakness of these networks against a variety of attacks has been unveiled. MANETs doesn't have clear and efficient mechanisms to detect or prevent the attacks, so attacker node can easily interrupt and destroy the whole system or may take control over the information being transmitted in the network. Attackers introduce various kinds of attacks and every attack has its own degree of impact on the network. Security is a major concern in MANETs because of its intrinsic vulnerabilities. Each mobile node can work either as a host or as a router. There is no necessity of fixed infrastructure and these mobile nodes organize themselves in an arbitrary fashion to form a temporary network with dynamically changing topology. Nodes within each other's wireless transmission ranges can communicate directly but nodes outside each other's rangehave to depend on neighbouring nodes to relay messages.

Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba proposed different mechanisms of collaboration and defense in collaborative security. We systematically investigate numerous use cases of collaborative security by covering six types of security systems. Aspects of these systems are thoroughly studied, including their technologies, standards, frameworks, strengths and weaknesses.We then present a comprehensive study with respect to their analysis target, timeliness of analysis, architecture, network infrastructure, initiative, shared information and interoperability. We highlight five important topics in collaborative security, and identify challenges and possible directions for future research. Our work contributes the following to the existing research on collaborative security with the goal of helping to make collaborative security systems more resilient and efficient. Security is oftentimes centrally managed. An alternative trend of using collaboration in order to improve security has gained momentum over the past few years. Collaborative security is an abstract concept that applies to a wide variety of systems, and has been used to solve security issues inherent in distributed environments. Thus far, collaboration has been used in many domains such as intrusion detection, spam filtering, botnet resistance, and vulnerability detection.

III. PROBLEM FORMULATION

Initially, we should take into account Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol and then we shall explain JellyFish Attack.

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

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network band width utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are contro lmessages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in [13]. When the source node wants to make a connection with the destination node, it broad cast an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Figure below shows how the RREQ message is propagated in an ad-hoc network.

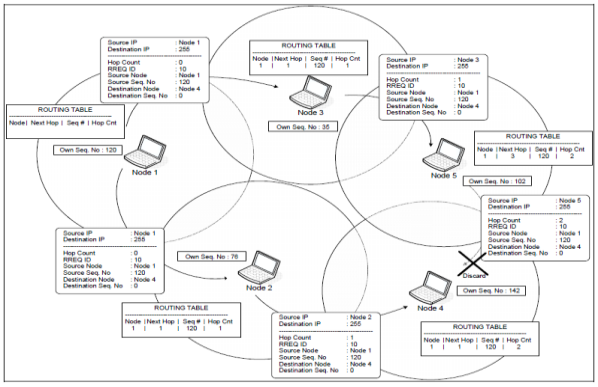

Figure 3.1 – Propagation of the RREQ message

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node.

Afterwards the RREP message is unicasted to the source node. The difference between the broadcasting an RREQ and unicasting RREP can be seen from Figures 9 and 10. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol. The default constant values of the AODV protocol are listed. Thus the node knows over which neighbor to reach at the destination. In terminology, the neighbor list for destination is labeled as "Precursor List". Figure 3.1 shows how the RREP message is unicasted and how the route entries in the intermediate nodes are updated.

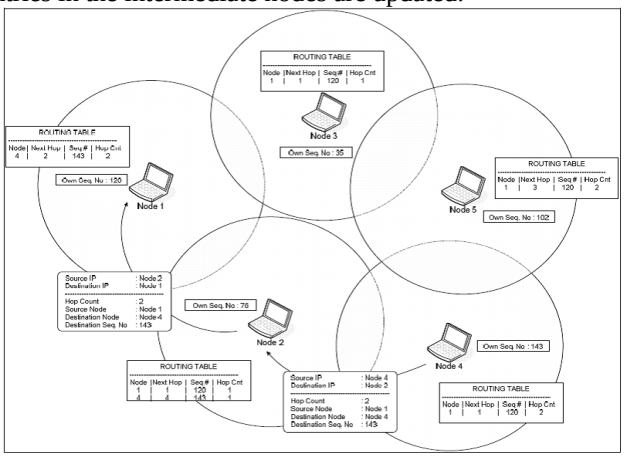

Figure 3.2 – Unicasting the RREP message

3.2. Sequence Numbers

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes.

