Eloa Beside Vampire Attacks in Wireless Sensor Networks

[1]P.Geeta Prasanthi, [2] P.Seshu Babu

[1] Pursuing M.Tech in CSE Department
[2] Assistant Professor, Dept of CSE,
Vignan University, Vadlamudi, Guntur, Andhra PradeshIndia

Abstract:

Wireless Sensor Networks in today's world are the basic means of communication. An ad hoc network is a group of wireless nodes, in which each node can communicate over multihop paths to any other node without the help of any preexisting infrastructure such as base station or access points. Owing to these feature ad hoc low power wireless networks are capable of sensory and pervasive computing which forms the wireless ad hoc sensor network. The limitations of system are resources like battery power, communication range and processing capabilities. One of the major challenges in Wireless Sensor Networks is the security concerns. The attacks affecting these systems are increasing as they progress. One of the resource depletion attacks called vampire attacks are the major concern. They not only affect a single node but they bring down the entire system draining the power i.e. Battery power. In this paper, the system proposed overcomes this challenge by using the Energy load observing Algorithm (ELOA) and the energy consumption is reduced to a great-extend.

Keywords: Wireless Sensor Networks, Routing; Attacks; Security; Energy consumption; Energy load observing Algorithm (ELOA)

1. INTRODUCTION

A network is composed of nodes each of which has computing power and can transmit and receive message over communication links, wireless or cabled. In Wireless networks each node use radio signal to communicate with other nodes. A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. The basic characteristic of ad-hoc sensor network is the communication among nodes of network without any pre-existing infrastructure. Wireless Ad hoc Sensor Network have become very essential in communication environment. Due to distributed nature of these networks and their deployment in remote areas, these networks are Susceptible to several security threats that can adversely affect their proper functioning. Ad hoc sensor network guarantees pervasive computing, instantly deployable communication for military and continuous connectivity, for creating a new application in future.

Resource constrains is one of the main characteristic of a Wireless sensor networks

Simplicity in WSN with resource constrained nodes makes them very much vulnerable to denial of service [1], attacks on routing infrastructure, and reduction of quality attacks. Routing techniques are required for sending data between sensor nodes and base station for communication. There are many ways to classify the routing protocols. Almost all of the routing protocols can be classified as data-centric, hierarchical and location based according to the network structure. In data-centric routing all nodes are typically assigned equal roles or functionality. In hierarchical-based routing however, nodes will play different role in the network. In location based routing sensor node's positions are exploited to route data in the network. The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The

Wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks. Developing energy-efficient routing protocol on wireless sensor networks is one of the important challenges. Therefore, a key area of WSN research is to develop a routing protocol that consumes low energy.

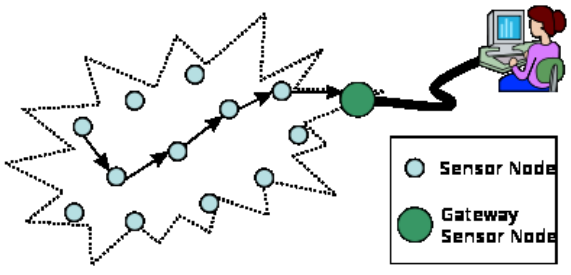

Figure 1..wireless sensor network

Unfortunately, current routing protocols suffer from many security vulnerabilities. Already many solutions have been proposed to defend attack that live for short duration on the network [3][4]. But these solutions do not defend permanent resource depletion attack. The battery power consumption attacks at routing layer protocol to completely disable networks, by depleting node's battery power and it is defined as vampire attacks. These attacks never flood the network with large amount of data instead it drains node's life by delaying the packets. Protocols such as SEAD[6], Ariadne[7], SAODV[13]are securely designed but do prevent the vampire attacks Existing security scheme are limited to other layers such as medium access control or application layers but not to the routing layer to secure vampire attacks[5]. In section 2 energy draining attacks in source routing protocol is reviewed. In section 3 evaluation of energy draining attacks on stateless and stateful routing protocol. In section 4 *Energy load observing Algorithm (ELOA)* against vampire attacks are discussed. In section 5 Simulation Results. In section 6 Concussion.

