TOBB UNIVERSITY OF ECONOMICS AND TECHNOLOGY
INSTITUTE OF NATURAL AND APPLIED SCIENCES

THE IMPACT OF INCAPACITATION OF MULTIPLE CRITICAL SENSOR NODES ON WIRELESS SENSOR NETWORK LIFETIME

MASTERS THESIS

Behnam Ojaghi KAHJOGH

Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. M.Fatih DEMIRCI

AUGUST 2017

Approval of the Graduate School of Natural and Applied Sciences.

.....
Prof. Dr. Osman EROĞUL
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

.....
Assoc. Prof. Dr. Oğuz ERGIN
Deputy Head of Department

This thesis entitled **THE IMPACT OF INCAPACITATION OF MULTIPLE CRITICAL SENSOR NODES ON WIRELESS SENSOR NETWORK LIFETIME**, by **Behnam Ojaghi KAHJOGH**, 141111020, a graduate student at TOBB University of Economics and Technology, Institute of Natural and Applied Sciences, has been prepared after fulfilling all the requirements determined by the committee members for the degree of Master of Science in Computer Engineering, and is recommended for approval and acceptance on **August 14, 2017**.

Supervisor: **Assoc. Prof. Dr. M.Fatih DEMIRCI** .....
TOBB University of Economics and Technology

Co-Supervisor: **Prof. Dr. Bulent TAVLI** .....
TOBB University of Economics and Technology

Committee: **Prof. Dr. Erdoğan DOĞDU (Chair)** .....
Cankaya University

Asst. Prof. Dr. A.Murat ÖZBAYOĞLU .....
TOBB University of Economics and Technology

Asst. Prof. Dr. H.Uğur YILDIZ .....
TED University

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

I hereby declare that all the information provided in this thesis was obtained with rules of ethical and academic conduct. I also declare that I have sited all sources used in this document, which is written according to the thesis format of the Graduate School of Science and Technology of TOBB ETU.

Behnam Ojaghi KAHJOGH

ABSTRACT

Master of Science

THE IMPACT OF INCAPACITATION OF MULTIPLE CRITICAL SENSOR NODES ON WIRELESS SENSOR NETWORK LIFETIME

Behnam Ojaghi KAHJOGH

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Assoc. Prof. Dr. M.Fatih DEMIRCI

Date: August 2017

Wireless Sensor Networks (WSNs) are envisioned to be utilized in many application areas such as critical infrastructure monitoring, therefore, WSN nodes are potential targets for adversaries. Network lifetime is one of the most important performance indicators in WSNs. Possibility of reducing the network lifetime significantly by eliminating a certain subset of nodes through various attacks will create the opportunity for the adversaries to hamper the performance of WSNs with a low risk of detection. However, the extent of reduction in network lifetime due to elimination of a group of critical sensor nodes has never been investigated in the literature. Therefore, in this study, we created a novel Linear Programming (LP) framework to model the impact of critical node elimination attacks on WSNs and explored the parameter space through numerical evaluations of the LP model. Our results show that critical node elimination attacks can shorten the network lifetime significantly.

Keywords: Wireless sensor networks, Network optimization, Mathematical programming, DDOS attacks , Wireless security.

ÖZET

Yüksek Lisans Tezi

KRITIK DÜĞÜMLERIN ETKISIZLEŞTIRILMESININ KABLOSUZ ALGILAYICI AĞ YAŞAM SÜRESI AZALMASINA ETKILERI

Behnam Ojaghi KAHJOGH

TOBB Ekonomi ve Teknoloji Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği

Danışman: Doç. Dr. M.Fatih DEMIRCI

Tarih: August 2017

Kablosuz Algılayıcı Ağlar (KAA) askeri güvenlik ve çevre gözetleme vb. kritik kontrol etme uygulamalarında sıkça kullanılmaktadır. Bu tip kritik uygulamarda algılayıcı düğümler düşman saldırıları için potansiyel birer hedeftir. KAA'ların en önemli performans ölçütlerinden birisi ağ yaşam süresi olduğuiçin çeşitli saldırılarla algılayıcı düğümlerden en kritik olanlarının ele geçirilmesi ve işlevsiz hale getirilmesi ağ yaşam süresini ciddi miktarda etkilemektedir. Bu çalışmada Doğrusal Programlama (DP) tabanlı iki tane özgün algoritma geliştirilmiş olup kritik düğümlerin ele geçirilmesinin KAA yaşam süresine olan etkileri sistematik biçimde ele alınmıştır. Bu çalışma sonucunda kritik düğümlerin ele geçirilmesinin ağ yaşam süresini ciddi ölçüde düşürdüğü sonuçlarına varılmıştır.