The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message.

In Figure 3.1, while Node 2 forwards the RREP message coming from Node 3, it compares its own previously stored sequence number with that of Node 3. If it notices that the sequence number is newer than its own, then it changes its route table entry as necessary.

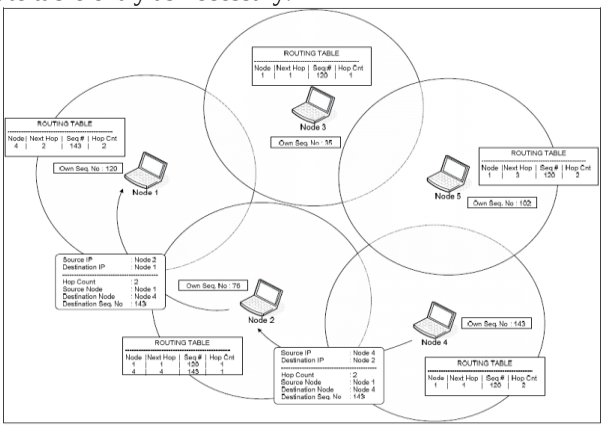

Figure 3.3 – Updating the Sequence Number with fresh one

3.3. JellyFish Attack

JellyFish Attack is briefly explained in the previous Chapter. In this Chapter we shall explain it in more detail as we have already explained the AODV protocol. In an ad-hoc network that uses the AODV protocol, a JellyFish node absorbs the network traffic and drops all packets. To explain the JellyFish Attack we added a malicious node that exhibits JellyFish behavior in the scenario of the figures of the previous section.

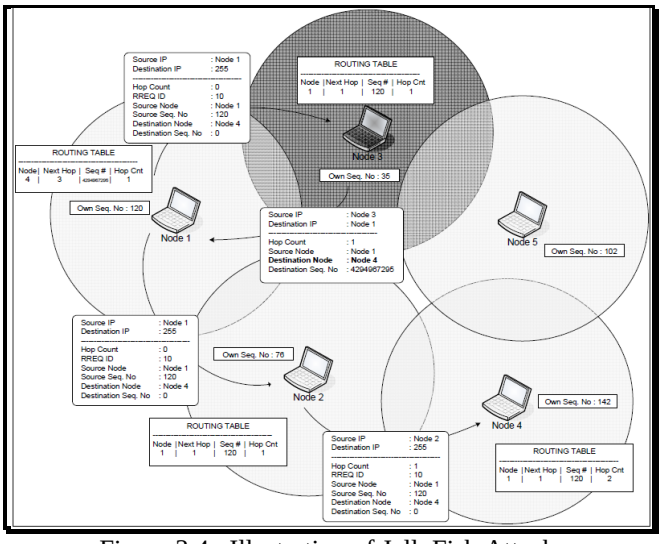

Figure 3.4– Illustration of JellyFish Attack

In this scenario shown in Figure 3.4, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets. In a JellyFish Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.In our scenarios we use UDP data packets and we will explain our scenarios and their results below.Before we will describe how JellyFish behavior is implemented in the simulator program, MATLAB- 10.

IV. METHODOLOGY

4. Result, Discussion and Simulation

In this work, we have tried to evaluate the effects of the JellyFish attacks in the wireless Ad-hoc Networks. To achieve this we have simulated the wireless ad-hoc network scenarios which includes JellyFish node using MATLAB-10[14] program. To simulate the JellyFish node in a wireless ad-hoc network we have implemented a new protocol that drops data packets after attracting them to itself. In this chapter we present MATLAB- 10and our contribution to this software.

4.1. MATLAB- 10

MATLAB- 10 is an event driven MATLAB- 10 program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. The MATLAB- 10 is a part of software of the VINT project [15] that is supported by DARPA since 1995.

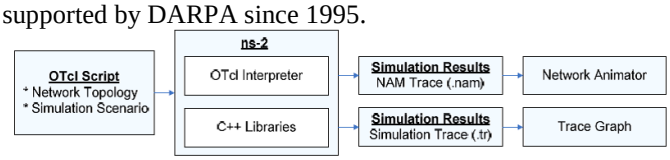

Figure 4.1 - MATLAB- 10 schema

At the simulation layer MATLAB- 10 uses OTcl (Object oriented Tool Command Language) programming language to interpret user simulation scripts. OTcl language is in fact an object oriented extension of the Tcl Language. The Tcl language is fully compatible with the C++ programming language. At the top layer, MATLAB- 10 is an interpreter of Tcl scripts of the users, they work together with C++ codes. In Chapter 5 the usage of the Tcl Language will be explained in detail.

