International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 9, 2017 ISSN: 2348-6600
Reference ID: IJCS-200 PAGE NO: 1228-1237

Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

SURVEY ON DOS ATTACKS AND ITS PREVENTION PROTOCOLS IN IN WSN

Dr.A.MariMuthu[1] N.Geetha Lakshmi[2]

HOD & Associate Professor, Dept. of Computer Science ,Govt.Arts& Science College, Coimbatore[1]
Research Scholar, Department of Computer Science, Karpagam University, Coimbatore[2]

ABSTRACT- Wireless ad-hoc sensor network is increasing popularity in all organization and it is useful for communication. Wireless ad-hoc sensor network is vulnerable to Denial of Service (DOS) attack. The network resources are unavailable to users due to DOS attack. In DOS attack affects the node to consume more battery power and degrades the network performance. Various techniques are used for detection and prevention of DOS attack such as spread spectrum, Secured lightweight Mechanism, packet leash and energy weight monitoring system but DOS attack cannot fully prevented using this techniques. The paper reviews various types of DOS attacks and its Detection techniques.

Keywords— ad-hoc sensor network, Denial of Service (DOS) attack.

I. Introduction

Wireless sensor networks can be considered as a special type of ad hoc wireless networks, and there are already some proposals addressing security in general ad hoc networks, but sensor networks have some additional concerns that limit the applicability of those traditional security measures. Sensor networks are very limited in local memory and calculation capacity ,and so security mechanism for sensor networks cannot require each sensor node to store long-sized key to run very complex cryptology protocols. They have low power consumption and so sensor network protocols must focus on power conservation. Usually sensor networks consist of large number of communication nodes, do not have global identification number, and could face easy node failure. WSN consists of different nodes connected to one or more several sensor nodes. These nodes are used in many applications like monitoring environment conditions, continuous communication for military and factory performance. All this application require, node is more consistent and reliable. Life of the node depends on the battery power. The performance of the network is goes down when the node consumes more battery power. In DoS attacks, the attacker's objective is to make target destinations inaccessible by legitimate users. A sensor network without sufficient protection from DoS attacks may not be deployable in many areas. Nodes misbehavior may range from simple selfishness or lack of collaboration due to the need for power saving, to active attacks aiming at DoS and subversion of traffic. The paper reviews various types of DOS attacks and its Detection techniques.

Denial of service (DOS) attack is an attempt to make a machine or network resource unavailable to its intended users. There are various types of DOS attack such as power exhaustion, jamming the signal and flooding with useless traffic. In jamming adversary it sends a strong signal for external model to destruct the message. In internal model adversary adds the extra data in to the packet and makes packet corrupt. In SYN flood attack adversary sends consecutive SYN request to target system to consume enough server resources and makes the system unresponsive. SYN flood messages comes under Path based DOS attack. In wormhole adversary, this is attack on the network and changes the routing data. So packet is traversed in longest path instead of shortest path and causes DOS attack. Power exhaustion is also causes DOS attack. A power exhaustion attack on the node consumes large battery power of the node. One type of power exhaustion attack is Vampire attack. Vampire attack is combination of stretch attack and carousel attack. In stretch attack adversary sends the packet in longest possible path instead of shortest path so that it consumes more battery power of the node and in carousel attack adversary sends the packet in routing loop .

II. DOS ATTACKS

- **Passive attacks:** Selfish nodes use the network but do not cooperate, saving battery life for their own communications; they do not intend to directly damage other nodes.
- **Active attacks:**Malicious nodes damage other nodes by causing network outage by partitioning, while saving battery life is not a priority.

DoS attacks can happen in multiple sensor network protocol layers. Table 1 depicts the typical DoS attacks and the corresponding defense strategies.

Table 1:

DoS attacks in sensor networks	DoS attacks Defense strategy
Radio interference	Use spread-spectrum
Physical tampering	make nodes tamper-resistant
Denying channel	Use error correction code
Black holes	Multiple routing paths
Misdirection	Source authorization
Flooding	Limit the connections

In wireless sensor networks there are two ways to attempt DOS attack by *power exhaustion and Jamming the signal.* In jamming sending a strong signals enough to destruct message in Wireless sensor networks and hence DOS attack is activated. In power exhaustion attack more battery power of the node consumption takes place, so node becomes inactive. Such inactive nodes reduce network performance and causes Denial of service attack.