Anahtar Kelimeler: Kablosuz algılayıcı aglar, Doğrusal programlama, Servis kesintisi, Fiziksel saldırı.

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to Prof. Dr. Bulent TAVLI and Prof. Dr. Erdoğan DOĞDU for giving me the chance to take this challenging experience, and providing me the scholarship and for their continuous support of my graduate study at TOBB University of Economics and Technology , I also thank Assoc. Prof. Dr. M.Fatih Demirci for accepting my supervision after Prof. Dr. Erdoğan DOĞDU.
My sincere gratitude goes to Prof. Dr. Osman EROĞUL, the director of Institute of Natural and Applied Sciences whose office was always open to share my concerns either personal or educational issues.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 Wireless Sensor Networks

The concept of a sensing system created by multiple low-cost and tiny devices for information extraction over a predetermined deployment area is, defined as Wireless Sensor Networks (WSNs) [2]. Some of the application areas for WSNs are remote monitoring, military applications, automation systems, smart grid, underwater surveillance, and agriculture (among many others) [3, 7, 14, 44]. Conserving energy, security, scalability, latency, throughput, and energy consumption are critical concerns in WSN design. Sensor networks are present in almost all aspects of our modern life, and also are more important in collecting the required data through smart environments. They can easily sense physical or environmental conditions such as temperature, sound, pressure, etc [26, 40].

WSNs almost are composed of hundreds and/or thousands of sensor nodes distributed randomly in a distinctive area. They can be dispersed to an indicated area, and subsequently can be shaped as a self-organized wireless communication network as shown in Figure 1.1.

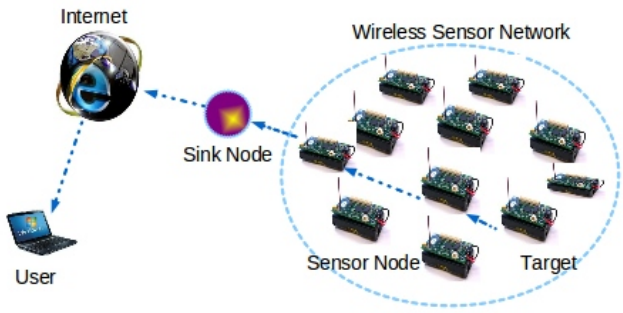


Figure 1.1: WSN Architecture.

Providing useful service for extended durations is, arguably, the most important Quality-of-Service (QoS) metric for WSNs [6].

In principle, the main purpose of wireless sensor network is gathering the sensory information with various types of sensor nodes from the target area and send it to the sink (*i.e.*, base station) in order to accomplish a specific task. The base station has a high storage capacity, and energy of processing. In addition, all data packet of sensor nodes are forwarded to this station. Hence, the position of the sink node has an important role on the energy consumption and lifetime of WSNs.

WSNs act as *sensing node, relaying node or as a base station (B.S).*

- **Sensing Mode:**

  The main aim of sensor nodes are to sense several criterion such as temperature, pressure, electrical fields, sound, light, etc. When some event is happening, the sensor node senses and records this event, and then transmits it to the neighbour nodes in the network system. At this mode, the majority of energy consumption is used for sensing and transmission.

- **Relaying Mode:**

  In multi-hop communication it is impossible to send all injected information directly to the sink node (*i.e.*, base station), and the transmission is accomplishing by forwarding the received information through intermediate sensor nodes. This process continuously repeats until to reach all data of sensor nodes to the base station. Sensor nodes at this mode consume most of their energy to send and receive information.

- **Base Station (BS):**

  In WSNs, one or more sensor nodes are considered as a sink node (*i.e.*, base station) that functions as the hub in the wireless network. All the injected information terminates at this node and it disseminates this information to the external world. In general, the energy consumption is not limited at this mode and the energy dissipation is ignored.

