Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT

[1]Tawseef Ahmad Naqishbandi and [2]Imthyaz Sheriff C

Department of Computer Science and Engineering

B.S.Abdur Rahman University

Chennai, India

Abstract-The widespread growth of Ad-hoc sensor networks represents the next evolution of internet having the ability to gather, analyze, and distribute data that can turn data into information, knowledge, intelligent decision making and ultimately for future prediction. This latest state-of-the-art sensing, computing and communication system are not only changing consumer expectation in people's everyday lives but gradually taking them closer to the future era of connected everyday things, using mixtures of wired and wireless connectivity. The communication of these network devices creates the Internet of Things (IoT), wherein Ad-Hoc Wireless Sensor Networks (WSN) are ready to dynamically be a part for accomplishing distinctive tasks. To attain this vision, there is a need for energy efficient systems to support the challenging requirements for future internet to survive. Ad hoc sensor networks are susceptible to attacks which will drain the battery life. IoT will be susceptible to same problems but at a larger level. This paper explores the energy issues and attacks that challenge that are faced by Ad-Hoc WSNs and eventually the future IoT. It also discusses a resilient strategic approach for handling energy attacks.

I. INTRODUCTION

It is estimated that Ad Hoc mobile internet devices that can act as sensors will outnumber humans in 2014 and by 2015, there will be about 15 billion internet-connected devices. An installed base of 212 billion connected "things" and an overall economic benefit of $8.9 trillion by 2020 are impressive numbers behind the hype of the Internet of Things, or short just IoT [19]. According to IDC, the "Internet of Things" will change everything and be "a new construct in the information and communications technology world."

Wireless Ad hoc Sensor networks are emerging as a widely used technology with evidence of their deployment in space, educational, agricultural, domestic, commercial, military environments. The sensors utilized within these systems are generally utilized in particular geographic areas and these sensors self-compose to form an ad-hoc wireless network to gather data. Because of Ad hoc nature these sensor networks 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, agricultural growth and security deployment at borders.

A major consideration in Ad hoc sensor networks and IOT is energy efficiency and low power consumption. Ad hoc WSNs consist of many randomly scattered and possibly moving sensor nodes. Ad hoc wireless sensor nodes and smart devices which form IOT are generally powered by either non-rechargeable or rechargeable limited power batteries and generally located at remote locations. Efficient use of power is key to this type of environment. Due to Ad hoc nature, these wireless sensors are vulnerable to denial of service (DoS) attacks [7], can replicate in IOT also and a great deal of research has been done to enhance survivability [2-7]. A major concern in Ad hoc wireless sensor networks are Energy attacks which are not protocol specific. Since these energy attacks drain energy from nodes which directly affects communication between nodes.

The purpose of this paper is to thoroughly explore the vulnerabilities of existing secure routing protocol such as Ad hoc On-Demand Distance Vector (AODV) and study the impact of energy attacks through simulation using NS2. In Section 2, focus is on the current state of research work done for energy related issues in Ad hoc wireless sensor networks. In section 3, energy attacks and its impact on AODV is discussed. Performance of Ad-Hoc WSNs under different energy attacks scenarios is presented in Section 4 and mitigation methods are discussed in section 5. Section 6 and 7 discusses the proposed methodology and algorithm.

A. Protocols and Assumptions

This paper considers the effect of energy attacks on AODV. The protocol covered is an important subset of the routing solution space and stresses that energy attacks are likely to apply to other protocols. The corrupted nodes location within the network is assumed to be fixed. This paper will show later how corrupted node also effects honest nodes and drains their energy. Moreover, a new proposed protocol called CBEWRA is discussed to improve resilience in Ad hoc wireless sensor networks

II. RELATED WORK

Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. Energy attacks have not been rigorously defined at the routing layer.

Stajano et. al. [8] proposed a "Sleep deprivation torture". This proposed attack prevents nodes from entering a lower-power sleep cycle and thus depletes their battery life faster. In this a malicious user may interact with a node in an otherwise legitimate way, but for no other purpose than to consume its battery energy.

J.H.Chang et. al.[20] focussed on minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g. by minimizing wireless transmission distance) is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios.

H.Chan et. al.[9-10] have briefly mentioned malicious cycles i.e. routing loops, but no effective strategies are discussed other than increasing efficiency of MAC and routing protocols.