There are various types of Denial of Service attack discussed as follows:

A. Denial of sleep attack: Denial of sleep attack is one of the type of DOS attack which targets the node's power Consumption. In this attack adversaries have knowledge of MAC layer protocol and it has an ability to bypass encryption and authentication protocols. The one protocol designed for wireless sensor network is MAC protocol. The battery power of node saved by placing radio in low power modes when node not sending and receiving data. MAC protocol is an ability to overcome radios primary sources of energy loss such as collision, control packet overhead and overhearing.

B. Path Based DOS attack: In path based DOS attack adversaries attacks on network. This is done by flooding the data packet over multi hop end to end communication path. Path based DOS attack is easy to launch and destroying large portion of wireless sensor network.

The following **Fig 1** consists of Aggregator nodes which process and summarize the data from member nodes, and send the aggregated result to a base station via a multihop, end-to end communication path and adversaries launches DOS in wireless sensor network by flooding data along multi hop path which quickly exhaust the communication bandwidth, limited energy and memory.

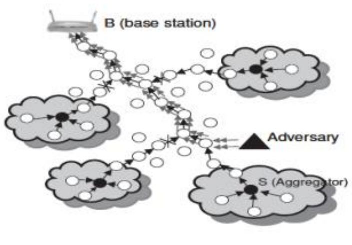

Fig 01: PDOS attack in End to End Communication in WSN

Fig 01: PDOS attack in End to End Communication in WSN

C. Jamming attack : Jamming is one type of DOS attack which has two types such as Jamming under external threat model and internal threat model. In External threat model jammer is not a part of network and jammer is sequentially or randomly transmits high power interference signal. In internal threat model any adversary who knows network secretes and implementation details of protocol of the network launching selective jamming attack. In selective jamming attack massage with high importance are targeted.

D. Wormhole attack: In wormhole attack adversary record the individual bit of packet or whole packet at one location. After recording the packet tunnel into the other location and then revise them in to the networks. This tunnel distance is longer than normal wireless transmission range of single hop. It is simple for attacker to make tunnelled packet arrive sooner than other packets transmitted over a normal multihop route. Wormhole places the attacker in strong position for gain unauthorized access.

E. Vampire Attack:Vampire attacks are not protocol-specific.it is one type of Denial of Service attack in which consuming more energy, node can be discharge and it can be disconnected from the network. Vampire attack consists of two different types of attacks called Stretch attack and Carousel attack. These attacks are mainly depends on reducing the energy of the nodes.

1) Carousel attack :

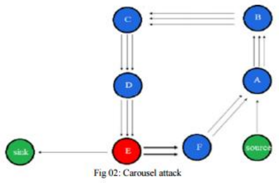

Fig 02: Carousel attack

In Carousel attacks, an adversary sends the packets in routing lop as shown in fig 2. in above fig packet is sending from source to sink. The shortest path for sending packet from source to sink is source - node f- node E and then Sink. But here packet is not follows shortest path and adversary composes the packet in loops. Packet is repeatedly traversing the same set of nodes. in above fig 2 packet is forwarded in the sequence such as source ◊ node A◊ node B◊ node C◊ node D◊ node E .then node E instead of forwarding packet to Sink, it is Sends packet to node F. then node F forward packet to node A and forms a loop. it causes more energy consumed by the nodes by repeating same path. So, because of this energy depletion, performance of the networks degrades.

2) Stretch attack: In Stretch attack, an adversary forms artificially longest possible routes and potentially traversing every node in the network which increases path length.

