VAMPIRE DETECTION IN DATA AGGREGATION PROCESS FOR WSN

Mohamed Ashik. H
M.Phil Scholar, Computer Science
Dr.SNS Rajalakshmi College, Coimbatore
State: Tamilnadu,India

Mrs.Vydehi.S
Assistant Professor & Head
Dr.SNS Rajalakshmi College, Coimbatore
State: Tamilnadu,India

Abstract : Wireless sensor networks have emerged as a new information-gathering paradigm in a wide range of applications, such as medical treatment, battlefield surveillance, emergency response, etc. This paper proposes a new data-gathering mechanism for large-scale wireless sensor networks by introducing mobility into the network. A mobile data collector, for convenience called an M-collector, could be a mobile robot or a vehicle equipped with a powerful transceiver and battery, working like a mobile base station and gathering data while moving through the field. An M-collector starts the data-gathering tour periodically from the static data sink, polls each sensor while traversing its transmission range, then directly collects data from the sensor in single-hop communications, and finally transports the data to the static sink. Deployment of sensor network in hostile environment makes it mainly vulnerable to battery drainage . The motivation of a large portion of research efforts has been to maximize the network lifetime, where the lifetime of network is measured from the instant of deployment to the point when one of the nodes has exhausted its limited power source and becomes in-operational commonly referred as first node failure. But there is a class of resource consumption attack called vampire attack which permanently disables the whole network by quickly draining nodes battery. Forwarding as well as discovery phase of the protocol are considered to avoid an attack. Discovery phase is considered to avoid vampire attack.

Index Terms: Wireless sensor network, Mobility, M-collector, Data sink, Vampire attack.

1. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

source, usually a battery or an embedded form of energy harvesting[1].

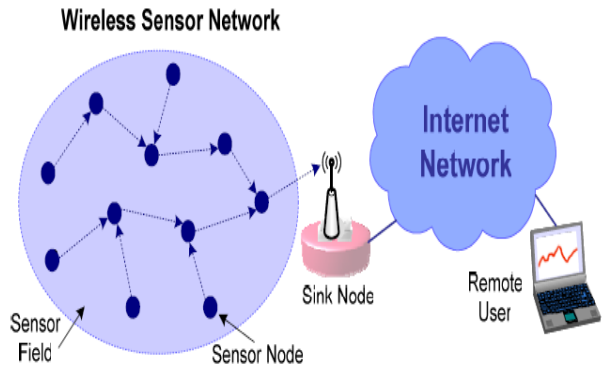

Figure1: Wireless Sensor Network Architecture

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Vampire attack[3] is an instance of denial of service attack and it can be defined as the composition and transmission of a message that causes more energy to be consumed by the network than if a honest node transmitted a message of identical size to the same destination, although using different packet headers. The strength of the attack can be measured by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide 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 disrupt immediate availability, but rather work over time to entirely disable a network. This type of 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. Neither do these attacks rely on flooding the network with large amounts of data, but try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

2. RELATED WORK

Sensor nodes observe and sense the phenomenon with a sensing module, process the data with a computing module, and send the data to a required destination over a radio interface with a communication module. A various survey has been carried out for the power consumption in the wireless sensor networks. Several energy management schemes have been proposed in the literature survey.

In [42] Y.T. Hou, Y. Shi and S.F. Midkiff Proposed a method for Prolonging Sensor Network Lifetime with Energy Provisioning and Relay Node Placement. Wireless sensor networks [4] that operate on batteries have limited network lifetime. There have been extensive recent research efforts on how to design protocols and algorithms to

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

prolong network lifetime. However, due to energy constraint, even under the most efficient protocols and algorithms, the network lifetime may still be unable to meet the mission's requirements. This paper considers the energy provisioning problem for a two-tier wireless sensor network. In addition to provisioning additional energy on the existing nodes, This paper consider deploying relay nodes (RNs) into the network to mitigate network geometric deficiency and prolong network lifetime. Formulate the joint problem of energy provisioning and relay node placement (EP-RNP) into a mixed-integer nonlinear programming (MINLP) problem. Since an MINLP problem is NP-hard in general, and even the state-of-the-art software and techniques are unable of offer satisfactory solutions, This paper develop a heuristic algorithm, called SPINDS, to address this problem. A number of novel algorithmic design techniques in the design of SPINDS that effectively transforms a complex MINLP problem into linear programming (LP) problems without losing critical points in its search space. Through numerical results, this paper shows that SPINDS offers very attractive solution and some important insights to the EP-RNP problem.