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 mechanisms must give special effort to be communication efficient in order to be energy efficient. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency. Depending on the function of the particular

sensor network, the sensor nodes may be left unattended for long periods of time. Vampire attack has influenced the protocols like link state, distance vector, source routing, beacon routing and sensor routing . In source routing protocol a malicious source can construct a route that leads to (a) carousel attack and (b) stretch attack. In carousel attack an adversary forms a
loop for routing packets as shown in Fig.2

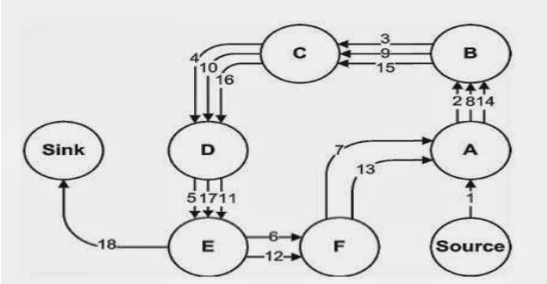

Fig 2. Carousal attack

Many methods are analyzed to limit the damage caused by vampire attack. The first mechanism considered to protect these attacks is loose source routing, in which any forwarding node can reroute the packet if it knows a shortest path to the destinations. In second attempt to modify the protocol (PLGP) from [12] to guarantee that a packet makes progress through the network. This is called as No- backtracking property, because it holds if and only if a packet is moving strictly closer to destination with every hop. No-backtracking is not satisfied in case of non source routing protocol. To preserve no-backtracking property add a verifiable path history to the packet. Elliptic curve cryptography technique is used to verify the packet comes originate from authorize node.

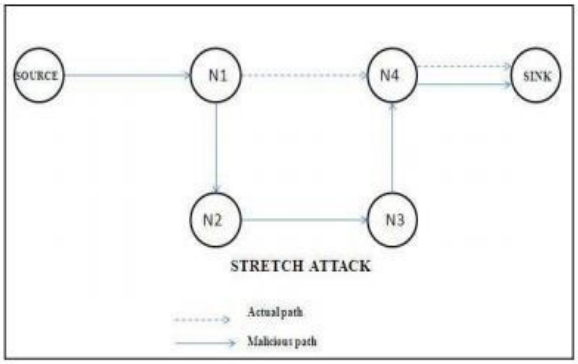

Fig 3. Stretch attack

In our second attack, likewise focusing on source routing, an opponent builds misleadingly long courses, conceivably crossing each node in the network. We depict this stretch attack, since it builds packet way lengths, bringing on correspondence to be prepared by various nodes that is autonomous of bound tally along the briefest way between the opponent and bundle objective

III. ENERGY DRAINIING ATTACKS ON STATELESS AND STATEFUL PROTOCOL

.

The fardel is on the source to ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop. Both the carousel and stretch attacks are evaluated in a randomly generated 30-node topology. It causes delay as well as increase communication overhead and energy consumption in
resource limited networks .The effect of denial or degradation of service on battery life and other finite node resources has not generally been a considered securely.

***1) Carousel attack*:** In this attack, a malicious node forward a packet with a route included a chain of loops, such that the packets traverse several times in the same route. This strategy can be used to increase the route length beyond the number of nodes in the network an example of this type of route is in Fig.4 the thick path shows the honest path and thin shows the malicious path.

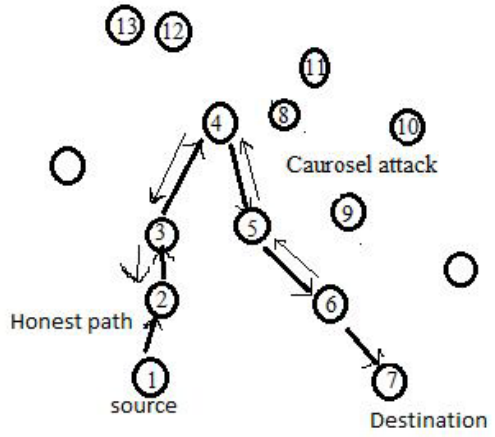

Fig.4 *Carousel attack*: Thick path shows the honest path and thin shows the malicious path.

2) Stretch attack: Another attack in the same layer is the stretch attack, where a malicious node constructs falsely long source routes, causing packets to traverse a longer than optimal number of nodes. In this example given below honest path shown with thick lines and adversary or malicious path with thin lines. The honest path is very less distant but the malicious path is very long to make more energy consumption. Per-node energy usage under both attacks. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected.