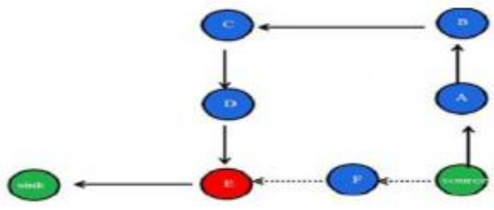

Fig 03: Stretch Attack

An example illustrated in fig 03. In this type of attack, packet sending from Fig 03: Stretch Attack source to sink. Shortest path for forwarding packet is sourcenode F to destination node Sink via node F. but in this attack, an adversaries forward packet in long route path as shown by dark line instead of dotted line path in above Fig 3. So it increases energy usage by the network. Stretch attack achieves more effectiveness and these attacks are independent on attackers' position relative to the destination. The impact of these attacks can be influenced by combining both Carousel and Stretch attack and increasing the number of adversarial nodes in the network. Although network does not employ authentication or network use only end-to-end authentication. So here adversary can replace routes in any overhead packets.

III. DOS PREVENTION TECHNIQUES

There is very little work done on the prevention of DoS attacks. Attempts to add DoS resistance to existing protocols often focus on cryptographic authentication mechanism. Aside from the limited resources that make digital signature schemes impractical, authentication in sensor networks poses serious complications. It is difficult to establish trust and identity in large-scale sensor network deployments. Adding security afterward often fails in typical sensor networks. Thus design-time consideration of security offers the most effective defence against DoS attacks. This paper formulates the prevention of passive denial of service attack at routing layer in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously. We propose a framework to enforce cooperation among nodes and punishment for non-cooperative behaviour. We assume that the rational users optimize their profits over time. Intrusion detector residing at the base station keeps track of other nodes' collaboration by monitoring them. If performances are lower than some trigger thresholds, it means that some nodes act maliciously by deviation. Intrusion detector rates other nodes, which is known as subjective reputation and the positive rating accumulates for each node as it gets rewarded.

Currently there are four mechanisms that could be helpful to overcome DoS attacks in sensor networks.

1. Watchdog scheme: A necessary operation to overcome DoS attacks is to identify and circumvent the misbehaving nodes.

Watchdog scheme attempts to achieve this purpose through using of two concepts: watchdog and path-rater. Every node implements a watchdog that constantly monitors the packet forwarding activities of its neighbors and a path-rater rates the transmission reliability of all alternative routes to a particular destination node.

The disadvantages of this scheme are that:

(1) It is only practical for source routing protocols instead of any general routing protocol

(2) Collusion between malicious nodes remains an unsolved problem.

(2) Rating scheme: In Rating scheme the neighbours of any single node collaborate in rating the node, according to how well the node execute the functions requested from it. It strikes a resonant chord on the importance of making selfishness pay. Selfishness is different from maliciousness in the sense that selfishness only aims at saving resources for the node itself by refusing to perform any function requested by the others, such as packet forwarding and not at disrupting the flow of information in the network by intension.

The disadvantages of this approach are that:

(1) How an evaluating node is able to evaluate the result of a function executed by the evaluated node.

(2) Evaluated node may be able to cheat easily

(3) The result of the function may require significant overhead to be communicated to the evaluating node.

3.Virtual currency: This scheme introduces a type of selfish node that are called nuglets . To insulate a node's nuglets from illegal manipulation, a tamper-resistant security module storing all the relevant IDs, nuglet counter and cryptographic materials is compulsory. In Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out nuglets for its forwarding services.

The disadvantages of this schemes are that :

(1) malicious flooding of the network can not be prevented,

(2) intermediate nodes are able to take out more nuglets than they are supposed to
(3) overhead .

4.RouteDoS Prevention: It attempts to prevent DoS in the routing layer by cooperation of multiple nodes. It incorporates a mechanism to assure routing security, fairness and robustness targeted to mobile ad hoc networks. The disadvantage of this approach is that misbehaving nodes are not prevented from distributing bogus information on other nodes' behavior and legitimate nodes can be classified as misbehaving nodes .

III. DETECTION OF DOS ATTACKS

A. Detection of Denial of Sleep attack: In denial of Sleep attack adversary is knowledge of MAC layer protocol and ability to bypass encryption and authentication protocols.MAC layer protocol designed for wireless sensor network and use various algorithm to save battery power by placing radio in low power mode. In this paper divide MAC protocol in four types i.e. Sensor MAC(SMAC), Berkeley MAC (B-MAC), Gateway MAC (G-MAC) and Timeout MAC (T-MAC).

