# Power Conservation and Security in Wireless Sensor Networks – A Survey

K.Amirthavalli
*PG Scholar-Embedded System Technologies*
*S.K.P Engineering College*
*Tiruvannamalai*
amirthakarthikeyan1@gmail.com

P.Sivakumar
*Professor-ECE*
*S.K.P Engineering College*
*Tiruvannamalai*
sivakumar.poruran@gmail.com

*Abstract*—**In Wireless Sensor Network (WSN), two major challenges are how to conserve the battery power of a sensor and to impose a series of security challenges. The intend of this paper is to investigate the power conservation techniques and security related issues and challenges. We also discuss the holistic view for ensuring and robust security in Wireless Sensor Networks.**

***Keywords-Wireless Sensor Network (WSN), Power Conservation, Security, Holistic.***

## I. INTRODUCTION

A typical Wireless Sensor Network structure has four main parts: Sensors – to sense data, Processor – for data processing with memory, Communication hardware – for data communication and Power supply unit. It is shown in Figure 1.

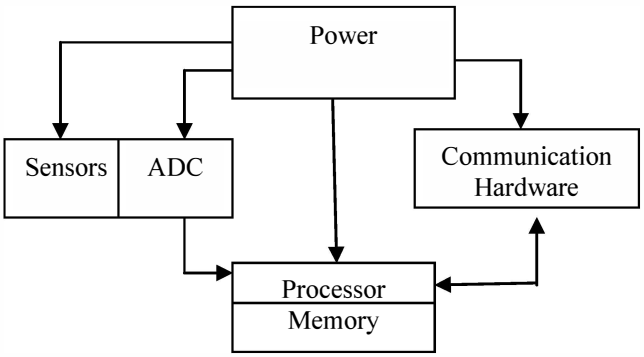


Figure 1. Structure of Wireless Sensor Networks

A wireless sensor networks consist of many wireless sensors that collect data like temperature, light, humidity, vibration and other physical environmental conditions. The information is processed and sent it to the sink[1] . Each node has a battery with limited capacity which is very difficult to recharge and change due to the environment in which they are deployed.

There are different techniques are used to prolong the lifetime of a sensor network[2]. During network activities, energy efficient are used to reduce energy consumption to minimum. A large amount of energy is consumed by other components also like CPU and radio in the idle state. So, power management schemes are used to switch off the components that are not used.

The sensor network also introduces severe resource constraints due to their lack of data storage and power. These represent major obstacles to the implementation of computer security techniques. Our main challenges are to maximize the processing capabilities and reducing energy consumption of the sensor nodes and also secure them against attackers.

In this survey, Power Conservation and Security schemes are explained. The Section II highlights some causes of energy loss in Wireless Sensor Networks. The Section III discusses the power conservation techniques. The Section IV highlights the security threats and issues in WSN. The Section V discusses the proposed security schemes. Finally, we will discuss the conclusion.

## II. ENERGY LOSS IN WIRELESS SENSOR NETWORKS

There are many challenges in wireless sensor networks, most of them leads to energy loss. In this section, it highlights some causes of energy loss in wireless sensor nodes communication [3].

**Idle listening**: means when sensor nodes wake up and listen for incoming packets even when no data is being sent. This causes the depletion of lifetime of wireless sensor networks.

**Collision**: describes when two or more stations want to transmit packets at a time. When it happens, collision occurs and the packets are discarded then retransmitted which results in energy loss.

**Overhearing**: is an indirect communication where an agent receives data which is not an addressee. It results an unnecessary traffic so energy loss will occur.

**Control packet overhead**: control packet consumes more energy than ordinary packets while sending, listening and receiving, therefore it is necessary to use less number of

control packets for data transmission, thus it reduces the overhead.

## III.POWER CONSERVATION TECHNIQUES

Energy is one of the critical resources in wireless sensor networks but one common problem is lack of power source for each sensor in the sensor network. Data communication consumes more energy whereas data processing consumes significantly less. The energy consumption of the sensor depends upon specific sensor type[4]. To extend the lifetime of a WSN, many power conservation techniques are proposed to minimize the energy consumption of the communication unit. This is achieved by following approaches: *Duty cycling, Data driven approaches, mobility based approaches, clustering method, and Game theory approach [6].*

### *A.Duty Cycling*

There are two modes in sensor nodes radio operation: active mode and sleep mode. The sensor nodes switch between active and sleep mode based on their activities are called "Duty cycling"[5]. During the idle mode, the idle energy is very significant in saving energy in WSN. Duty cycle is thus defined as the percentage of a node's time is active its lifetime. The Techniques of Duty Cycling is shown in Figure 2.