In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks drastically network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10 percent of their total energy reserve per message.Two important classes of stateful protocols are linkstate and distance-vector. In link-state protocols, such as OLSR [2], nodes keep a record of the up-or-down state of links in the network, and flood routing updates every time a link goes down or a new link is enabled. Distance vector protocols like DSDV [11] keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated. Routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions, so adversaries have limited power to affect packet forwarding, making these protocols immune to carousel and stretch attacks.

In GPSR, a packet may encounter a dead end, which is a localized space of minimal physical distance to the target, but without the target actually being reachable. The packet must then be diverted until a path to the target is available. In BVR, packets are routed toward the beacon closest to the target node, and then move away from the beacon to reach the target. Each node makes independent forwarding decisions, and thus a Vampire is limited in the distance it can divert the packet. These protocols also fall victim to directional antenna attacks in the same way as link-state and distance-vector protocols above, leading to energy usage increase factor of O(d) per message, where

d is the network diameter. Moreover, GPSR does not take path length into account when routing around local obstructions, and so malicious misrouting may cause up to a factor of O(c) energy loss, where c is the circumference of the obstruction, in hops.

IV. ENERGY LOAD OBSERVING ALGORITHM (ELOA) AGAINST VAMPIRE ATTACKS

This section focuses on the design details of our proposed protocol ELOA. Where energy of a node gets to threshold level it plays a vital role by performing energy intensive tasks there by bringing out the energy efficiency of the sensors and rendering the network endurable. This pattern based on the energy levels of the sensors.

ELOA functions two phases namely.

1. Network configuring phase
2. Communication phase

1. *Network configuring phase*: The goal of this phase is to establish an optimal routing path from source to destination in the network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication.

In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node upon receiving this stored in its routing table to facilitate further computations

Now the node establishes the routing path, first the traces the next node by computing the energy required to transmit the required data packet that is suitable energy node and less distant node selected as the next forwarding node in this way it establishes the route from source to destination with suitable energy and less distant.

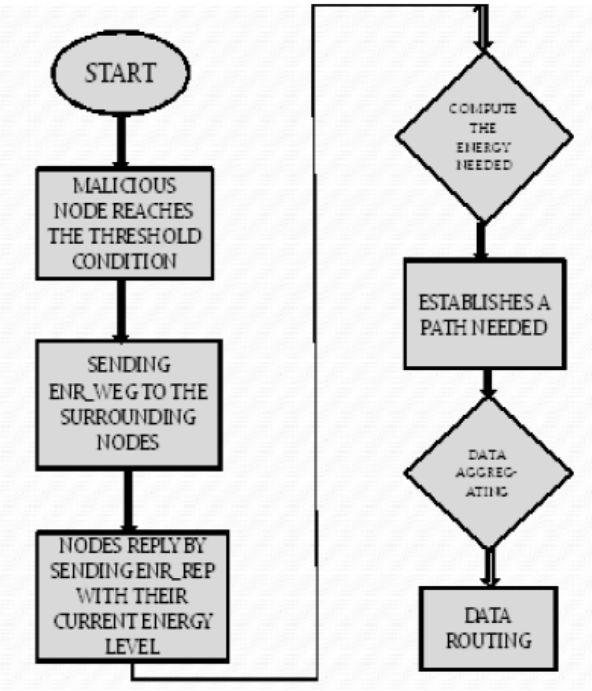

Fig 5. ELOA

Thus energy spent by the allotted node suitable to the data packet sent from the node in this way this algorithm avoids data packet dropping and this allotted forwarding node transmits the packets safely to the destination. This algorithm gives prime importance to achieve balancing of load in the network. The suitable energy node will be assigned as a forwarding node as long as this node as this node has the capacity to handle. In this way a multi hop minimal less distant path is established to bound the network damage from vampire attack.

EWMA avoids the collapsing of entire network by dropping the packets in the network. The load is evenly balanced

depending upon the capacity of the nodes. In this way multi hop load balanced network is achieved.

2. *Communication Phase:* The main job of communication phase is to avoid the same data packets transmitting through the same node repeatedly to deplete the batteries vastly and leads to network death because of vampire 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 copying the content of the packet that is transmitting through the node. This copied content compares 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 protects the depletion of batteries ghastly. Then send the required data packets through the established node safely to the destination.

