PLGPa Approach to Alleviate Energy Draining Attacks in Adhoc Wireless Sensor Networks

Rashmi Konda[1], Naresh Kumar[2]

[1]*PG Scholar, Department of Computer Science Engineering, KITS, Markapur, A.P, India*

[2]*Assistant Professor, Department of Computer Science Engineering, KITS, Markapur, A.P, India*

Abstract: **- Ad hoc wireless sensor networks are thought-provoking topic of research in general computing. Positioning of sensor network in aggressive environment is vulnerable to battery drainage attacks as it is not possible to recharge the sensor nodes. This paper explores on the class of resource depletion attack called the "Vampires" which deactivates the whole network by draining out the nodes' battery power. These Vampire attacks are not specific to any protocol rather we find that all examined protocols are susceptible to Vampire attacks, which makes it difficult to detect. Here we make an attempt discussing methods to mitigate these type of attacks. In this approach forwarding as well as discovery phase of the protocol are considered to avoid attack. Here algorithm overhead is reduced and discovery phase is considered to avoid vampire attack.**

Keywords: **Wireless Sensor Networks, Vampire Attacks, Denial of service, energy efficiency, routing.**

I. INTRODUCTION

Ad hoc wireless sensor networks have wireless communication capability and some level of intelligence for signal processing and networking of the data.These sensor systems have applications in military observing, wellbeing, modern control, climate checking, item following, and home control. The steering systems choice is an imperative issue for the effective conveyance of the parcels to their destination. In addition, in such systems, the connected directing technique ought to guarantee the base of the vitality utilization and subsequently augmentation of the lifetime of the system. One of the first WSNs was composed and created amidst the 70s by the military and resistance commercial ventures. WSNs were likewise utilized amid the Vietnam War as a part of request to bolster the location of adversaries in remote wilderness regions. On the other hand, their usage had a few downsides. It incorporates the huge size of the sensors, the vitality they devour and the restricted system capacity. From that point forward, a great deal of work on the WSNs field has been did bringing about the advancement of the WSNs on a wide assortment of utilizations and frameworks with immensely changing necessities and attributes. In the meantime, different vitality proficient steering conventions have been outlined and created for WSNs with a specific end goal to bolster productive information conveyance to their destination. In this manner, every vitality effective steering convention might have particular attributes relying upon the application and system construction modelling. The WSNs may be utilized as a part of an assortment of ordinary life exercises or benefits. For instance a typical use of WSNs is for checking. In the region of observing, the waves, diverse sorts of remote imparting gadgets furthermore furnished with a vitality source, for example, battery. The whole system works at the same time by utilizing sensors of distinctive measurements and a directing calculation. They are basically centred on giving conveyance information from the source to the destination hubs. WSN is conveyed over a locale so as to screen some wonder. A viable utilization of such a system could be a military utilization of sensors to recognize adversary interruption.

1.1 Energy Consumption in WSN

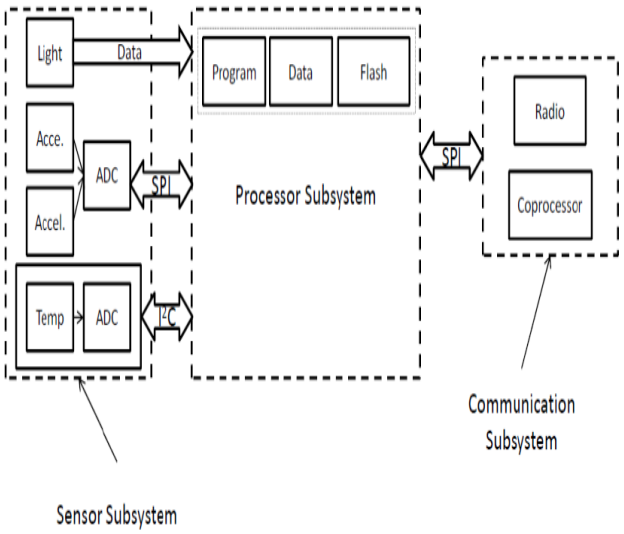

Fig1.0 Architecture of a WSN

The sensor networks consist of a small or large amount of nodes called the sensor nodes. These nodes vary in size. WSNs make use of these sensor nodes which are designed in a special way such that they contain micro-controller to control monitoring, a radio transceiver for generating radio

1.1.2 Network Lifetime

Much of the time the term system lifetime compares to the time when the first hub debilitates its vitality, or when a sure portion of the systems hubs is dead, or notwithstanding when all hubs are dead. In some different cases it might be sensible to quantify the system lifetime by application-specific parameters, for example, the time when the system can no more transfer the video. The significance of a WSN is to be operational and ready to perform its errands amid its utilization. In WSNs, it is essential to augment the system lifetime, which intends to expand the system survivability or to draw out the battery lifetime of hubs.