As shown in Figure 4.1, an OTcl script written by a user is interpreted by MATLAB- 10. While OTcl script is being interpreted, MATLAB- 10 creates two main analysis reports simultaneously. One of them is NAM (Network Animator) object that shows the visual animation of the simulation. The other is the trace object that consists of the ehavior of all objects in the simulation. Both of them are created as a file by MATLAB- 10. Former is .nam file used by NAM software that comes along with MATLAB- 10. Latter is a ".tr" file that includes all simulation traces in the text format.

MATLAB- 10 project is normally distributed along with various packages (MATLAB- 10, nam, tcl, otcl etc.) named as "all-in-one package", but they can also be found and downloaded separately. In this study we have used version 2.29 of MATLAB- 10 all-in-one package and installed the package in the Windows environment using Cygwin. After version 2, MATLAB- 10is commonly using a MATLAB- 10 and in our thesis we shell refer to it as MATLAB- 10. We have written the ".tcl" files in text editor and analyzed the results of the ".tr" file using"cat", "awk", and "wc" and "grep" commands of Unix Operating System.

4.2 SIMULATION OF JellyFish ATTACK AND ITS EFFECTS

We explained JellyFish Attack in AODV Routing Protocol and in Chapter 4 we described how this attack is implemented into the MATLAB- 10. In this Chapter, first, we will briefly explain the Tcl Language to understand the simulation scenarios. Having shown how we tested the JellyFish implementation, we will present the simulations of JellyFish Attack to demonstrate its effects. Then we will evaluate the effects of JellyFish Attack in an Ad-Hoc Networks.

V. RESULTS

5.1 Implementation process under MATLAB Considering AODV, DSR and DSDV Modification:

The nature of wireless network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack

.

Impersonation: In wireless networks a node is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious nodes. The attacker use MAC and IP spoofing in order to get identity of another node and hide into the network. This kind of attack is also known as spoofing attack. Man in middle Attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender. Selective Forwarding: In such attacks, malicious nodes may refuse to forward certain packets and simply drop them, ensuring that they are not propagated any further. An adversary will not, however, drop every packet. To avoid raising suspicions, the adversary instead selectively drops packets originating from a few selected nodes and forwards the remaining Traffic .

False Node: A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false.

Passive Traffic Monitoring: It can be developed to identify the communication parties and functionality which could provide information to launch further attacks.

Eavesdropping: The term eavesdrops implies overhearing without expending any expending any extra effort. In this intercepting and reading and conversation of message by unintended receiver take place. Mobile host in mobile ad-hoc network shares a wireless medium. Majorities of wireless communication use RF spectrum and broadcast by nature. Message transmitted can be eavesdropped and fake message can be injected into network.

Traffic Analysis: Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

Syn flooding: This attack is denial of service attack. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. It produces severe resource constraints for legitimate nodes.

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. In this thesis, we have analyzed security attacks its prerequisite and vulnerability for processing and collecting the information in WSN and presented the security objective that need to be achieved.

VI. CONCLUSION AND FUTURE WORK

Our solution tries to eliminate the JellyFish effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start the packets. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the JellyFish Node. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Our solution finds the path in the AODV level. Finding the JellyFish node with connection oriented protocols could be another work as a future study.

REFERENCE

[1] Sanjeet1, Asst Prof. Sonia Rani2 "Detection And Elimination Of JellyFish Attack In Manet" International Journal For Technological Research In Engineering Volume 2, Issue 12, August-2015 ISSN (Online): 2347 – 4718. www.ijtre.com Copyright 2015.All rights reserved. 2996.

[2] 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.

[3] 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.

[4] Sumit Agrawal, Shilpa Jaiswal "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

[5] Saritha Reddy Venna1, Ramesh Babu Inampudi "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.

[6] Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba "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.

[7] 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.

[8] 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.

[9] 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.

[10] 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

[11] 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.

[12] 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.

[13] 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.