We analyze all these MAC protocol in detail as follows: Sensor -MAC frame is divided in to listening and Sleep period. The listening period is divided in to synchronization and transfer period. Periodic updating is done by SYNC packet, Receivers adjust their timer counters. All the nodes announce their sleep schedule for correcting network time out in Synchronization period. T-MAC is an improvement in the S-MAC protocol by concentrating all traffic at the beginning of the duty period, as shown in Fig 04 .the figure indicates transmitted and received messages shown by arrows. T-MAC uses adaptive timeout (TA) mechanism allows nodes to transition to sleep mode when there is no more traffic in the cluster. T-MAC has network lifetime than S-MAC.B-MAC is does not attempt to synchronize sleep schedules. B-MAC uses the low-power listening (LPL) to reduce the energy consumption. LPL checks wireless sensor network for valid preamble byte that indicate the pending data transmission of another node. A node sends the pending data and

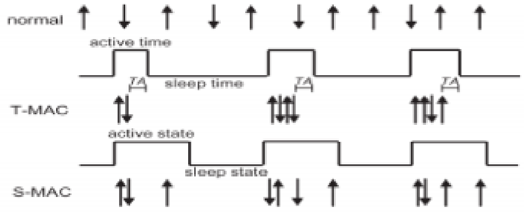

Fig 04: T-MAC adaptive timeout

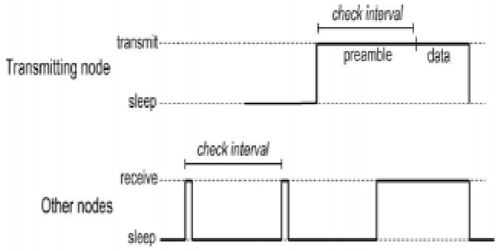

Fig 05: B-MAC low power listening

preamble. It ensure that all nearby nodes have the opportunity to receive the preamble and subsequent data message If interval between receiver samples is longer. In denial-of-sleep attack adversary broadcasting unauthenticated traffic into the network. This unauthenticated traffic reduces network lifetime of the node which uses SMAC and T-MAC protocol. In G-MAC protocol requests to broadcast traffic must be authenticated by the gateway node before the traffic can be sent to other nodes. Therefore, only the gateway suffers power loss due to unauthenticated broadcast. G-MAC protocol is used to improve network lifetime.

B. Detection of Path Based DOS attack : In this path based DOS attack is launched by flooding data packet along multi hop end to end path. an intermediate node must able to detect spurious packet or replayed packet and then reject them. to detect spurious packet and to defend against path based DOS attack use secured lightweight mechanism. In this scenario configures one way hash chain along a path enabling each intermediate node to detect a Path based DOS attack and prevents propagation of spurious or replayed packet. Every packet sent by end point includes new one way hash chain number which is used for message authentication. Different hash chain number is used for each time slot and intermediate node forward packet only if new hash chain number is verified. This process of verification by each intermediate node is continue and each time slot it verify new hash chain number. If number is not validate then the drop the packet.

C. Detection of jamming attack: In jamming attack adversary attack in the network under external as well as internal threat model. In the external threat model jammer is not part of the network. In external model jammer is continuously or randomly transmits high power interference signals. For the prevention of jamming attack from external jammer spread-spectrum communications technique used. Spread Spectrum techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code known only to the communicating parties. In the jamming under internal thread model any sophisticated adversary who is knowledge of network protocol can launch selective jamming attack. To launch selective jamming attack adversary must be capable of implementing "classify then jam" strategy before completion of wireless transmission. After classification, the adversary must introduce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. For the prevention of jamming attack from internal thread model use packet hiding method. In packet hiding method before classification of the packet by adversary we hide the packets. Hence adversary can't add bit error in to the packet and it is securely transmits. There are two methods for packet hiding i.e. commitment methods and cryptographic puzzle. In commitment method sender commits the packet and it is verify by the verifier. In the cryptographic puzzle packet m is encrypted with a randomly selected symmetric key k of a desirable length l. The key k is blinded using a cryptographic puzzle and sent to the receiver. For adversary, the puzzle carrying k cannot be solved before the puzzle is received and transmission of the encrypted version of m is completed. Hence, the adversary cannot classify m for the purpose of selective jamming.