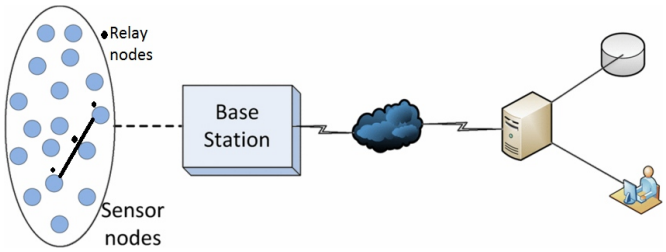


Figure 1.2: A scheme of typical WSN.

Furthermore, some characteristics of a well-designed wireless sensor network can be *energy efficiency, scalability, responsiveness, reliability and mobility*.

- **Energy efficiency:**

  WSNs equipped with some optimizing algorithms so that to minimize the duty cycle of each sensor node which will be discussed at preceding sections. Figure 1.3 shows the device in which consumes less energy while maximizing the corresponding tasks. These tasks are done by performing under extremely low power levels.

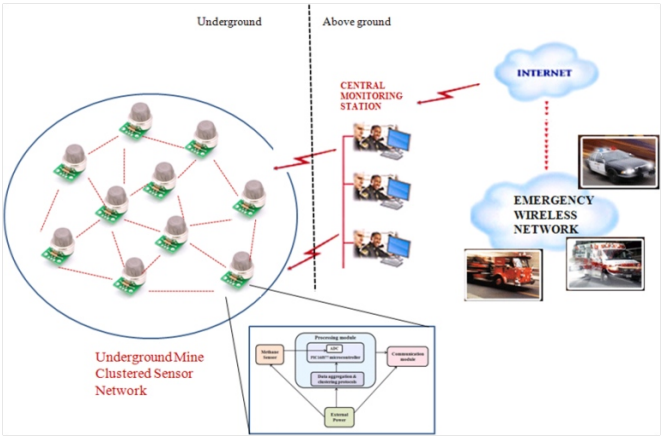


Figure 1.3: Energy efficiency in WSN.

- **Scalability:**

  The capability of network to cooperate with an increased number of nodes which can be attached any-time to the wireless sensor network, and in turn has some extra packet overhead to the network system. Moreover, the probability of failure in packet delivery is high when the network size grows. Figure 1.4 shows the scalability in WSNS.

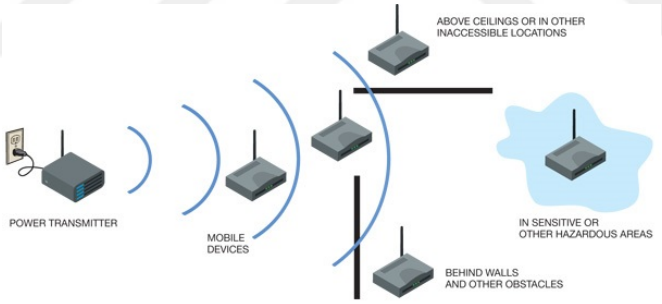


Figure 1.4: Scheme of Scalability in WSN.

- **Responsiveness:**

  This feature is another important characteristic in WSNs which defined as the potential of the network to quickly conform itself when the topology is changed, and then update the network policy based on new topology. Figure 1.5 is representative of this property. The packet delivery, latency, and scalability can reduce the responsiveness of network system.

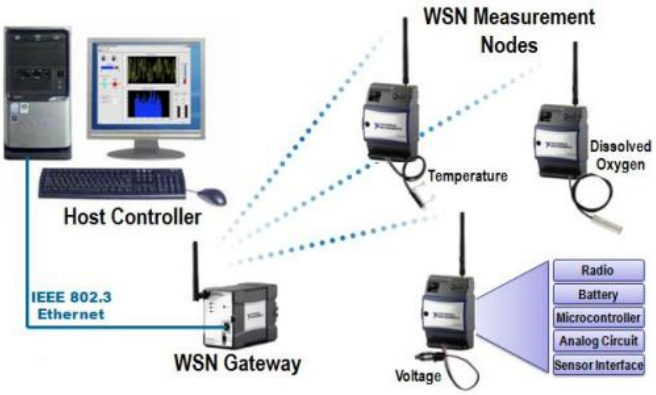


Figure 1.5: Scheme of Responsiveness in WSN.