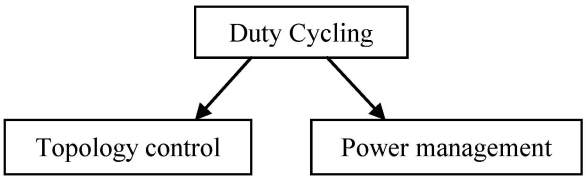


Figure 2. Duty Cycling

Duty cycling can be done using two different techniques. The first method is "topology control", its main aim is to save energy and reduce interference between nodes and extend lifetime of the wireless sensor networks.

The second method is "power management" scheme which introduces MAC protocols and wakeup scheduling protocols, in which during idle state a sensor node sleeps in more slots and maintains network connectivity.

The MAC protocols with low duty cycle are BMAC, ZMAC and TRAMA.

In BMAC contention based protocol, each sensor node has an individual schedule of sleep/wake period which uses low power listening to gain low power communication.

ZMAC is a hybrid protocol of TDMA and contention based schemes. ZMAC employs contention based scheme when the contention level is low and switches to TDMA scheme when the contention level is high. TRAMA is a TDMA scheme where the sensor nodes can communicate their information only through their assigned slots, thus reduces the energy consumption. There are three wakeup mechanisms: On-demand wakeup, scheduled neighbor discovery and asynchronous neighbor discovery.

**On-demand wakeup mechanism**, sleeping nodes are waken on demand. It means that a node should wakeup only at when other node is ready to communicate with it. But there is a problem that is how to inform the sleeping node that other node is ready to communicate with it. To overcome this problem, it employs multiple radios with different energy levels and this method is very energy efficient.

**Scheduled wakeup mechanism**, sleeping nodes wakeup at the same time of wakeup schedule to communicate with each other and then go back to sleep again until the next scheduled period. The examples of this method are S-MAC protocol and multi-parent schemes protocol.

**Asynchronous wakeup mechanism**, does not need clock synchronization like scheduled wakeup mechanism. A sensor node wakes up when it wants to communicate with the other node. The advantage in this method is the implementation with low message overhead for data communication is easy.

### *B.Data Driven Approaches*

The energy conservation is reduced in data driven approaches by two ways. First, it removes all unneeded samples that utilizes the energy consumption and stops them by transmitting to the sink. Secondly, it reduces the energy spent on the sensing subsystem. There are two schemes in this approach: Data reduction and data acquisition schemes.

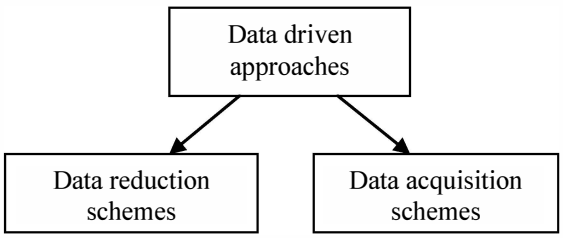


Figure 3. Data driven approaches classification

#### *a.Data Reduction Schemes*

The data reduction [7] solves the problem of unneeded samples while the data acquisition reduces the energy spent on the sensing subsystem.There are three methods to minimize the amount of data that is transmitted to the sink. (i)In-networking processing, (ii) Data compression, and (iii) Data prediction.

**In-networking processing:** It does data aggregation at intermediate nodes to minimize the amount of data that is transmitted to the sink.

**Data compression:** It encodes the data at the source node and decodes at the sink node to reduce the amount of data transmission.

**Data prediction:** It predicts the data at both source and sink nodes by adaptive filters.

By these three methods, it produces upto 50% energy savings when compared to several sensing schemes.

*b.Data Acquisition Schemes*

The energy efficient data acquisition schemes mainly focus on reducing the radio energy consumption [8] rather than reducing the energy consumption of the sensing subsystem. It is of three types: (i)Hierarchical sampling, (ii)Adaptive sampling and (iii)Model based sampling.

**Hierarchical sampling**: The hierarchical sampling requires that nodes contain different types of sensors. Each sensor has its own accuracy and power consumption. It determines which class to activate to get tradeoff between accuracy and power conservation.