II. OVERVIEW

Energy/Power Consumption of the sensing device should be minimized since their limited energy resource determines their lifetime. Communication is especially expensive in terms of power. Security components must give exceptional push to be correspondence productive keeping in mind the end goal to be vitality proficient. Giving security over such a system is just as trying. Security instruments must adaptable to vast systems while keeping up high calculation and correspondence productivity. Contingent upon the capacity of the specific sensor arrange, the sensor hubs may left unattended for drawn out stretches of time. Vampire attacks has affected the conventions like connection state, separation vector, source directing, reference point steering and sensor steering.

III. ENERGY DRAINIING ATTACKS ON STATELESS AND STATEFUL PROTOCOL

Vampire attack [1] is an instance of denial of service attack and it can be defined as the alignment and transmission of a message that roots more energy to be expended by the network than if an honest node transmitted a message of similar size to the same destination, though using altered packet headers. The power of the attack can be measured by the ratio of network energy used in the gentle case to the energy used in the malicious case, i.e., the ratio of networkwide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1. Energy used by malicious nodes is not considered since they can always unilaterally drain their own batteries.

These attacks do not disturb immediate availability, but rather work over time to entirely disable a network. But instead work after some time to totally debilitate a system. These kind of attacks are not convention particular, in that they don't depend on outline properties or usage issues of specific directing conventions, yet rather misuse general properties of convention classes. Neither do these attacks depend on flooding the system with a lot of information, however attempt to transmit as meagre information as could be allowed to accomplish the biggest vitality channel, keeping a rate constraining arrangement. Since Vampires use protocol-compliant messages, these attacks are actually difficult to detect and prevent.

3.1 Directional antenna attack

Main cause of vampire attack is directional antenna attack. Vampires have little control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy by restarting a packet in various parts of the network. Using a directional antenna adversaries can deposit a packet in arbitrary parts of the network, while also forwarding the packet locally.

This type can be considered a half-wormhole attack, since a directional antenna establishes a private communication channel, but the node on the other end is not essentially malicious. It can be performed more than once, putting the packet at various distant points in the network, at the extra cost to the opponent for each use of the directional antenna. There are two types of vampire attacks based on this directional antenna attack. They are Stretch attack and carousel attack.

Carousel attack [1]: In carousel attack, an adversary composes packets with purposely introduced routing loops. It sends packets in circles as shown in Fig 3.1. It targets source exploiting so as to direct conventions the constrained confirmation of message headers at sending hubs, permitting a solitary bundle to more than once navigate the same arrangement of hubs.

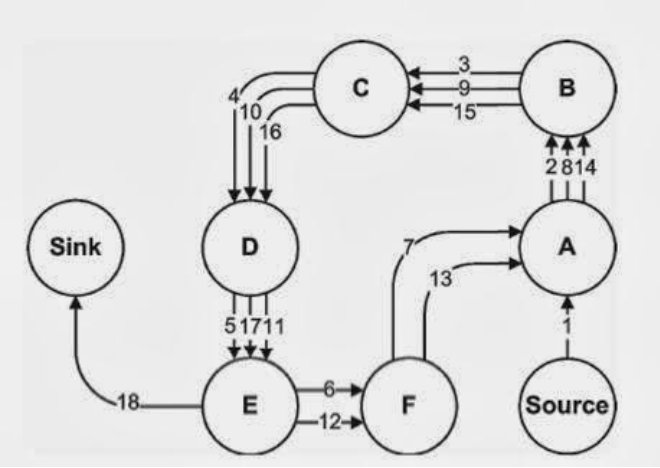

Fig 3.1 A honest node would exit the loop immediately from node E to Sink, but the malicious packets makes its way around the loop twice more before exiting.