- **Reliability:**

  One of the fundamental requirements of WSNs is to be reliable. WSNs should have adequate security mechanisms to impede unexpected attacks and threats targeted the data interior of the sensor node.

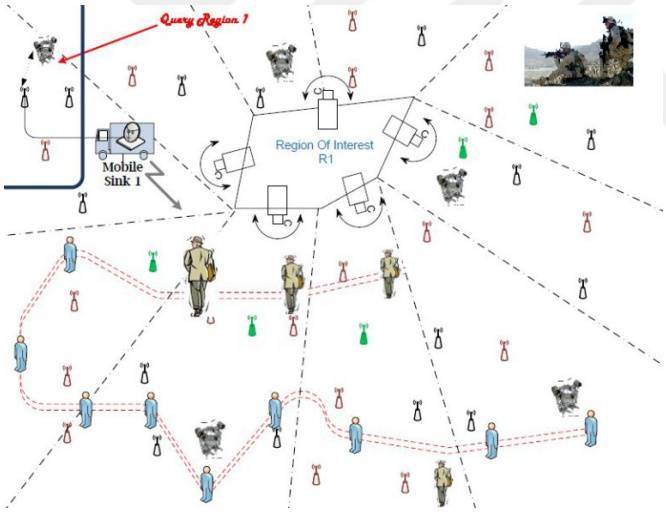


Figure 1.6: Reliability scheme in WSN.

- **Mobility:**

  This characteristic is the ability to control mobile nodes and variable data paths.

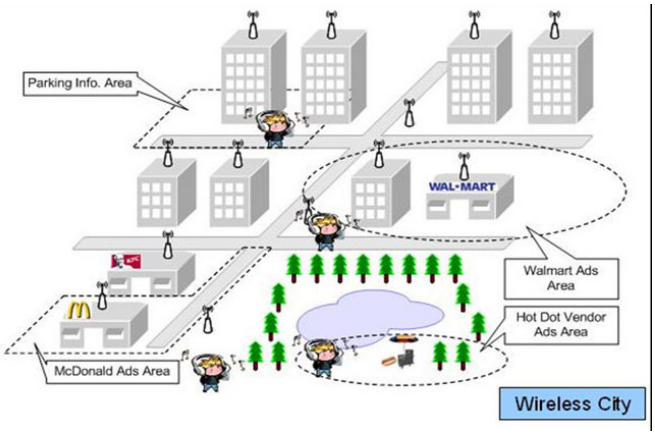


Figure 1.7: Mobility scheme in WSN.

1.2 Wireless Motes

A sensor node (*i.e.*, mote), is a node that acts computing, collecting and exchanging sensory data with other sensor nodes in the network system. In *mote selection* the most important factor is the lifetime of node in which various motes provide several technical specification which in turn have an impact on the lifetime of sensor nodes. In the preceding we will discuss some type of motes more specially MICA2 Motes which are utilised in our study.

- **TelosB Motes:**

  TelosB mote first designed and published to the research community by University of California, Berkeley. Figure 1.8 shows TelosB mote.

Figure 1.8: A representation of a TelosB Mote.

- **IRIS**

  This platform supports high communication range close to 500 meters in LoS and employs a 2.4 GHz IEEE 802.15.4 wireless module. Figure 1.9 is representing IRIS platform.

Figure 1.9: A representation of a IRIS Mote.

- **MICA2 Mote**

  The MICA2 Mote is a third generation mote module utilised in low-power, wireless sensor networks. This model is progressed version of MICA mote. It supports temperature, humidity and light sensors, and acts as an interface for connecting sensors. It is shown in Figure 1.10.

Figure 1.10: A representation of a Mica2 Mote.

1.3 Research Motivation

In WSNs, lifetime of network is one of the significant topics of study. Hence, studying the key roles of lifetime variation might be an important topic to study. In this case, focusing on the distinguished features of WSNs may help to find optimal solutions.