**Adaptive sampling**: The adaptive sampling is used to reduce the amount of data acquired from the transducer with respect to the available energy.

**Model-based active sampling:** It is used to reduce the number of data samples to be communicated to the sink.

*C.Mobility Based Approaches*

Mobility means some of the sensor nodes are mobile for reducing energy consumption. There are two different ways in mobility of sensor nodes. First, a mobilizer is attached to a sensor that changes its location, this changes are limited to a few nodes which are not inhibited by energy. Secondly, sensors are fixed in mobile elements like animals and vehicles. By these two methods, there is no energy loss due to mobility. It is classified into two: Mobile Sink(MS) and Mobile Relay(MR).

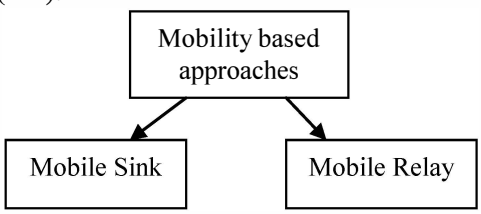


Figure 4. Mobility based approaches

*a.Mobile Sink*

Mobile sinks[9] are used to change the sensor nodes location to the new location whenever the needs come. It balances the power conservation and maximizes the network lifetime by applying Linear Programming (LP) to the sinks. So, the mobile sink has greater efficiency than the static sink.

By introducing another method to increase the lifetime of the sensor by Greedy Maximum Residual Energy (GMRE) heuristic[10]. It adopts a Mixed Integer Linear Programming (MILP) model to control the movement of the sink in order to increase the lifetime of the wireless sensor networks.

Next approach is the combination of mobility and routing algorithms. Here, the base station is mobile, so it reduces the traffic of the heavily loaded nodes. This combination of mobility and routing algorithm has high improvement of the network lifetime[11].

Each sensor node delays the data transmission until the mobile sink is at a location than extends its lifetime [12]. So, it increases the network lifetime when compared to the static sink.

*b.Mobile Relay*

One of the best approach schemes in mobile relay is message ferrying (MF) scheme[13]. MF is a set of special mobile nodes called as message ferries to transmit messages within the deployment area. Another best known method is data-MULE (Mobile Ubiquitous LAN Extensions) system.

It prolongs the network lifetime by reducing the communication rate of the sensors. The mobile entity may be animals, vehicles or even people can be MULEs. The MULE acquires data from the sensors near it, screen it and drop it off to wired access points. It leads to power saving at the sensors base station due to short distance wireless communication. When compared to adhoc-network, data-MULE achieves twice more energy saving[14].

Another scheme in mobile relay is Zebranet. Zebranet is a mobile wireless sensor network developed by joint effort of biologist and Computer scientist for tracking of wildlife. It does energy efficient tracking nodes and stores and forwards the data, thus it improves tracking technology. Zebranet was developed to track wildlife in large forest area using communication equipments[15].

*D.Game Theory*

Game theory[16] is a mathematical model defines the phenomenon of conflict and co-operation between intelligent decision makers.

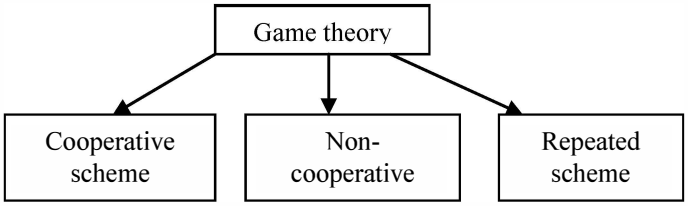


Figure 5. Classification of Game theory

Game theory is classified into three types: Cooperative scheme, Non- cooperative scheme and repeated scheme.

*a.Co-operative scheme*

Cooperative game theory is also called as coalitional game theory[17]. Cooperative game theory is divided into two types: (1) Transferable utility game (TU) and (2) Non transferable utility game (NTU). In TU the payoff of the measurement allocation game is transferable. In NTU the payoff for each agent in a coalition depends only on the action selected by the agents in the coalition.

*b.Non-cooperative scheme*

Non-cooperative game theory defines the interactions among the competing players. In this non-cooperative game, a player is called an agent and his goal is to extend the utility by choosing its strategy individually. It provides incentives for each player .