D.J.Bernstein [11] suggests that in non-power-constrained systems, diminution of resources such as memory, CPU time, and bandwidth may easily cause problems for example SYN flood attack, wherein adversaries make multiple connection requests to a server, which allocates resources for each connection request, eventually running out of resources, while the adversary, who allocates nominal resources, remains operational. Such attacks can be weighed down by putting greater burden on the connecting entity (e.g. SYN cookies).These solutions place minimal load on genuine clients which only initiate a small number of connections, but prevent malicious entities, but these solutions may not sufficiently justify the excess load on genuine nodes.

Eugene.Y.Vasserman et. al. [12] explores 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. This paper proposed defenses against some of the forwarding-phase attacks described in PLGPa [10], the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. This paper had not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa.

Chris Karlof et. al. [13] proposed security goals for routing in sensor networks, shows how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks—sinkholes and Hello floods, and analyze the security of all the major sensor network routing protocols. They described crippling attacks and suggests countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks. This paper conclude that Secure routing is vital to the acceptance and use of sensor networks for many applications, but this paper has demonstrated that currently proposed routing protocols for these networks are insecure. This research paper leaves it as an open problem to design a sensor network routing protocol that satisfies proposed security goals.

Chul sung et. al. [14] proposed that Battery life extension is the principal driver for energy-efficient wireless sensor network (WSN) design. However, there is growing awareness that in order to truly maximize the operating life of battery-powered systems such as sensor nodes, it is important to discharge the battery in a manner that maximizes the amount of charge extracted from it. In spite of this, there is little published data that quantitatively analyse the effectiveness with which modern wireless sensor nodes discharge their batteries, under different operating conditions.

Yingtao Jiang et. al. [15] discuss that the next generation of internet is becoming the "Internet of Things (IoT)"which is a worldwide network of interconnected objects and their virtual representations uniquely addressable based on standard communication protocols. Identified by a unique address, any object including computers, mobile phones, RFID tagged devices, and especially Wireless Sensor Networks (WSN) will be able to dynamically join the network, collaborate, and cooperate efficiently to achieve different tasks. The purpose of this special issue thus is to report on the recent and original advances on WSN and IoT that are to be innovative to open the new era of the Internet of Things.

III. ENERGY ATTACKS ON AODV PROTOCOL

AODV is a secure method of routing messages between nodes. It allows these mobile nodes, to pass messages through their neighbours to other nodes with which they cannot directly communicate. AODV uses a method by discovering the routes along which messages can be passed. AODV makes sure these paths do not contain loops and tries to find the shortest route possible. Energy attacks by an insider adversary on AODV secure routing protocol proves catastrophic when implemented. Two types of attacks are implemented in this paper i.e. Carousel and Stretch Attack [12] as shown in Fig 1 and 2

Carousel Attack: - In this type of attack, a malicious node sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length and in this way the energy is lost from the nodes.

*Stretch Attack***: -** In this type of attack, a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. The honest path is very less distant but the malicious path is very long to make more energy consumption.

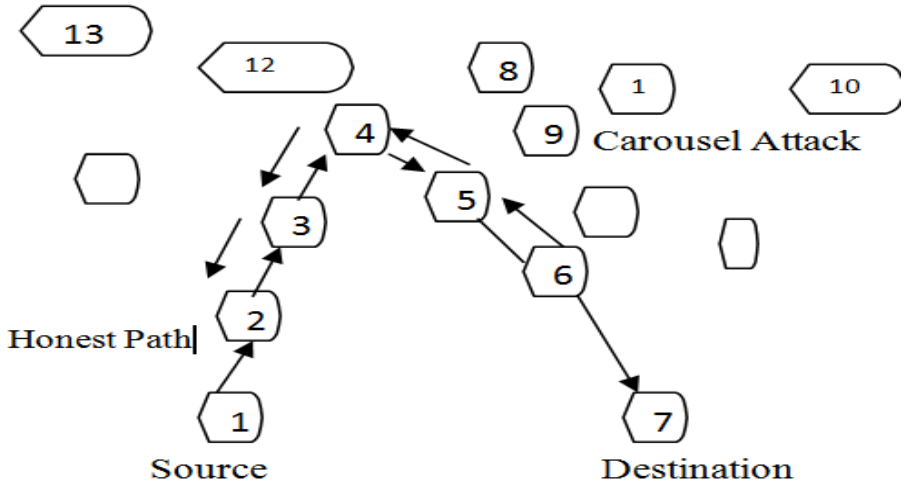

Fig.1. Craousel Attack same node in the Route Many times.