D. Detection of wormhole attack : Packet leash is used for detection of wormhole attack. There are two types of packet leash i.e. temporal packet leash and Inte In temporal packet leash sender node uses its timestamp (sending time of the packet). In geographical packet leash sender uses its location and sending time of the packet to receiver. Based on this information receiver estimates distance between sender and receiver. If the estimated distance is longer than the possible radio range, receiver will reject the communication with Sender node.

E. Detection of Vampire attack : In this Vampire attack can be prevent by using energy weight monitoring algorithm(EWMA).In this algorithm energy of the node is consider for find out threshold level of the node. To detect malicious node in the network every node is add the test field while receiving the packet and forward packet to next node and then test field is check for each node. if the test field is correct then normal operation is continue and if the test field is wrong then create an alarm packet then alarm packet is broadcast and announce that node is malicious so that it avoid for further communication.

This algorithm is divided in two phases such as communication phase and network configuring phase. In network configuring phase establish optimum routing path from source to destination. Attacked node consumes more energy and reaches threshold energy level. 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 is establishes the routing path from source to destination. The source nodes select the node which is less distance from source and require minimum energy to transmit the packet. In communication phase avoid same data packet transmitted repeatedly through same node. These repeatedly transmission of same packet through same node depletes more battery power of the node and degrade the network performance.

The process of repeating the packet is eliminated by aggregating the data transmitting within forwarding node. In data aggregation copy the content of the packet which is transmitting through the node. This copied content compare with the data packet transmitting through the node. If the transmitted packet is matched with copied packet then stop the packet transmitted through them. so it avoids the redundant packet transmitting through the same node and protect from the vampire attack. Fig 06: EWM Algorithm IV. DISCUSSION In TABLE I we compare Detection techniques of Denial of Service attack.

For each type of Denial of Service attack detection technique is different. The one type of attack is Denial of sleep which uses the MAC protocol to prevent node from entering in to the sleep cycle. But the drawback is that it considers attacks only at MAC protocol not for others. The wormhole attack is avoided by packet leash technique but it is not always applicable and requires high cost. Vampire attacks is detected and prevented by Energy weight monitoring System using threshold level of the nodes. By using threshold level of the node we also detect and prevent Denial of sleep attack, Path based DOS attack, Wormhole attacks.

Energy Weight monitoring System is an effective technique to prevent the Denial of Service attacks because it is based on threshold level of the node.

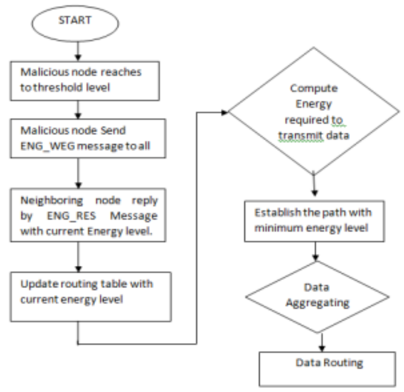
START
Malicious node reaches to threshold level
Malicious node Send ENG_WEG message to all
Neighboring node reply by ENG_RES Message with current Energy level.
Update routing table with current energy level
Compute Energy required to transmit data
Establish the path with minimum energy level
Data Aggregating
Data Routing