To achieve the longest possible lifetime for WSNs, each sensor node should function in a harmony with other nodes by forwarding the data packets gathered from the environment. There is a possibility of a new type of attack targeting on the lifetime of sensor nodes by disabling a certain group of sensor nodes which are most critical in obtaining optimal energy balancing. Such an attack is capable of decreasing network lifetime with elimination of the subset of sensor nodes. This process can be executed by physical eradication of a limited number of critical sensor nodes by adversaries. Furthermore, it is also possible that critical sensor nodes disabled due to natural risks such as landslides.

Note that the definition of critical nodes in our study is different from the general use in WSN literature where elimination of critical nodes results in network disconnection [16] whereas in our case, we presumed that the network is strongly connected, therefore, incapacitation of a few nodes do not result in network partitioning.

1.4 Problem Statement

With analysis of the previous studies on the lifetime of wireless sensor network and its affecting facotrs, reduction on the network lifetime due to the elimination of a subset of nodes critical in achieving maximal network lifetime is an important research topic left uninvestigated in the literature. The only study on the impact of sensor node elimination attacks on WSN lifetime is [49], which explored the effects of eliminating a single node only (*i.e.*, not a group of nodes). To analyse this problem under optimal functioning conditions we construct a novel Linear Programming (LP) framework and designed two algorithms based on the LP model. We do not make any assumptions on the causes of the elimination of critical nodes and focus on the impact of the incapacitation of the critical nodes on WSN lifetime.

1.5 Contribution

In the following we briefly indicate the contributions of this thesis as *Related Work and Background, Energy Saving in WSN, Proposed Approach, Experiments and Analysis, Conclusion*.

2. RELATED WORK AND BACKGROUND

2.1 WSNs Security

In WSNs, in principle, there exist some potential security threats, and regarding to the capability of attackers these threats can be categorised as :

External Attacks:

These attacks do not target on any internal data in the wireless network system such as cryptographic information. External attacks try to eavesdrop during communication between sensor nodes [33]. This act leads to some attacks such as jamming attacks, tampering, and replay attacks which are aiming to make network inoperable. Some properties of external attacks are :

- Outsider to the wireless network system
- Accomplished by unlawful parties
- Launch attack without authentication [8, 31]

Internal Attacks:

When a legal node treats as an illegal way, it can be considered as an internal attack. The important purposes of an internal attacker are :

- Targeting the performance of wireless network
- Hacking the public or private keys
- Compromising sensor nodes [31, 41].

In the next sections, we will further discuss about possible attacks and countermeasure solutions.

2.2 Mathematical Programming

Mathematical Programming framework initially published in a peer-reviewed scientific journal in 1971, that is, modelling of a problem with optimizing a function of many variables, and limited resources to achieve the best possible solution is known as Mathematical Programming. The solution of the problem is an optimal where it fulfils the objective function with respect to the existing constraints. Linear Programming (LP) and Mixed Integer Programming (MIP) are the special case of mathematical programming platform. These mathematical optimizations utilise linear objective functions both for objective and the problem constraints.

2.2.1 Linear programming

According to the objective function, a linear programming algorithm aims to find a point which has the least (or the most) value in case of existing of this point. Linear programming has the application in different fields. The application area in business, economics, and is broadly used in engineering problems.

A linear programming (LP) formulation is used in our case to optimize the lifetime of network system.

2.2.2 Mixed integer programming

A mixed-integer programming (MIP) problem is one where some of the decision variables are constrained to be integer values (i.e. whole numbers such as -1, 0, 1, 2, etc.) at the optimal solution.

2.3 MAC Layer

Media Access Control layer also called physical address is one of two sublayers of the data link protocol. MAC layer is a unique identifier assigned to network interfaces, and is related to sharing the physical connection of the network system. It decides which node can access to the physical channel and which one can transmit and when is its turn to send data to the network system. Thereby, MAC plays and important role in the performance of a sensor network where numerous users can transmit simultaneously over the same channel (Ethernet segment, same radio channel, etc.), such as IEEE 802.11, Bluetooth, etc. The most frequent MAC layer standards are CSMA/CD and CSMA/CA, which are applied in Ethernet and Wi-Fi protocols.