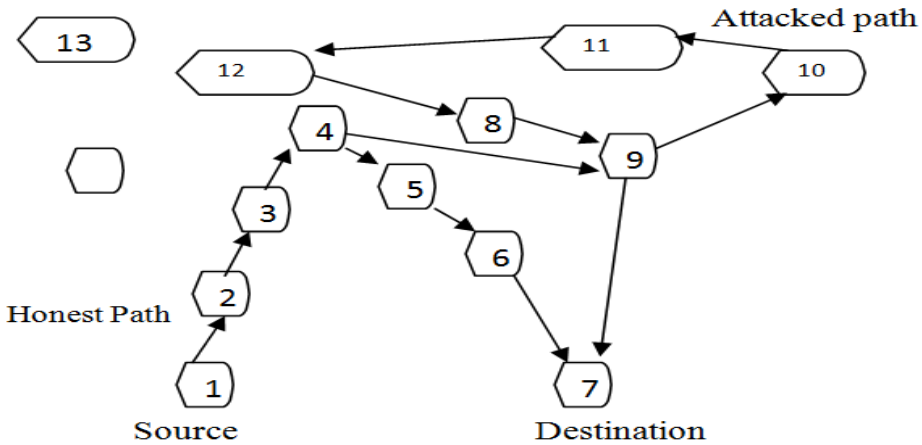

Fig.2. Stretch Attack with two different paths from source to destination(4-9-10-11-12-8-9-long Route).

Carousel and Stretch attack in a randomly-generated 20-node topology and a single randomly-selected malicious AODV agent, using the ns- 2 network simulator [1] were simulated in this work. Each node has been provided with 3 joules of energy and data is sent from source to destination. Source node sends 512 bytes of data per every 0.1 second towards destination and simulation is run for 600, 1200 and 1800 seconds, and after proper analysis of energy attacks, simulation results show how fast energy of the nodes drains out and network becomes disabled.

IV. SIMULATION

4.1 Simulation Environment

Analysis of energy attacks is performed using the network simulator NS2 [18]. In this simulation, the experimental model is built on 20 nodes which can be further increased up to 1000 distributed randomly. The sensor nodes operate on non-renewable batteries and start the simulation by an initial energy equal to 3J. Each node uses its limited reserves of energy throughout the duration of simulation. Thus, any node which has exhausted its energy reserve is considered dead. Therefore, it can't transmit or receive data. The simulation parameters used in the simulation model are summarized in the table below.

TABLE1.: Simulation Parameters

Parameter	Value
Traffic Type	CBR
Channel type	Channel/Wireless Channel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11

Interface queue type	Queue/Drop Tail/PriQueue
Antenna model	Antenna/Omni Antenna
Routing protocol	AODV
Initial energy in Joule	3

A. Simulation Results

This paper shows simulation of a simple scenario of Ad hoc wireless sensor network using AODV protocol without any energy attack as shown in Fig.3.(a) and measures the remaining nodes energy reserve using awk graphs, the number of nodes whose energy has reached to threshold and the packet delivery ratio of data for 1200 seconds. The simulation results after analysis shows that energy is draining slowly with respect to time simulation is run.