Fig 06: EWM Algorithm

TABLE I. DETECTION TECHNIQUES OF DOS ATTACK

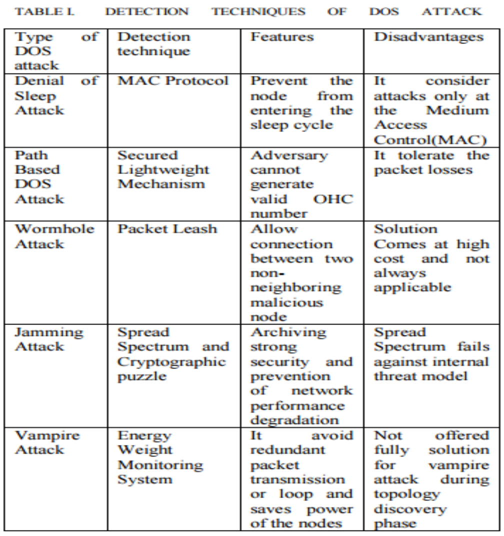

TABLE I. DETECTION TECHNIQUES OF DOS ATTACK

Type of DOS attack	Detection technique	Features	Disadvantages
Denial of Sleep Attack	MAC Protocol	Prevent the node from entering the sleep cycle	It consider attacks only at the Medium Access Control(MAC)
Path Based DOS Attack	Secured Lightweight Mechanism	Adversary cannot generate valid OHC number	It tolerate the packet losses
Wormhole Attack	Packet Leash	Allow connection between two non-neighboring malicious node	Solution Comes at high cost and not always applicable
Jamming Attack	Spread Spectrum and Cryptographic puzzle	Archiving strong security and prevention of network performance degradation	Spread Spectrum fails against internal threat model
Vampire Attack	Energy Weight Monitoring System	It avoid redundant packet transmission or loop and saves power of the nodes	Not offered fully solution for vampire attack during topology discovery phase

& fut

V. CONCLUSION &FUTURE ENHANCEMENT

DOS attack is much easier to launch in ad-hoc wireless sensor network. In this paper we defined types of Denial of service attack (DOS) such as Jamming, power consumption and SYN flood that permanently disables the ad-hoc sensor network. Our aim is to study various types of Denial of service (DOS) attack and its prevention techniques. After developing many prevention techniques wireless ad-hoc sensor network is still vulnerable to DOS attack.DOS attack cause the serious problem to users. In future we improve our techniques to prevent DOS attack which are not able to stop DOS attack fully.

References :

[1] A. Agah, K. Basu, and S. K. Das, "A game theory based approach for security in sensor networks," International Performance Computing and Communications Conference (IPCCC), pp:259-263, Phoenix, AZ, Apr. 2004.

[2] A. Agah, S. K. Das and K. Basu, "Preventing DoS attack in sensor and actor networks: A game theoretic approach," IEEE International Conference on Communications (ICC), pp:3218-3222, Seoul, Korea, May 2005.

[3] A. Agah, S. K. Das, and K. Basu, "Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling, " Proceedings of 2nd IEEE International Conference on Mobile AdHoc and Sensor Systems (MASS), Washington, D.C., Nov. 2005.

[4] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, 2002, pp:393-422.

[5] R. Bace and P. Mell, "Intrusion detection systems," NIST Special Publication on Intrusion Detection systems, http://www.snort.org/docs/nistids.pdf.

[6] G. E. Bolton, A. Ockenfels, "ERC a theory of equity, reciprocity, and competition," The American Economic Review, vol. 90, 2000.

[7] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks," International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2002.

[8] S. Buchegger and J. L. Boudec, "Nodes bearing grudges: toward routing security, fairness and robustness in mobile ad hoc networks," Proceedings of the 10th Euronicro Workshop on parallel, Distributed and Network-based Processing, Canary Islands, Spain, January 2002. International Journal of Network Security, Vol.5, No.2, PP.145–153, Sept. 2007 152

[9] L. Blazevic, L. Buttyaan, S. Capkun, S. Giordano, J. P. Hubaux, J. LeBoudec, "Self-organization in mobile ad hoc networks: the approach of terminodes," IEEE Commun.Mag., vol. 39, no. 6, 2001, pp:161- 174.

[10] L. Buttyaan, J. P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks," Mobile Computing and communications Review, vol.6, no.4, 2002.

[11] L. Buttyaan, J. P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in selforganized mobile ad hoc networks, " Technical Report DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology, 2001.

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

[13] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenge," Proceedings of the IEEE, special issue on sensor networks and application, vol. 91, no. 8, 2003, pp:1247-1256.

[14] J. Deng, R. Han, S. Mishra, "INSENS:Intrusiontolerant routing in wireless sensor networks," Technical Report TR CU-CS-939-02, Dept. of Computer Science, University of Colorado, 2002.