In [2] Jae-Hwan Chang and Leandros Tassiulas introduces new method for Maximum lifetime routing in wireless sensor networks. A routing problem in static wireless ad hoc networks is considered as it arises in a rapidly deployed, sensor based, monitoring system known as the wireless sensor network. Information obtained by the monitoring nodes needs to be routed to a set of designated gateway nodes. In these networks, every node is capable of sensing, data processing, and communication, and operates on its limited amount of battery energy consumed mostly in transmission and reception at its radio transceiver. Assume that the transmitter power level can be adjusted to use the minimum energy required to reach the intended next hop receiver then the energy consumption rate per unit information transmission depends on the choice of the next hop node, i.e., the routing decision.

This paper formulate the routing problem as a linear programming problem, where the objective is to maximize the network lifetime, which is equivalent to the time until the network partition due to battery outage. Two different models are considered for the information-generation processes. One assumes constant rates and the other assumes an arbitrary process. A shortest cost path routing algorithm is proposed which uses link costs that reflect both the communication energy consumption rates and the residual energy levels at the two end nodes. The algorithm is amenable to distributed implementation. Simulation results with both information-generation process models show that the proposed algorithm can achieve network lifetime that is very close to the optimal network lifetime obtained by solving the linear programming problem [2].

In [5] Stephanie Lindsey, Cauligi Raghavendra,Krishna M. Sivalingam introduces Data Gathering Algorithms in Sensor Networks Using Energy Metrics. Sensor webs consisting of nodes with limited battery power and wireless communications are deployed to collect useful information from the field. Gathering sensed information [5][10] in an energy efficient manner is critical to operating the sensor network for a long period of time. In a data collection problem is defined where, in a round of communication, each sensor node has a packet to be sent to the distant base station. There is some fixed amount of energy cost in the electronics when transmitting or receiving a packet and a variable cost when transmitting a packet which depends on the distance of transmission. If each node transmits its sensed

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

data directly to the base station, then it will deplete its power quickly.

3.PROPOSED WORK

Vampire attack[3] is an instance of denial of service attack and it can be defined as the composition and transmission of a message that causes more energy to be consumed by the network than if a honest node transmitted a message of identical size to the same destination, although using different packet headers. The strength of the attack can be measured by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide 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 disrupt immediate availability, but rather work over time to entirely disable a network. This type of 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. Neither do these attacks rely on flooding the network with large amounts of data, but try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

3.1 Directional antenna attack

Main cause of vampire attack is directional antenna attack [3][6]. 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. There are two types of vampire attacks based on this directional antenna attack. They are Stretch attack and carousel attack.

3.1.1 Carousel Attack

In carousel attack[3], an adversary composes packets with purposely introduced routing loops. It sends packets in circles and it targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.

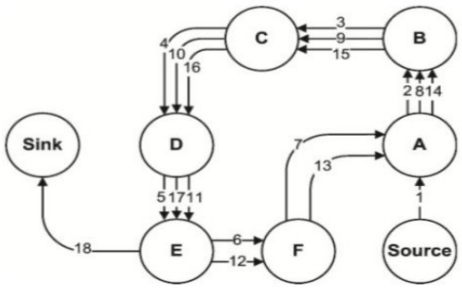

Figure 2: Carousel Attack

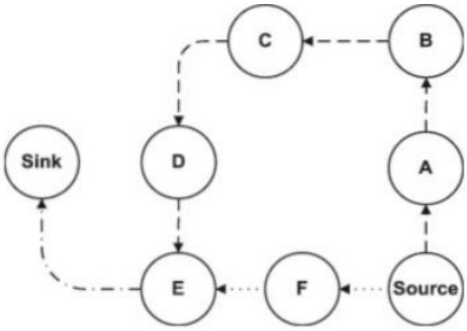

Figure 3: Stretch Attack

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

3.1.2 Stretch Attack

In Stretch attack[3], an adversary constructs artificially long routes, potentially traversing every node in the network. It increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.

3.2 Clean-State Sensor Network

A clean-state secure sensor network[3] routing protocol is an efficient, highly resilient to active attacks. This protocol is introduced by Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig(PLGP from here on). It has two phases, they are topology discovery phase and packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to Vampire attacks. Here PLGP can be modified to provably resist. Vampire attacks during the packet forwarding phase.