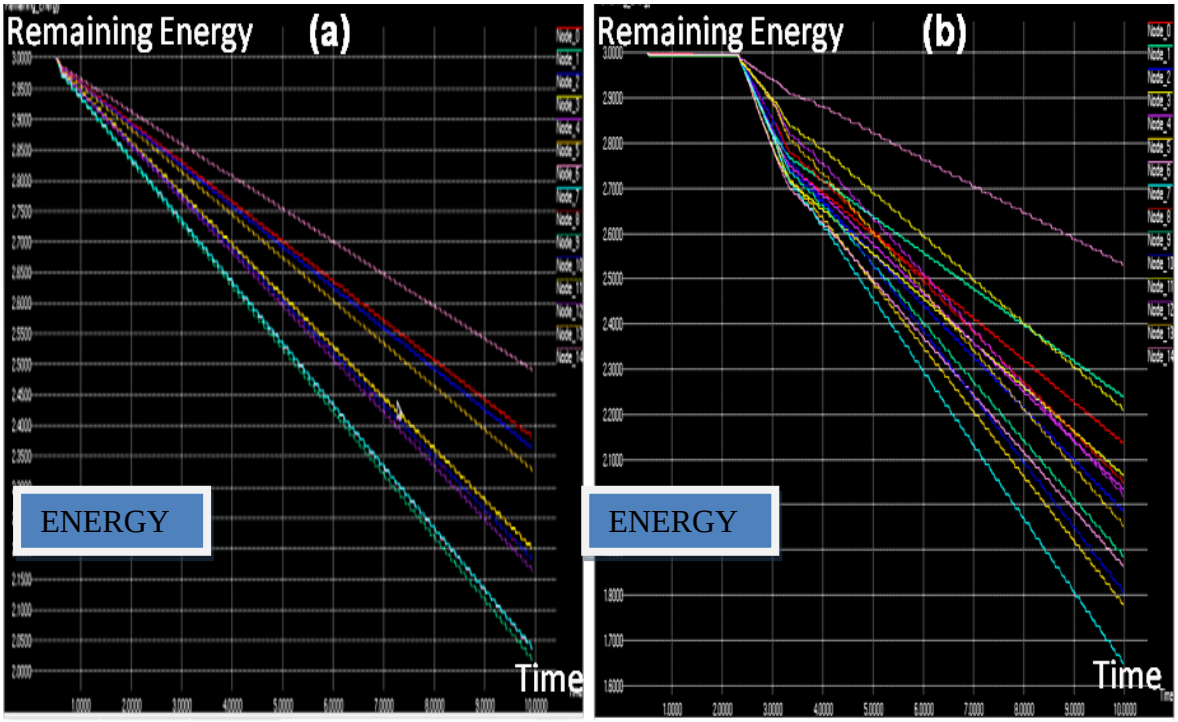

Fig.3. (a) X graph showing Energy levels before any attack
(b) Shows the simulation result when carousel attack is implemented.

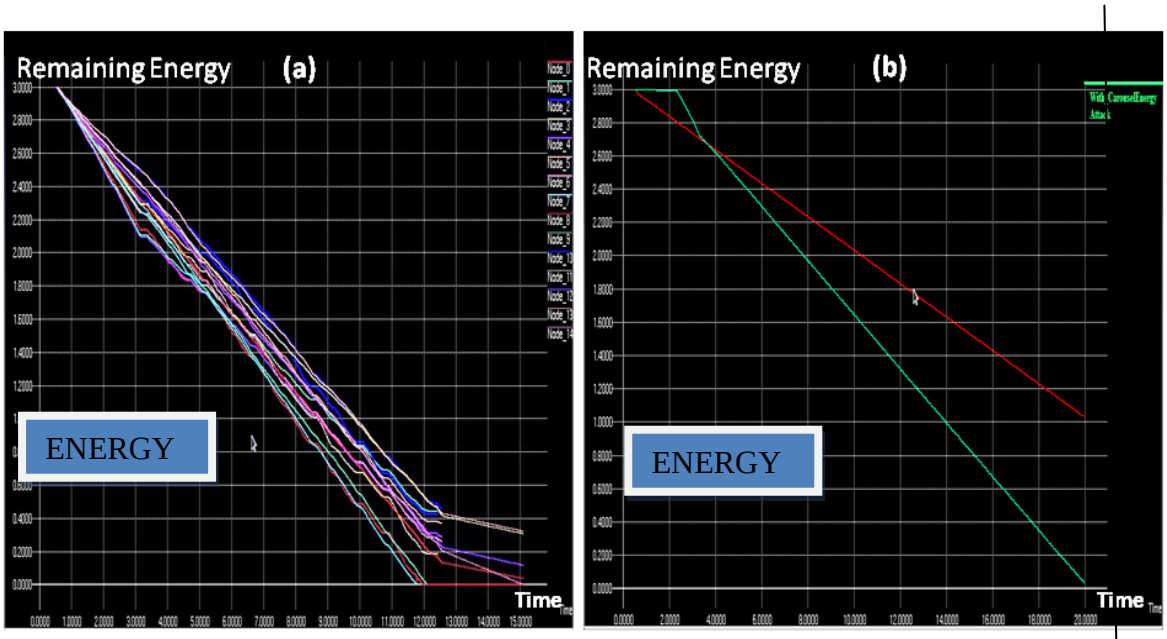

Fig.4(a).shows the impact of stretch attack on energy levels and Fig 4(b) shows the remaining energy level comparision before and after energy attack