*c.Repeated scheme*

Repeated game theory is an extensive form of game theory, a player has to take into account the impact of its current action on the future actions of others.

Agah and Das studied a repeated game formulation between malicious sensor nodes and an intrusion detector to prevent passive Denial of Services (DoS) attacks at the routing layer of Wireless Sensor Networks[18].

Yang *et al*. managed the problem of dropping packets attacks in WSN and designed the interactions between the sensor nodes as a repeated game[19].

*E.Priority Based Approach*

Before transmitting the packet, priority has to be given to each sensor by using First In First Out (FIFO) technique. So, the power consumption is more compared to all above methods.

**Table 1 Comparing the power conservation techniques**

| S.No. | Power conservation techniques | Idle listening | Collision | Overhearing | Control packet overhead | Energy saving | Time consumption |
|---|---|---|---|---|---|---|---|
| 1 | Duty Cycling | Very high | Very high | Very high | Very high | Very less | Very high |
| 2 | Data driven approaches | high | high | High | high | less | High |
| 3 | Mobility based approaches | Comparatively less | Comparatively less | Comparatively less | Comparatively less | Comparatively high | Comparatively less |
| 4 | Game theory | less | less | less | less | high | Less |
| **5** | **Priority based** | **Very less** | **Very less** | **Very less** | **Very less** | **Very high** | **Very less** |

IV.SECURITY ISSUES AND THREATS IN WSN

Wireless networks are usually more vulnerable to various security threats and attacks because of the “eavesdropping”. The architectural aspect of WSN could make the employment of a security easier as the base stations could be used extensively. Usually, most of the sensors are expected to be deployed in the hazardous area. Therefore, even if the base station resides in the safe area, the sensors should be protected against the attackers[20].

*A. Attacks in Wireless Sensor Networks*

Here we will discuss the major attacks in wireless sensor networks.

*a.Denial of Service (DoS)*

Denial of Service is produced by the malicious nodes. The DoS attack usually sends the extra unnecessary packets and also prevents rightful users from accessing services to which they are allowed[21]. There are many types of DoS attacks in different layers in WSN.

**Table 2. DoS attack in different layers**

| LAYER | TYPES OF DOS ATTACK | PREVENTION MECHANISM |
|---|---|---|
| PHYSICAL | Jamming and Tampering. | |
| LINK LAYER | Collision, exhaustion, unfairness. | 1.Pushback,<br>2.Strong |

| | | |
|---|---|---|
| NETWORK | Neglect and greed, homing, misdirection, black holes. | authentication and<br><br>3.Identification of traffic. |
| TRANSPORT | Malicious flooding, desynchronization. | |

*bSybil attack*

The attack where a sensor node forges the identities of more than one node is called the "Sybil attack". Sybil attack usually tries to degrade the integrity of data, security and resource utilization. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, misbehavior detection and resource allocation. Wireless adhoc network (peer-to-peer network) [22] is vulnerable to Sybil attack. Newsome et. al[23] used radio resource testing to detect the presence of Sybil node in wireless sensor network and the presence of Sybil node is detected by the probability,

$$Pr(detection) = 1 - (1 - \sum_{all\,S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c})^r$$

Where, $n$ is the number of nodes in a neighbor set, $s$ is the number of sybil nodes, $m$ malicious nodes, $g$ number of good nodes, $c$ is the number of nodes that can be tested at a time by a node, of which $S$ are sybil nodes, $M$ are malicious (faulty) nodes, $G$ are good (correct) nodes and $r$ is the number of rounds to iterate the test.

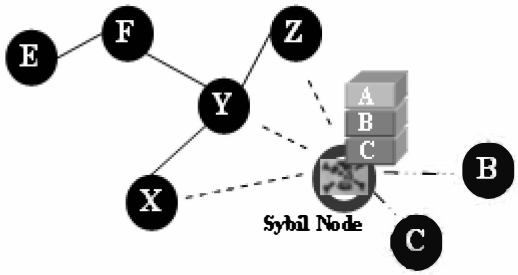


Figure 6. Sybil attack

*c. Wormhole attack*

Wormhole attack[24] is a critical attack in which the attacker records the packets at one location and tunnels them to other location in a network. The tunneling or retransmitting of packets could be done selectively. This attack could not be compromised in a network because it is a significant threat. It could be performed even at the initial phase when the sensors start to discover the neighborhood node information.