3.2.1 Topology Discovery

Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. 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. Throughout this process, nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing. Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key, signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0.

3.2.2 Packet Forwarding

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originators address as shown in figure. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Thus every forwarding event (except when a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

3.3 Algorithm Description

PLGP with attestations[3] (PLGPa) uses this packet history together with PLGPs tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, it this by attaching a non replayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space. Following function Secure _forward _packet(p) defines the modified protocol.

3.3.1 Light Weight PLGP Based Method

Light Weight Scheme is mainly focused on avoiding vampire attacks in the discovery phase of PLGP by checking signal strength of the nodes which transmit the group joining messages. A vampire would send high energy

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

signal so as to suppress the group joining messages of other node. So avoid a node which sends at high signal strength.

Following function modified discovery phase(node) defines this concept.

```
if ( transmit_power(node) > THRESHOLD )
then
return /*drop(node)*/
else
insert_into_routingtable(node)
end if
```

In this novel method the attestation process is as shown below:

1.Encrypt the message using a secret key, then the packet includes encrypted data, cost of the operation, sender's identity (A). The whole data are encrypted with private key of A then this packet send to B as in previous case.

ENC((Msg)Prk,4,A)PrA == X =) B

2.When B receives the packet decrypts it and retrieves the encrypted message only. After retrieving the encrypted message B then includes the path information along with the updated cost into the packet. These whole informations are encrypted with B's private key and send to C.

B =) DEC(X)PA =) ENC((Msg)Prk,3,AB)PrB == Y =) C

3.When C receives the packet, above process will repeat as shown below:

C=) DEC(Y)PB =)ENC((Msg)Prk,2,ABC)PrC == Z =) D

D=)DEC(Z)PC=)ENC((Msg)Prk,1,ABCD)PrD =) D

Based on these concepts Secure_forward_packet(p) can be modified as shown below.

Algorithm: Modified_forward_packet(p)

```
s←extract_source_address(p)
a←extract_attestation(p)
if (not verify_source_sig(p)) or (empty(a) and
not is_neighbour(s)) or (not saowf_verify(a))
then
return /*drop(p)*/
prevnode ← node
if (not are_neighbours(node,prevnode)) or (not
making_progress(prevnode,node))
then
return /*drop(p)*/
end if
end if
c ← closest_next_node(s)
p← saowf_append(p)
if (is_neighbours(c)) then
forward(P,c)
else
forward (P,next_hop_to_non_neighbour(c))
end if
```

The packet is moved from one node to another node with secure signature.

4. SIMULATION RESULTS ANALYSIS

Simulation tool for wireless sensor networks [7] are increasingly been used to study sensor webs and to test new applications and protocols in this evolving research field. However, it requires a suitable model based on solid assumptions and an appropriate framework to ease implementation. In addition, simulation results rely on the particular scenario under study (environment), hardware and physical layer assumptions, which are usually not accurate enough to capture the real behavior of a WSN. In this section the results of the simulation analysis is performed.

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

Node deployment: Initially node, Mobile collector and Base station is declared in the network simulator. Then vampire node initialized (which spend high energy).

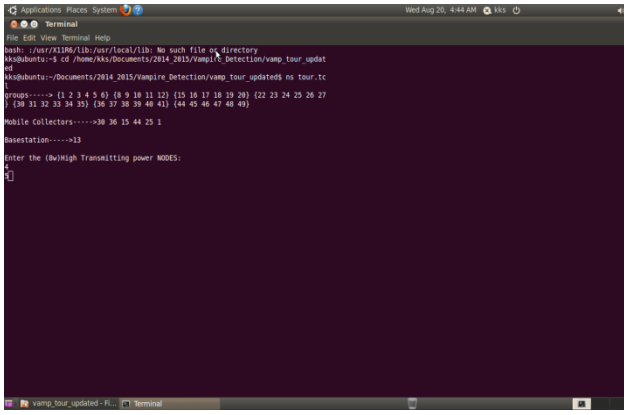

Figure 4: Node Initialization.