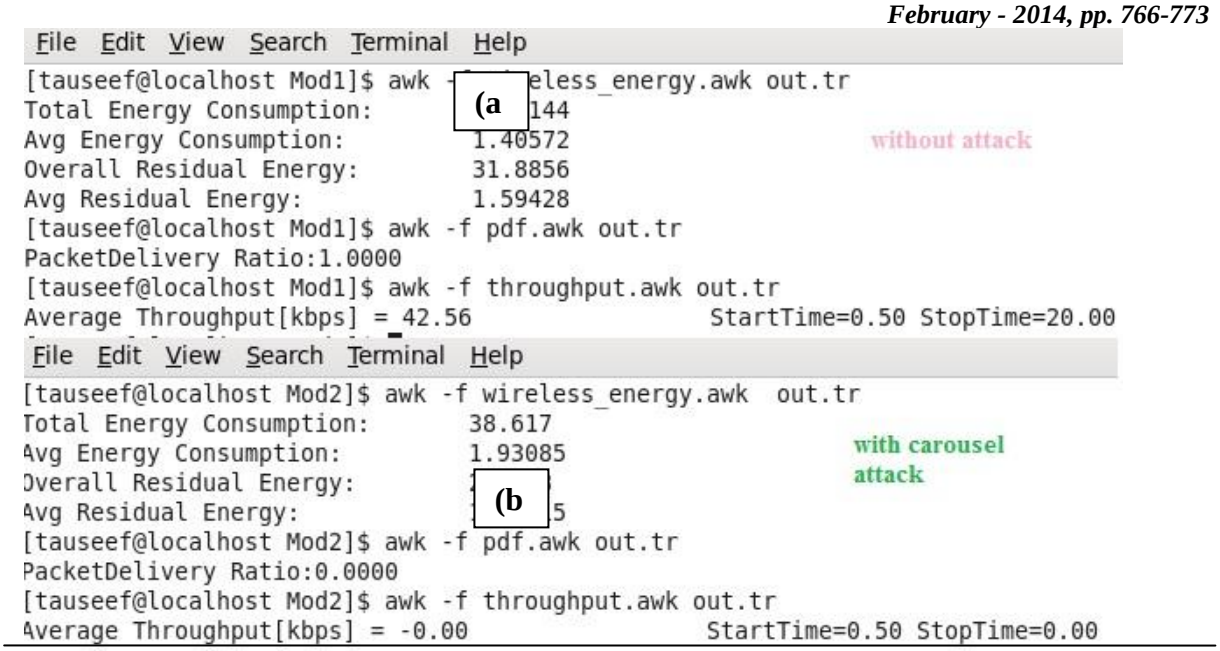

Fig.5(a). Deviation analysis in Total Energy Consumption, Residual Energy and Packet Delivery Ratio when there is no Energy Attack with (b) Carousel Energy Attack

The notional limit of Carousel Attack is an energy usage factor of O (λ), Where λ is the maximum route length. The simulation results as shown in (a) and (b) when compared show that the total energy consumption increases by 10.5020J for 20 Nodes as compared to the scenario when no energy attack is present and average energy consumption increases by factor of 0.53313J.

V. MITIGATION METHODS FOR ENERGY ATTACKS

The carousel attack can be prevented entirely by having forwarding nodes check source routes for loops. But this adds extra forwarding logic and thus more overhead. The ns2 AODV protocol does implement loop detection, but does not use detection to check routes while forwarding packets. When a loop is detected, the source route can corrected and the packet moves further towards its destination, but one of the good features of source routing is that the route can itself be signed by the source node and destination node while sending Route Request Message (RREQ) and Route Reply (RREP). Hence, it is better to just drop the packet, considering that the sending node is likely malevolent i.e. honest node will not likely to introduce loops. The other solution is to make some changes to show how intermediate nodes process the source route. To forward a message from source to destination, a node must determine the next hop and the id of the node can be attached with the packet, so that it can locate itself in the source route. Consider, if a node wants to search for itself from the destination but from backward instead from the source forward, any loop that includes the present (current) node will be automatically reduced. Therefore no further processing is required for this strategy.