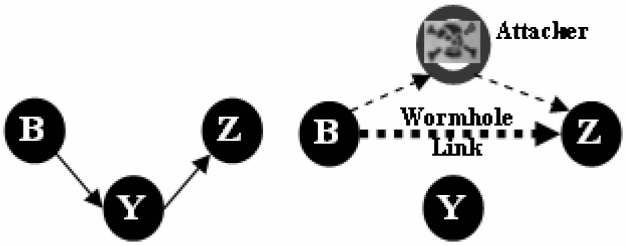


Figure 7. Wormhole attack

In the Figure 12, when a node B transmits the routing request packet, the attacker then receives this packet and replays to its neighborhood node. Each neighborhood node which receives this replayed packets are considered to be in the node B range and that node could be considered as a parent node. Even the victim nodes are apart from B, the attacker convinces them that B is the single hop away from them, then the wormhole is created.

*d.Hello flood attack*

Hello flood attack introduces the HELLO packets as an attacker to attack the sensor nodes in WSN. It sends HELLO packets to a number of sensors which are dispersed in a large area with a high radio transmission range and processing power. While transmitting the information to the base station, the victim nodes go through the attacker as they know that it is their neighbor and are spoofed by the attacker[25].

*e.Blackhole attack or Sinkhole attack*

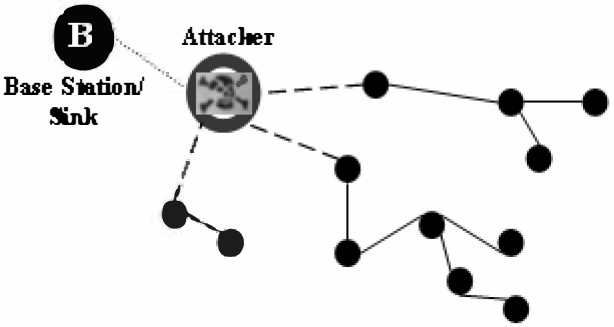


Figure 8. Blackhole attack

The malicious node acts as a blackhole attacker. The malicious node is inserted in between the source and sink nodes, it is able to do anything in the packets which are passed between them. This attack can attack the nodes even which are located far from the base station[26].

V.PROPOSED SECURITY SCHEMES

The proposed security schemes are illustrated in a table 3 below:

**Table 3. Proposed security schemes**

| ATTACKS | SECURITY SCHEMES | MAJOR FEATURES |
|---|---|---|
| DoS attack | JAM[27] | Avoidance of jammed region by using coalesced neighbor nodes. |
| | Wormhole based[28] | Avoid jamming by using wormhole. |
| Sybil attack | Radio resource testing, random key pre-distribution | Uses radio resource, Random key pre distribution,Registration procedure, Position verification and Code attestation for detecting sybil entity. |
| Wormhole attack | TIK[29] | Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes. |
| Hello flood attack | Bidirectional Verification, Multi-path multi-base station routing[30] | The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack. |
| Blackhole attack | REWARD[31] | Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect blackhole attacks. |

*a.Holistic security in WSN*

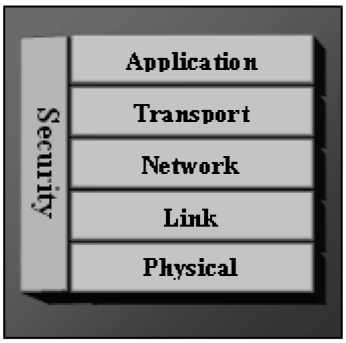


Figure 9. Holistic approach security

A holistic security approach improves the security in WSN, longetivity and connectivity under changing environmental conditions[32]. The security is to be ensured for all the layers of the protocol stack. A single security solution for a single layer is not an efficient solution, so we are employing holistic approach, the best solution.

## VI.CONCLUSION

In this paper, we surveyed the power conservation techniques, types of major attacks in WSN and proposed security schemes. In the field of power conservation in WSN, there are still other areas that need to be exploited in order to tackle the power conservation issue. One among is energy harvesting from the environment not only as a source of energy but also as a means of conserving the power in Wireless Sensor Networks.

In WSN, most of the attacks against security are caused by the insertion of false information by the compromised nodes. Detection of false reports of the nodes is the defense mechanism. Also, holistic approach improves the security in the network. Even the holistic approach is employed in the network, some mechanisms such as the cost effectiveness and energy efficiency are still great research challenge in the future.