Deployment of M-collector and Base station:

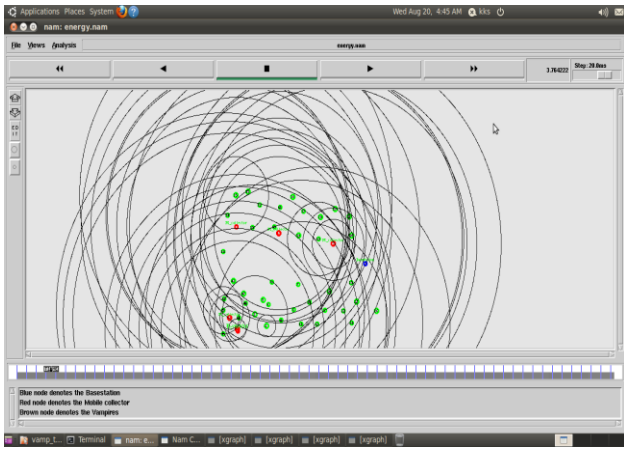

Figure 5: M-collector and Base Station Deployment.

M-collector: It will receive the data from the node in wireless environment. Which like moving vehicle containing receiving equipment. After gathering data from the node, M-collector will send it to the base station. M-collector will move periodically.

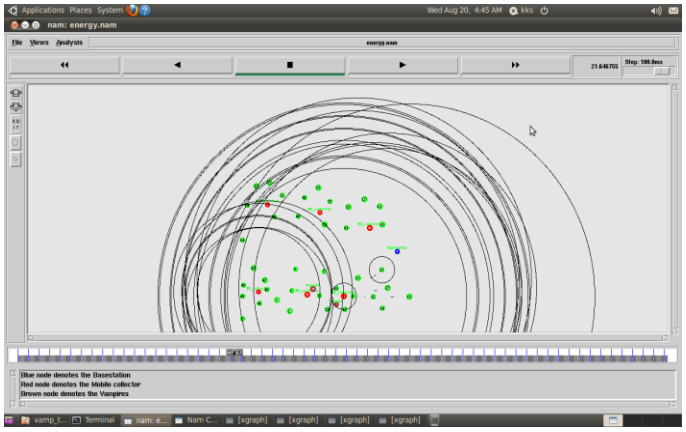

Figure 6: Vampire Detection

Vampire Detection: At the time of data transmission, adversary node will broadcast to high level, so it will drain more energy than the honest node. Brown color node denote the vampire node.

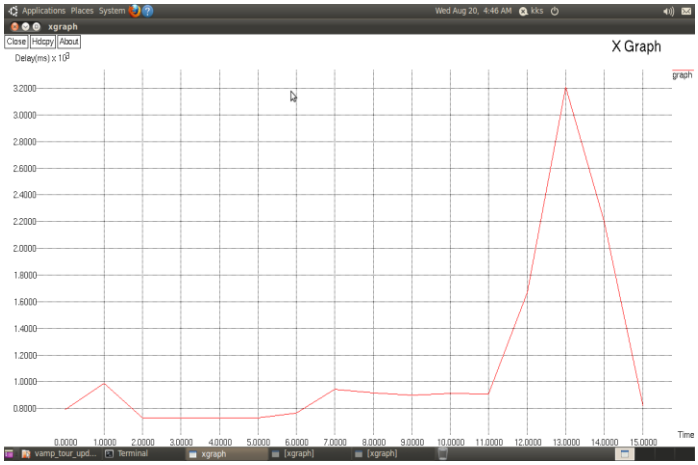

Figure 7: Delay Calculation Graph

Delay Calculation Graph: Delay will be calculated by this graph. If the vampire is active at particular time, the delay will be high.

5. CONCLUSION

The Wireless Sensor Network is an emerging area which has wide applications. . An M-collector starts the data-gathering tour periodically traverses the entire sensor network and gathers the data from sensors one by one,

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

and finally returns and uploads data to the data sink. Hence the security in wireless sensor network is of great concern. Vampire attacks are important attack against a wireless sensor network in which an adversary develop and transmit messages that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. So it is very important to detect the vampire nodes as early as possible.

Here Lighweight PLGPa protocol is used to employ the vampire attacks. Since Lighweight PLGPa has two phases vampire node detection is also done in this two phases. The novel algorithm is the first sensor network routing protocol that provably bounds the damage from vampire attack in two phases of Lighweight PLGPa. This method reduces the energy utilization, packet overhead, encryption efforts etc.