Stretch attack [1]: In Stretch attack, an adversary constructs artificially long routes, potentially traversing every node in the network.It expands bundle way lengths, making parcels be prepared by various hubs that is free of bounce number along the most brief way between the enemy and bundle destination. An example is illustrated in Fig 2.

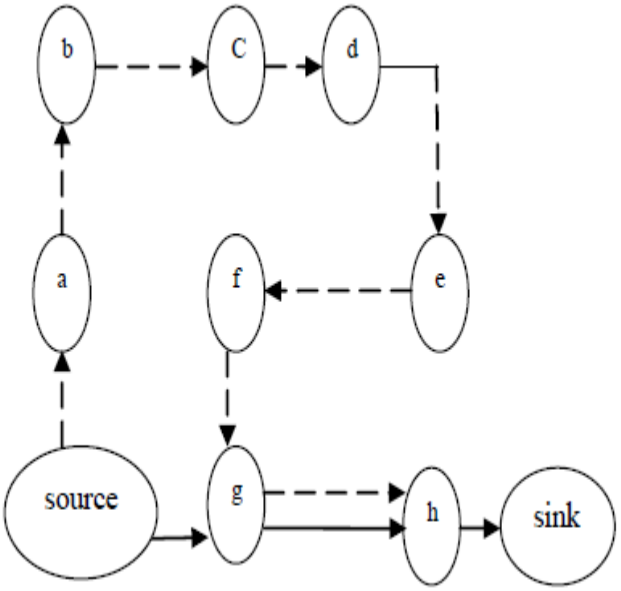

Fig 3.2.Honest node with thick line and malicious node with thin lines.

In a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretchattacks increase energy usage up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or use end-to-end authentication, adversaries are free to replace routes in any overheard packets and assume that only messages originated by adversaries may have maliciously composed routes.

Two important classes of stateful protocols are link-stateand distance-vector. In link-state protocols, such asOLSR [2], nodes preserve a record of the up-or-down state oflinks in the network, and flood routing updates every timea link goes down or a new link is enabled. Distance vector

Protocols like DSDV [11] reserve track of the next hop toeach destination, indexed by a route cost metric, e.g., thenumber of hops. In this scheme, only routing updates thatchange the cost of a given route need to be broadcast.Routes in link-state and distance-vector networks are built dynamically from many autonomous forwardingdecisions, so adversaries have limited power to affectpacket forwarding, making these protocols immune tocarousel and stretch attacks.

In GPSR, a parcel might experience a deadlock, which is a confined space of insignificant physical separation to the objective, yet without the objective really being reachable. The parcel should then be redirected until a way to the objective is accessible. In BVR, bundles are steered toward the signal nearest to the objective hub, and after that move far from the reference point to achieve the objective. Every hub settles on autonomous sending choices, and along these lines a Vampire is restricted out there it can redirect the parcel. These conventions additionally succumb to directional radio wire assaults similarly as connection state and remove vector conventions above, prompting vitality utilization expand component of O(d) per message, where d is the system width. Additionally, GPSR does not consider way length when steering around neighbourhood blocks, thus noxious misrouting might bring about up to a component of O(c) vitality misfortune, where c is the circumference of the obstruction, in loops.

IV. PROBLEM STATEMENT

Design of PLGP(a) – A Clean Slate Routing Protocol to handle the Vampire attacks in Wireless Sensor Networks. The original version of the protocol is vulnerable to vampire attacks. It consists of two phases the topology discovery phase followed by packet forwarding phase. This discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme for the forwarding phase.

4.1 Proposed Methodology

A clean-slate secure sensor network routing protocol by Parno, Luk, Gaustad, and Perrig “PLGP” can be modified to provably resist Vampire attacks during the packet forwarding phase. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, the topology discovery phase is optionally repeated on a fixed schedule to ensure that topology information stays current. Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme as showed in Fig4.1. When discovery begins, each node has a limited view of the network—the node knows only itself. Nodes discover their neighbours using local broadcast, and form ever expanding “neighbourhoods,” stopping when the entire network is a single group.

To preserve no-backtracking, we add a certifiable path history to each PLGP packet. This resulting protocol, PLGP with attestations PLGP(a) uses this history of packet together with PLGP’s tree routing structure so each node can strongly verify progress, averting any important adversarial influence on the path chosen by packet which traverses at least one honest node. Whenever node n forwards packet p, it does this by attaching a non re playable attestation (signature). These signatures form a chain attached to each packet, letting any node receiving it to authenticate its path. Every forwarding node verifies the attestation chain to ensure that the packet has at no time travelled away from its destination in the logical address space.