The stretch attack is more difficult to prevent as longest route for sending packets is way to drain energy from the sensor nodes. Its triumph rate relies on the forwarding node as no checking for optimality of the route is carried out. Some changes as specified in the header, Further; some loose source routing methods are defined, where intermediary nodes can replace some part or the entire route in the packet header if a better route to the destination so known. This makes it necessary for nodes to notice and store optimal routes to at least some portion of other nodes, moderately defeating the as-needed discovery gain. Moreover, storing must be done carefully lest a maliciously suboptimal route be introduced.

There are some algorithms proposed [16, 17], but there has been very little work on whether they could yield satisfactory results in the presence of adversaries. Alternatively bounding the damage of carousel and stretch attackers by limiting the allowed source route length based on the expected maximum path length in the network. But a way is needed to determine the network length. If the number of nodes is known ahead of time which are going to join the network, graph-theoretic techniques can be used to calculate approximately the diameter.

VI. PROPOSED METHODOLOGY

Simulation results show that AODV is vulnerable to Energy Attacks. Consider for example carousel and stretch attack: a receiving honest node may be beyond away from the packet destination than the malevolent forwarding node, but the honest node has no means to tell that the packet it received is moving away from the destination; the only information available with the honest node is his own address and the packet destination address, but not the address of the previous hop. Thus, the Victim node can move a packet away from its destination without being detected. The situation is worse if the packet returns to the victim node in the process of being forwarded — it can now be rerouted again, causing lot of energy drain .Nodes may sacrifice some local storage to retain a record of recent packets to prevent this attack from being carried out repeatedly with the same packet.

Energy Attacks on Ad hoc wireless sensor network affect the long term availability of the network, as it is very difficult to replace limited life batteries which are located at remote locations. So, a resilient strategy has been proposed in this work to save energy from attackers who by means of energy attacks are trying to drain battery life by attacking a single or multiple nodes. The flow diagram for the proposed methodology to detect malevolent node is depicted below in Fig.6.

Every node is given a Node id. Consider a malevolent node which is present inside the network, ready to launch energy attacks. Once a malevolent node receives the packet, it broadcasts that packet with Test Field. Once this packet is received by another node it will check the test field of the packet, if the Test field matches with the already added Test Field. Then normal operation will carry on, if it will not match then an Alarm packet with malevolent node id is created and broadcasted to all other nodes. In this way malevolent node can be detected to avoid further communication