Here only Lighweight PLGPa protocol is considered, how the proposed solution works in other routing protocol is not considered and how to reproduce the energy at the draining stage is also not considered. This method can be further extended to determine this problem.

REFERENCES

[1] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proc. ACM Int.Workshop Wireless Sens. Netw. Appl.*, Atlanta, GA, Sep. 2002, pp. 88–97.

[2] Jae-Hwan Chang and Leandros Tassiulas, "Maximum lifetime routing in wireless sensor networks", IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[3] Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.

[4] Laura M. Feeney, An energy consumption model for performance analysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001), no. 3.

[5] Stephanie Lindsey, Cauligi Raghavendra,Krishna M. Sivalingam, (2002)," Data Gathering Algorithms in Sensor Networks Using Energy Metrics", IEEE Transactions On Parallel And Distributed System, Volume 13, No.9, September 2002.

[6] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Networks", IEEE transactions on parellel and distributed systems, VOL. 12, NO. 2, February 2011

[7] Stankovic, A., "Wireless Sensor Networks", University of Virginia Charlottesville. (2006).

[8] Luis, J., Ana Lucila, S., Alicia, T., Cabrera, S., and Barenco Abbas, C.J., (2009), "Routing Protocols in Wireless Sensor Networks", *Sensors* 2009.

[9] Ming Ma, Yuanyuan Yang, Miao Zhao(2013)," Tour Planning for Mobile Data-Gathering Mechanisms in Wireless Sensor Networks", IEEE Transactions On Vehicular Technology, Volume 62,No 4,May 2013.

[10] Garcia-Hernandez, C.F., Ibargüengoytia-González, P.H., Garcia-Hernandez, J., and Pérez-Díaz, J.A., (2007), "Wireless Sensor Networks and Applications: a Survey", International Journal of Computer Science and Network Security, Vol.7, No.3.

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR

[11] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E., (2002), "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, pp.102-114.

[12] S. Chessa and P. Santi, "Crash faults identification in wireless sensor networks," *Comput. Commun.*, vol. 25, no. 14, pp. 1273–1282, Sep. 2002.

[13] L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in *Proc. ACM MobiCom*, 2001, pp. 151–165.

[14] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet," in *Proc. ASPLOS*, 2002, pp. 96–107.

[15] C. Ma and Y. Yang, "A battery-aware scheme for routing in wireless ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3919– 3932, Oct. 2011.

[16] T. Small and Z. Haas, "The shared wireless infostation model—A new ad hoc networking paradigm (or where there is a whale, there is a way)," in *Proc. ACM MobiHoc*, 2003, pp. 233–244.

[17] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, and P. Corke, "Data collection, storage and retrieval with an underwater sensor network," in *Proc. ACM SenSys*, 2005, pp. 154–165.

[18] A. Chakrabarty, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of a sensor network," in *Proc. 2nd Int. Workshop IPSN*, Apr. 2003, pp. 129–145.

[19] W. Wang, V. Srinivasan, and K. C. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proc. ACM Mobicom*, Aug. 2005, pp. 270–283.

[20] I. Slama, B. Jouaber, and D. Zeghlache, "Multiple mobile sinks deployment for energy efficiency in large scale wireless sensor networks," *e-Bus. Telecommun., Commun. Comput. Inf. Sci.*, vol. 48, no. 5, pp. 412–427, 2009.

[21] H. Lee, M. Wicke, B. Kusy, O. Gnawali, and L. Guibas, "Data stashing: Energy-efficient information delivery to mobile sinks through trajectory prediction," in *Proc. ACM IPSN*, 2010, pp. 291–302.

[22] Tapalina Bhattasali, Rituparna Chaki, Sugata Sanyal ,(2012)," Sleep Deprivation Attack Detection in Wireless Sensor Network", *International Journal of Computer Applications, Volume 40– No.15, February 2012.*

[23] E. Ekici, Y. Gu, and D. Bozdag, "Mobility-based communication in wireless sensor networks," *IEEE Commun. Mag.*, vol. 44, no. 7, pp. 56–62, Jul. 2006.

[24] X. Xu, J. Luo, and Q. Zhang, "Delay tolerant event collection in sensor networks with mobile sink," in *Proc. IEEE INFOCOM*,Mar. 2010, pp. 1–9.

ISSN: 2278 – 7798 All Rights Reserved © 2014 IJSETR