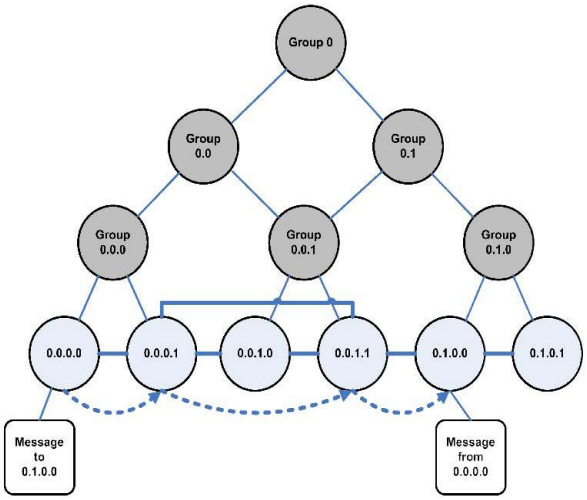

Fig.4. 1. The final address tree for a fully converged six-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that nonleaf nodes are not physical nodes but rather logical group identifiers.

This section shows that the modification of clean slate secure sensor routing protocol [12] is provable security against vampire attack. The real version of this protocol is designed for security but it is vulnerable to vampire attacks. A new valuable secure protocol(VSP) is proposed to prevent vampire attacks consists of following phases.

A. Network Configuring Phase

A network describes a collection of nodes and the links between them. The neighbour group formation process is done by each and every node in the network. This is the process of calculate theneighbour node value and find surrounding node. The neighbour list is maintained by all of nodes in the network. Discovery begins with a time- restricted period during which every node must announce its existence by broadcasting its node ID (Unique Physical Address). Dijikstra's Algorithm is used to calculate the shortest path from a single source to all other nodes.

B. Key Management

This key management process is used for cryptography application during data transfer. Nodes generate a key to communicate with nodes in a group. Generated Key is established to all other nodes in a group. Every packet is encrypted and forwarded along the route. The cryptography technique used to protect the node and data from different kind of attacks. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Compared with the other cryptography, ECC offers a better performance because it can achieve the same security with a smaller key size. It will minimize the number of calculation as well as save the time for nodes. Communication takes place independently by each node in a group.

C. Communication Phase

Communication across a network is performed by secure routing protocol is PLGP In PLGP node cannot able to determine the route to promote the packet. This makes malicious nodes to redirect the packets to any part of the network even if that distance is logically further away from the destination. The same data packets transmitting through the same node repeatedly to deplete the batteries quickly and leads to network death because of vampire. No-backtracking property is introduced to overcome this problem. It implies that for each packet in the protocol execution trace, the number of in-between honest nodes traversed by the packet between source and target is self-determining action of malicious nodes. The malicious node cannot perform carousel or stretch attack. Intelligent adversary may still influence packet progress. To prevent this situation by independently checking on packet movement to the destination. In non-source routing protocol packet routes are controlled by neighbour relationship and routing tree. Every node holds an identical copy of the address tree, and can verify the next logical hop. But this is not sufficient for backtracking.

Algorithm:-

Function secure packet_forward (p)
s - get source address (p);
a – attestation (p);
If(source sig is not verified (p)) or (empty (a) and not is neighbour (s)) then drop (p);
for each node in a a do prevnode – node;
if (not are neighbours (node, prevnode)) or (not making_progress (prevnode, node)) then - drop (p);
c – nearest next node (s); p' – add (p);
if is_neighbor (c) then send (p' ,c);
else forward (p' , next hop to non neighbor (c));

To preserve no-backtracking, we add a certifiable path history to each PLGP packet. This resulting protocol, PLGP with attestations PLGP(a) uses this history of packet together with PLGP's tree routing structure so each node can strongly verify progress, averting any important adversarial influence on the path chosen by packet which traverses at least one honest node. Whenever node n forwards packet p, it does this by attaching a non re playable attestation (signature). These signatures form a chain attached to each packet, letting any node receiving it to authenticate its path. Every forwarding node verifies the attestation chain to ensure that the packet has at no time travelled away from its destination in the logical address space.