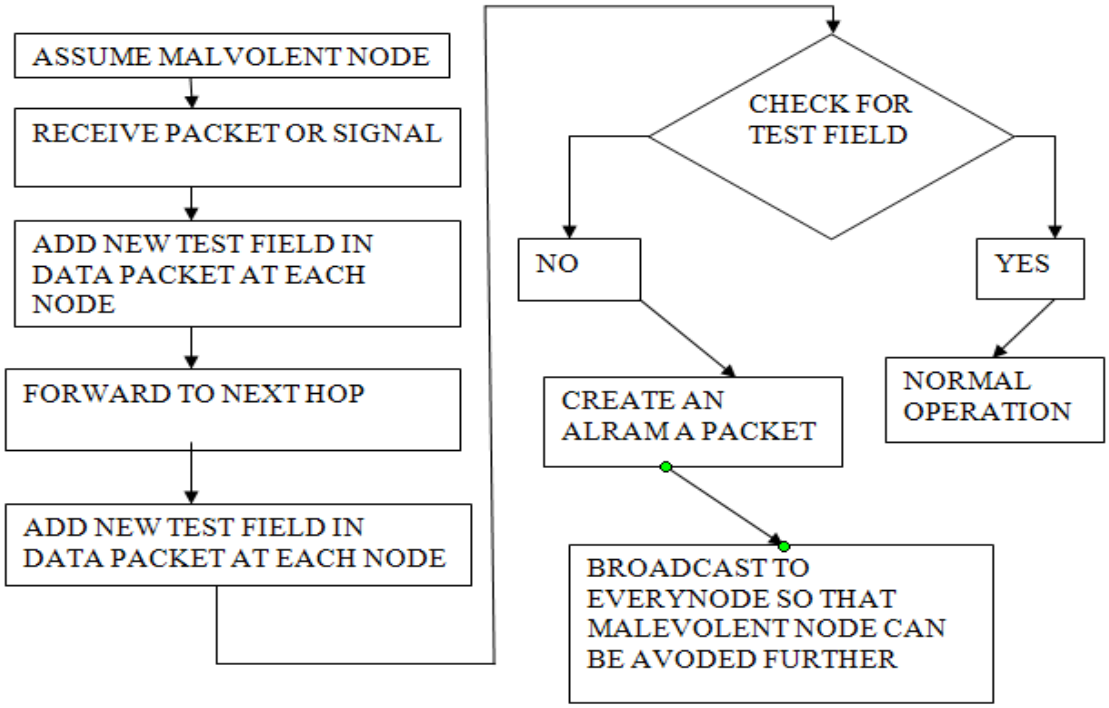

Fig.6. Flow Graph Showing Detection Of Malevolent Node

VII. PROPOSED ALGORITHM

Even if energy attack makes its way to drain the energy from Ad hoc wireless sensor nodes a resilient strategy should be applied so that nodes that are in communication mode will not stop. The proposed algorithm will provide resilience to the nodes .This section focuses on the design details of the proposed protocol CBEWRA (CREDIT BASED ENERGY WEIGHTED RESILIENT ALGORITHM). AS, soon as energy of a node reaches to threshold Level it plays a critical role by performing energy concentrated tasks there by bringing out the energy efficiency of the Ad hoc wireless sensors and rendering the network supportable. This pattern based on the energy levels of the sensors.

CBEWRA functions two phases namely.

A) Network Arrangement phase
B) Communication phase

A. Network Arrangement Phase: The main focus of this phase is to establish an optimal routing path from source to destination in the network. The key factor considered here is balancing the load of the nodes and minimization of energy consumption for communication. In this phase as soon as the energy of the node (which take part in communication) reaches to threshold (which is affected by energy attack) it sends CREDIT_ENG_WEG message to all its surrounding nodes. After receiving the CREDIT_ENG_WEG message the neighbouring nodes send the CREDIT_ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node (whose energy level has reached to Thresh Hold) upon receiving stores this in its routing table to smooth the progress of further computations. Now node establishes the routing path, first it traces the next node by computing the energy required to transmit the requisite data packet that is suitable energy node whose energy is below thresh hold level and less distant node is selected as the next forwarding node in this way it establishes the route from source to destination with suitable energy and less distance .Thus energy is spent by the allotted node suitable for the data packet to reach destination. In this way algorithm avoids data packet dropping and this allotted forwarding node transmits the packets safely to the destination. This algorithm gives major importance to attain balancing of load in the network. The suitable energy node will be assigned as a forwarding node as long as this node has the capacity to handle. In this way less distant path is established to bound the network damage from energy attack.