In principle, MAC layer can be grouped into two classes: *contention-based and contention-free protocols*.

Contention occurs when two adjacent sensor nodes both try access the communication channel. Contention triggers data collisions, which are more expected to happen in the network especially when traffic is high, and eventually they have an impact on the performance of network which usually leads reduction on the lifetime of network system.

Contention free protocols

A MAC protocol is considered as a contention-free if it does not permit occurrence of collisions on the network. In all contention-free MAC protocols it is presumed that the sensor nodes are time-synchronized in some way. This type of MACs are partitioned into time slots. Each sensor node uses the time slot to transmit data packet which makes the collision free communication.

Slot-based protocols

This protocol [47] uses a beacon which helps to communicate with any two nodes of our network system. Time slot is divided to a subset of fixed slots. Here, active slots are responsible of maintaining the nodes to be in active mode, transmitting the beacons to adjacent nodes and listening for both data packet acknowledgement or requests from other adjacent nodes. Figure 2.1 shows the 7 slot times and the process of Slot-based protocol [50].

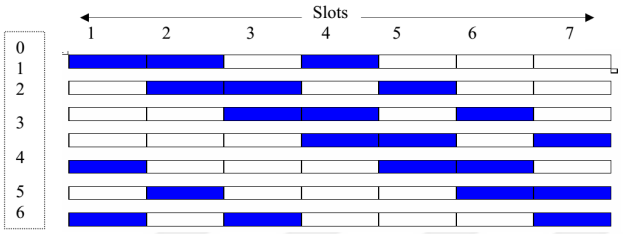


Figure 2.1: A scheme of Slot-based protocol.

Time Division Multiple Access (TDMA) protocols

TDMA is a digital technology of channel access that divides a same frequency channel into time slots in order to increase the amount of data that can be carried. Each time slot is utilized to send one byte or another segment of each signal in serial data format. This protocol is the most commonly used for compressed video, satellite systems and other high-speed data.

Employing TDMA protocol makes IDle-listening avoidable during the communication. Furthermore, the concern of MAC layer contention can be resolved by scheduling transmissions earlier, hence, when the radio turned on, the nodes may have more related information in advance and this leads to non-collision on the network system. Figure 2.3 illustrates time slot system in TDMA protocol. This method is hard to apply in multiple simultaneous transmissions, but is applicable in single hop communication.

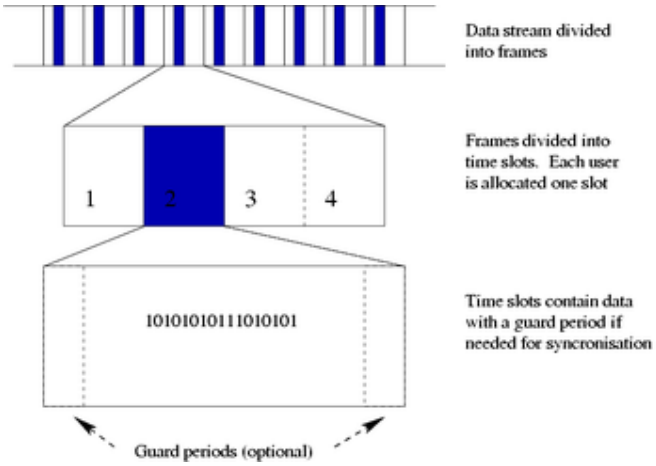


Figure 2.2: TDMA frame structure.

Traffic-Adaptive Medium Access (TRAMA) [37] is an energy efficient TDMA which is created related to Node Activation Multiple Access (NAMA)[43] for WSN. TRAMA divides time into time slot and provides time-slotted channel access for each node. Transmission scheduling is based on two-hop neighbourhood information and one-hop traffic information.

TRAMA's main goal is to obtain energy efficient while receiving data packets where the collision is bypassed. It permits the nodes which are not scheduled in transmission and reception, to employ a low power mode. Exploiting of low power mode can be regulated based on traffic pattern of network. *Random access period* is applied for synchronization and updating two-hop neighbor information. *Scheduled access period* is utilized for contention free data exchange between sensor nodes, and provides the capability of unicast, multicast and broadcast communication. To have energy efficiency TRAMA, it forces sensor nodes to sleep mode as long as possible.