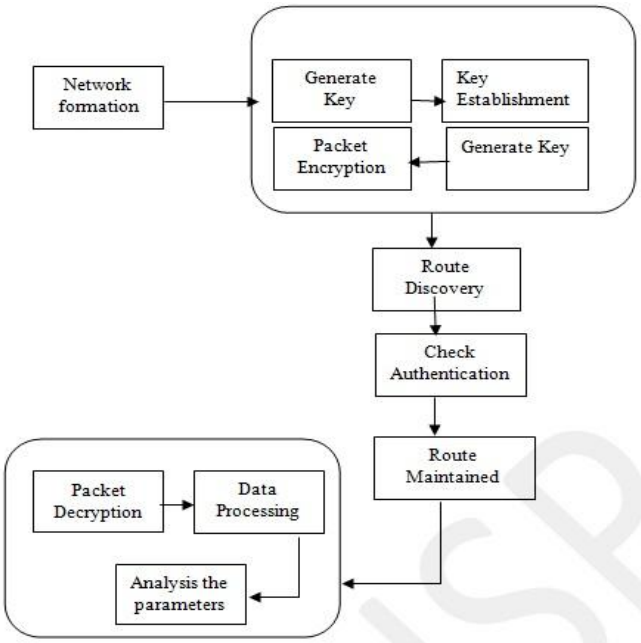

Fig 4.2 shows the data flow diagram of proposed protocol

V. PERFORMANCE EVALUATION

A. Simulation set up We conduct a series of simulations to evaluate the performance of PLGP, and compare with PLGPA with ECC. We unveil the simulation on NS2. The Distributed Coordination Function (DCF) of the IEEE 802.11 protocol is used as the MAC layer protocol. The radio channel model follows a Lucent's WaveLAN with a bit rate of 2 Mbps, and the transmission range is 250 meters. We consider constant bit rate (CBR) data traffic and randomly choose different source-destination connections.

Every source sends four CBR packets whose size is 512 bytes per second. The mobility model is based on the random waypoint model in a field of 1000 m X 1000 m.

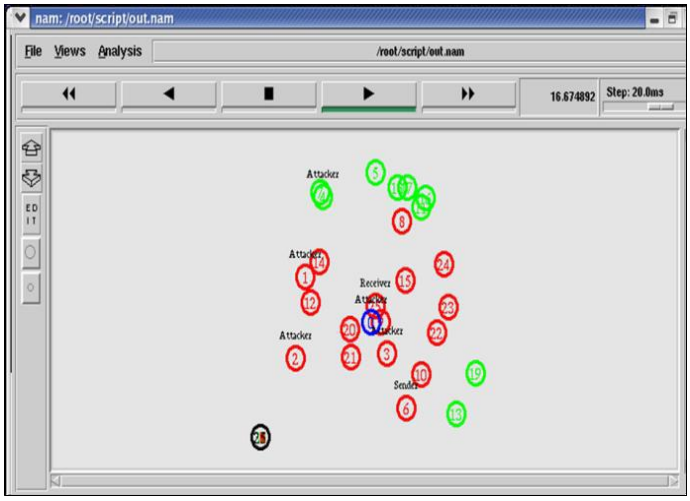

Fig.5.1 shows the attacks in nam output

A Valuable secure protocol is planned to prevent the reparation caused by vampire and reducing the energy usage in a network Evaluate the performance of existing and proposed protocol has been done using ns2 simulator. Fig 6 shows vampire attacks in a randomly generated topology of 30 nodes .Fig 7 shows prevention of vampire attack using PLGPa with ECC model.