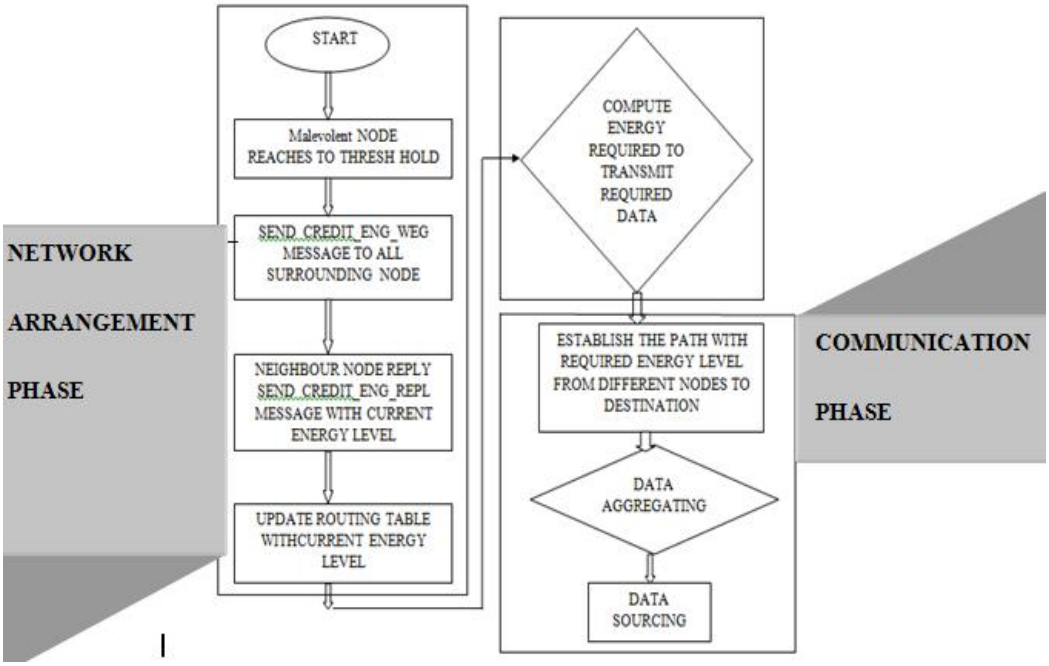

Fig.7.CBEWRA Algorithm Flow Chart.

B. Communication Phase: - The foremost job of this phase is to avoid the same data packets transmitting through the same node repeatedly to drain the batteries very fast and leads to network death because of Energy attacks. The process of repeating the packets is eliminated by aggregating the data transmitting within the forwarding node and route the remaining packets safely to the destination. The data aggregation is achieved by first duplicating the content of the packet that is transmitting through the node. This duplicate content is compared with the data packet that is transmitting through the node if the transmitted packet is same the node stops the data packet transmitting through them. In this way it avoids the redundant packets transmitting through the same node again and again and protects the depletion of energy life. Then send the required data packets through the established node safely to the destination. The flow chart of the algorithm is depicted above in Fig.7

VIII. CONCLUSION AND FUTURE WORK

This proposed work, defines energy attacks, a new class of resource draining attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery life. These energy attacks do not depend on particular protocols but rather exposes the weakness in AODV protocol class. The implementation of various energy attacks on AODV and the impact on energy levels were successfully simulated on a randomly generated topology of 20-30 nodes as shown in previous sections of this paper. The proposed Credit Based Energy Weighted Resilient Algorithm (CBEWRA) for WSN ad hoc routing smart infrastructure will be simulated in future work. For future work, we further wish to enhance the resilience and implement proposed protocol on hardware test bed to consolidate simulation results.

ACKNOWLEDGEMENT

The authors acknowledge valuable contribution from anonymous reviewers, and useful discussion with Dr. V. Sankaranarayanan, Professor of Eminence & Director (University Projects), B.S.Abdur Rahman University.

REFERENCES

[1] O. Vermesan, *et al.*, "Internet of Energy—Connecting Energy Anywhere Anytime" in Advanced Microsystems for Automotive Applications 2011: Smart Systems for Electric, Safe and Networked Mobility, Springer, Berlin, 2011, ISBN 978-36-42213-80-9

[2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, Mobi Com, 2004.

[3] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003

[4] Jing Deng, Richard Han, and Shivakant Mishra, Defending against path based DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[5] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[6] Asis Nasipuri and Samir R. Das, On-demand multipath routing for mobile ad hoc networks, Internationalconferenceon computer communications and networks, 1999

[7] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.

[8] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999

[9] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

[10] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach,CoNEXT, 2006

[11] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.

[12] Eugene Y. Vasserman∗ and Nicholas Hopper," Vampire attacks: Draining life from wireless ad hoc sensor networks," IEEE TRANSACTIONS ON MOBIL COMPUTING VOL.12 NO.2 year 2013

[13] Chris Karlof,David Wagner," Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks 1 (2003) 293–315

[14] Chulsung Park, Kanishka,Lahiri, Anand Raghunathan, "Battery Discharge Characteristics of Wireless Sensor Nodes: An Experimental Analysis" IEEE 0-7803-9012-1 /05 2005

[15] Yingtao Jiang, Lei Zhang, and LingWang, "Wireless Sensor Networks and the Internet of Things" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013.

[16] Alexander Kr¨oller, S´andor P. Fekete, Dennis Pfisterer, and Stefan Fischer, Deterministic boundary recognition and topology extraction for large sensor networks, Annual ACM-SIAM symposium on discrete algorithms, 2006

[17] Yue Wang, Jie Gao, and Joseph S.B. Mitchell, Boundary recognition in sensor networks by topological methods, Annual international conference on mobile computing and networking, 2006

[18] The network simulator — ns-2. http://www.isi.edu/nsnam/ns/.

[19] The Global Information Technology Report 2012

[20] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no.