## REFERENCES

[1]I. F. Akyildiz, W. Su, Y.Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey”, Computer Networks , Volume 38, No. 4, March 2002.

[2]Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[3]Bulbenkiene, V., Jakovlev, S., Mumgaudis, and G., Pridotkas, G., “Energy loss model in Wireless Sensor Networks”, IEEE Digital Information Processing and Communication (ICDIPC), 2012 Second International Conference, PP.36-38, 10-12 July 2012.

[4]N. Akilandeswari, B., Santhi , B. Baranidharan. “Energy conservation techniques in Wireless sensor Networks- A Survey”, ARPN Journal of Engineering and Applied Sciences, Vol 8, No. 4, April 2013.

[5]Shouwen Lai., “Duty-Cycled Wireless Sensor Networks-Wakeup scheduling, Routing and Broadcasting”, A thesis submitted to Virginia Polytechnic Institute and State University, Virginia, 26 April 2010.

[6]Anastasi G., Coti M., Frrancesco M. & Passarella A., “Energy Conservation in Wireless Sensor Networks: A Survey”, Ad Hoc Network, 2009.

[7] Zhang Q., “Cooperative Data Reduction in Wireless Sensor Network” Globecom 2012- Adhoc and Sensor Networking Symposium, pp 646-651.

[8] Alippi C., Anastasi G., Francesco M.D. & Roveri M., “Energy Management in Wireless Sensor Networks with Energy-hungry Sensors” IEEE Instrumentation and Measurement Magazine, Vol. 12, No. 2, pp. 16-23, 2009.

[9] Wang G.,Wang T.,Jia W.,Guo M. and Li J., "Adaptive location updates for mobile sinks in wireless sensor networks" Springer Science Business Media, pp 287a, 2008.
[10] Basagni S., Carosi A., Melachrinoudis E., Petrioli C. and Wang Z. M., "Controlled sink mobility for prolonging wireless sensor networks lifetime", ACM / Elsevier Journal on Wireless Networks, 2007.
[11] Luo J & Hubaux J.P., "Joint Mobility and Routing for Lifetime Elongation in Wireless Sensor Networks", Proc. IEEE Infocom-2005, vol. 3, PP. 1735-1746, Miami (USA).
[12] Yun Y. & Xia Y., "Maximizing the Lifetime of Wireless Sensor Networks with Mobile Sink in Delay-Tolerant Applications", Mobile Computing- IEEE Transactions Volume:9, 2010.
[13] Zhao W., Ammar M., and Zegura E., "A Message Ferrying approach for Data Delivery in sparse Mobile Ad-Hoc Networks", Proc. of ACM MobiHoc 2004, Tokyo, Japan.
[14] Shah R. C., Roy S., Jain S. & Brunette W. (2003), "Data MULEs: Modelling a Three-tier Architecture for Sparse Sensor Networks", Proc. IEEE Int'l Workshop on Sensor Network Protocols and Applications (SNPA 2003), PP. 30-41, 2003.
[15]Juang P.,Oki H.,Wang Y.,Martonosi M.,Peh L., Rubenstein D.,"Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with Zebranet", Proc. Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2002.
[16] A. Agah, M. Asadi, and C. Zimmerman, "A Game-theoretic Approach to Security and Power Conservation in Wireless Sensor Networks", International Journal of Network Security, Vol.15, No.1, PP.50-58, Jan. 2013.
[17] Saad W., Zhu H., Debbah M., Hjorungnes A., Basar T. "Coalitional game theory for communication networks: A tutorial". IEEE Sign. Process. Mag. 2009.
[18]Agah A., Das S. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. International Jounal on Network Security. 2007.
[19]Yang L., Mu D., Cai X. Preventing dropping packets attack in sensor networks: A game theory approach. Wuhan Univ. J. Nat. Sci. 2008.
[20] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.
[21] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.
[22] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
[23] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
[24] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
[25] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
[26] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
[27] Wood, A.D., Stankovic, J.A., and Son, S.H., "JAM: A Jammed-Area Mapping Service for Sensor Networks", 24th IEEE Real-Time Systems Symposium, TSS 2003, pp. 286-297.
[28] Cagalj, M., Capkun, S., and Hubaux, J-P., "Wormhole-based Anti-Jamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05 worm.pdf
[29] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
[30] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.
[31] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.
[32] Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.

.