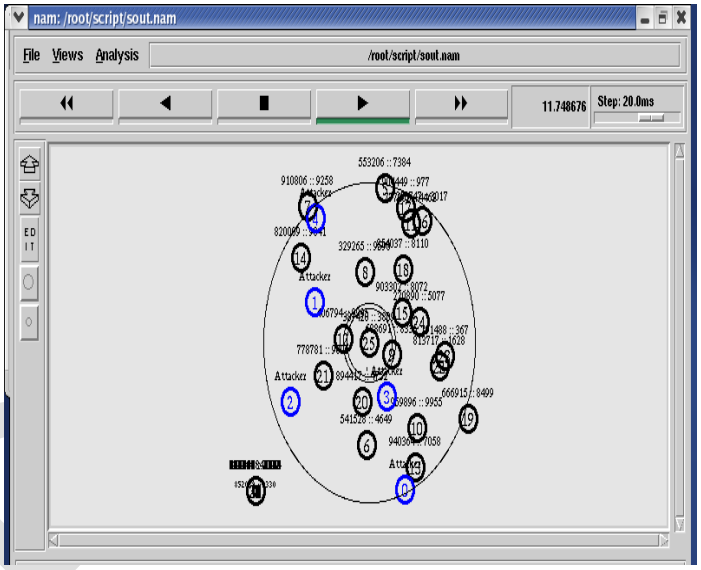

Fig.5.2 shows implementation PLGPa with ECC

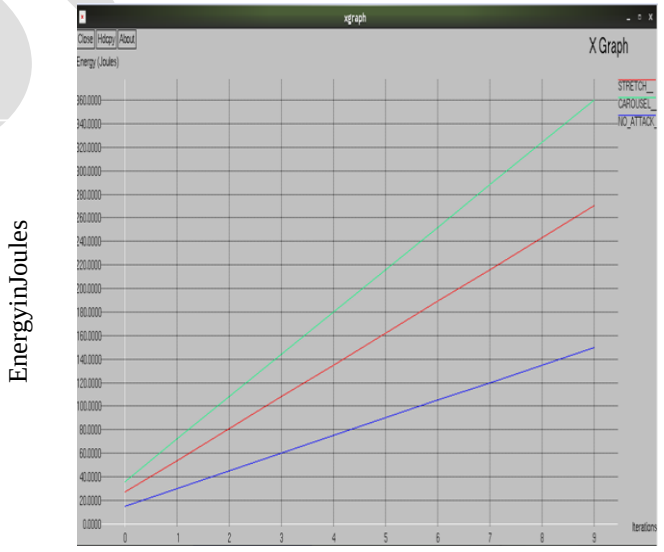

Fig.5.3 shows Energy consumption in case of attacks and no attack

Simulation results shows that PLGPa with ECC reduces the network energy expenditure compare to existing protocol. In Fig 8 each node generate public and private key pair for secure communication the average remaining energy available in a network is more while using PLGPa with ECC

VI. CONCLUSION

Vampire attack, a new class of resource consumption attack that use routing protocols to permanently disable wireless sensor networks by draining nodes battery power. These attacks do not depend on particular protocols or implementations, but rather uncover vulnerabilities in a amount of popular protocol classes. Secure routing protocol PLGPawith ECC is proposed to prevent vampire attacks by verifying that packets make progress towards their destination.

REFERENCES

[1]. I. Aad, J.-P. Hubaux, and E.W. Knightly, ―Denial of Service Resilienc in Ad Hoc Networks,‖ Proc. ACM MobiCom, 2004.

[2]. H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.

[3]. J. Deng, R. Han, and S. Mishra, ―Defending against PathBased DoS Attacks in Wireless Sensor Networks,‖ Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[4]. J. Deng, R. Han, and S. Mishra, ―INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks,‖ Computer Comm., vol. 29, o. 2, pp. 216-230, 2006.

[5]. Eugene Y.Vasserman , Nicholas Hopper, Vampire attack Draining life from wireless ad-hoc sensor networks. IEEE Transactions on Mobile Computing, Vol. 12, No. 2, February 2013

[6]. 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 2002.

[7]. Y.-C. Hu, D.B. Johnson, and A. Perrig, ―Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,‖ Proc. MobiCom, 2002

[8]. 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

[9]. D.B. Johnson, D.A. Maltz, and J. Broch, ―DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks‖Ad Hoc Networking, Addison-Wesley, 2001.

[10]. T.J. McNevin, J.-M. Park, and R. Marchany, ―pTCP: A Client Puzzle Protocol for Defending Against Resource Exhaustion Denial of Service Attacks,‖ Technical Report TR-ECE-04-10, Dept of Electrical and Computer Eng., Virginia Tech, 2004..

[11]. C.E. Perkins and P. Bhagwat, ―Highly Dynamic DestinationSequenced Distance-Vector Routing (DSDV) for Mobile Computers,‖ Proc. Conf. Comm. Architectures, Protocols and Applications,1994.

[12]. B. Parno, M. Luk, E. Gaustad, and A. Perrig, ―Secure Sensor Network Routing: A Clean-Slate Approach,‖ CoNEXT: Proc. ACM CoNEXT Conf., 2006.