V. SIMULATION RESULTS

The simulation environment is implemented in the NS-2, a network simulator that provides support for simulating wireless networks

Detection of Vampire Attack

We have evaluated both the carousel and stretch attack. A randomly generated 10 node topology for carousel attack and 16 node topology for stretch attack is taken. A single randomly selected malicious AODV agent, using ns2 network simulator is evaluated. The total energy set is 10J. For the stretch attack the energy consumed by the system is 4.37960 J and for the carousel attack the power consumption is 4.625225 J.

The energy calculated is given by the formula:

$$\text{Energy consumed} = \frac{EI - EF}{EI} \quad (1)$$

EI - Initial Energy

EF - Final Energy

The initial value in both the cases is assumed to be 10J. The simulation is done for 10ms. The data is transmission begins at 5ms and ends at 10ms.

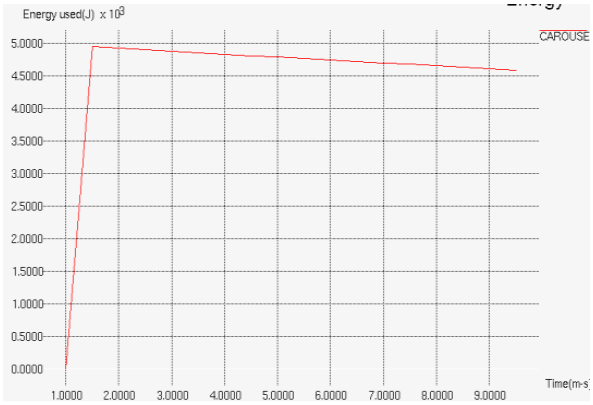

Fig 6. Energy consumption in carousel attack

Figure 6 shows the energy consumption during a carousel attack where the x axis is taken as the Time (ms) and the y axis is taken as the Energy (J) used that is done by the formula mentioned earlier. Energy consumption is 4.37960J for every 10J. Since the initial energy is 10J the peak rises above and then gradually decreases with the transmission of data and in the presence of carousel attack.

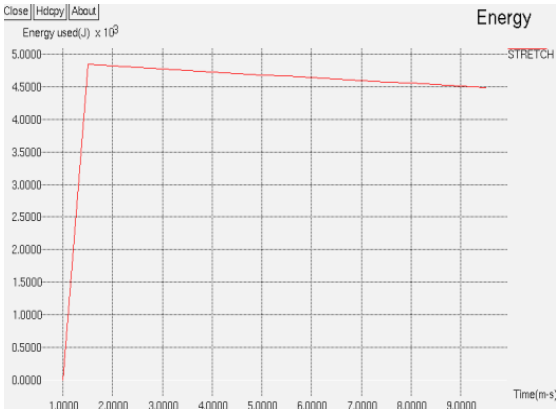

Figure 7 Energy consumption in stretch attack

Figure 7 shows the energy consumption in stretch attack where the x axis is taken as the Time (ms) and the y axis is taken as the Energy (J) used. The energy consumption in this case is 4.625225J for every 10 J. This value increases with the increase in number of nodes.

Mitigation of Vampire Attacks

After using the ELOA algorithm the simulation is repeated for the same values.

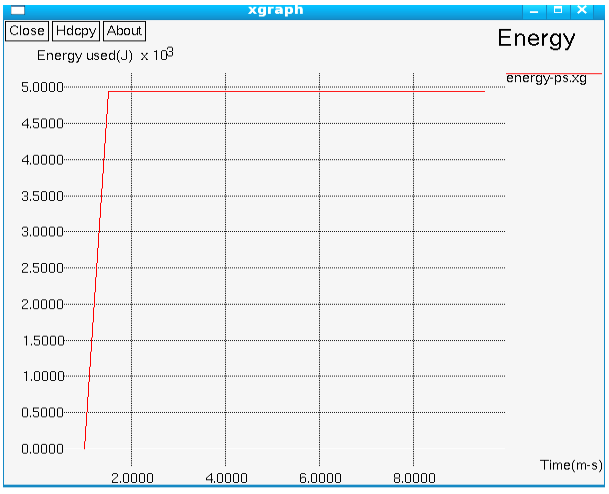

Fig 8 Mitigation of Carousel attack

Figure 8 shows the mitigation of carousel attack. From the analysis of the graph mentioned below the energy consumption is stable.

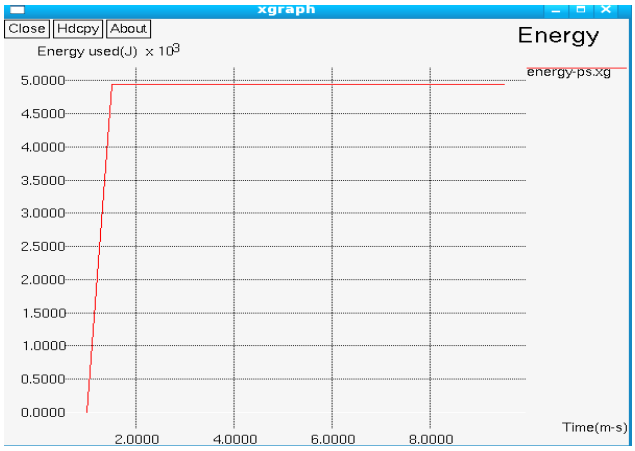

Fig 9 Mitigation of Stretch attack

In figure 9 the mitigation of stretch attack is shown. These analysis show that in case of an adversary present they lead to the death of the nodes energy. But with ELOA we can increase the lifetime of the nodes. This concept increases the overall lifespan of the network by choosing the energy efficient routing path.

VI.CONCLUSSION

A new class of energy draining attacks that use routing protocols to permanently halt ad hoc wireless sensor networks by depleting nodes' battery power. Vulnerabilities exposed in existing protocols are evaluated. Performance of existing protocols is quantified using small number of adversaries in a randomly generated 30 node topology. Simulation results show the network energy expenditure. The system proposed overcomes this challenge by using the Energy load observing Algorithm (ELOA) and the energy consumption is reduced to a great-extend in order 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 Path-Based 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 Destinationn-Sequenced 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.

[13] M.G. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. First ACM Workshop Wireless Security,2002

[14] F. Ye, H. Luo and S. "Statistical En-Route Filtering of Injected False Data in Sensor Networks," IEEE Journal on Selected Areas in Communication, vol. 23, No.4, 2005, pp.839-850.

[15] Gergely Acs, Levente Buttyan, and Istvan Vajda, "Provably secure on-demand source routing in mobile ad hoc networks", IEEE Transactions on Mobile Computing 05 (2006), no. 11.

[16] Guang Yang, M. Gerla, and M.Y. Sanadidi, "Defense against low-rate TCP-targeted denial-of-service attacks", ISCC, 2004.

[17] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[18] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, "Denial of service resilience in ad hoc networks", MobiCom, 2004.

[19] J. R. Douceur, "The Sybil Attack," in 1st international Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[20] J. Bruck, J. Gao, and A. Jiang, "Localization and Routing in Sensor Networks by Local angle Information", ACM Mobihoc, May 2005

[21] J. Deng, R. Han, and S. Mishra, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol 12. 4, pp. 609-619, Aug.2004

[22] J.Hill, R.Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in Preceedings of ACM ASPLOS IX, November 2000.

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

[24] L. Buttyan, et al., "Statistical Wormhole Detection in Sensor Networks," Lecture Notes in Computer Science Vol. 3813, 2005, pp. 128-141.

[25] L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6,November/December 1999

[26] M. Tubaishat and S. Madria, "Sensor Networks: An Overview," IEEE Potentials, Vol. 22, No. 2, 2003, pp. 20-23.

[27] M. McLoone and M. Robshaw, "Public Key Cryptography and RFID Tags," Proc. RSA conf. Cryptography, 2006

[28] Manel Guerrero Zapata and N. Asokan, "Securing ad hoc routing protocols", WiSE, 2002

[29] Tuomas Aura,"Dos-resistant authentication with client puzzles", International workshop on security protocols, 2001

[30] V Paxson, "An analysis of Using Reflectors for Distributed Denial-of-service Attacks", SIGCOMM Computing comm. Vol 31, no 3, pp38-41, 2001

[31] V. Vijaya Raja, R. Rani Hemamalini, and A. Jose Anand, "Multi Agent System Based Upstream Congestion Control in Wireless Sensor Network", 2011

[32] Y.C, Hu, A.Perrig, and D.B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep TR01-384, June 2002.

[33] 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 and Applications, 2002.

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