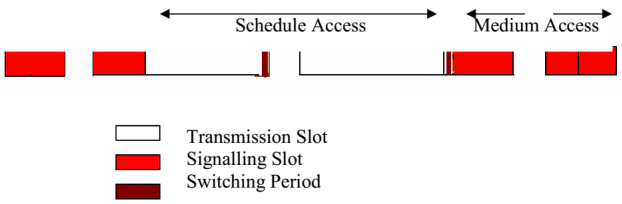


Figure 2.3: Time slot diagram.

Contention-based protocol (CBP)

Contention-based MAC protocol is a wireless communications protocol which permits multiple nodes to share in the single radio channel according to their

demand and without pre-coordination. This method tries to minimize collisions while in contention free methodology, stress was in avoiding collision. The "listen before talk" procedure is a most common example of CBP. This technology utilises a distributed algorithm (which allots the channel between communicating nodes) to decrease the probability of collision [13].

Conventional random access protocols like ALOHA [39] and Carrier Sense Multiple Access (CSMA) [29] are other two most popular contention-based protocols(CBP). Most of new wireless sensor networks [15, 17] still use them. In CSMA technique before transmission of data packets, stations sense the channel . This is because it just to guarantee that when started to send data, the channel is free, and in case of confronting with all busy channels, station (node) continuously sense channel till the channel be free to transmit data packet.

Nonetheless, in multi-hop communication networks this technique has a problem when faced with hidden nodes. In such networks, owing to lacking in radio frequency coverage as can be seen in Figure 2.4 station (node) n1 tries to communicate with node n2, and due to inadequate radio coverage node n1 can not send a message directly to node n2, n1 then attempts to transmit data via relaying nodes which are adjacent to n2 (here R is intermediate node). Since node n2 is not informed of this data transmission and at the same time n2 may launch to send a packet to node R which as a result leads a collision in the network. Extra signalling control messages is introduced to overcome such problem. A technique known as Busy Tone Multiple Access [29] almost handle the hidden node problem by transmitting busy tone in the middle of transmission so that other nodes will be aware of such transmission and thereby they avoid to send data.

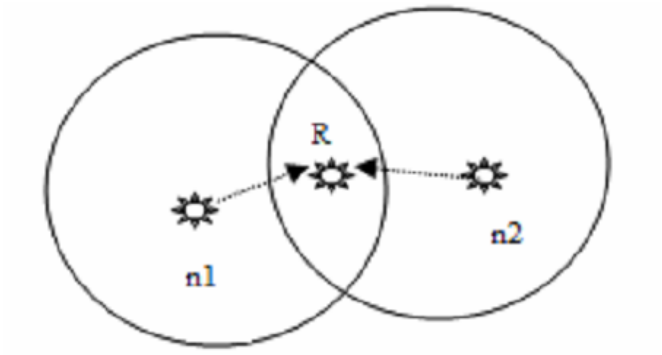


Figure 2.4: Hidden node Problem.

Sensor MAC (S-MAC)

S-MAC is a medium-access control (MAC) protocol in sensor networks which supports multi-hop functioning, and aims to minimize energy consumption

owing to overhearing, idle listening/sleeping, and collision [11, 18]. This protocol is a contention-based protocol with low duty cycle and decreases energy consumption in idle listening by allowing neighbouring nodes from virtual clusters to set up a common sleep schedule during transmission, if two adjacent nodes lie in different virtual clusters, then go to wake up mode at listen periods of both clusters. Hence, this process puts nodes into low duty cycle. S-MAC listen sleep schedule is illustrated in Figure 2.6 [47]. In this approach sensor nodes exchange their sleeping schedule and transmits this data as SYNC packet by broadcasting to adjacent nodes before going to sleep mode. Other sensor nodes sense this packet and act as following:

In case of not receiving packet, generate a new packet (sleep schedule packet). If it does not belong to adjacent nodes, discard it. if two nodes want to start a communication, sender exploits single RTS (request to send). In case of receiving by not related node, replies with CTS (clear to send). Consequently, after finishing this transaction, all nodes go to sleep mode.

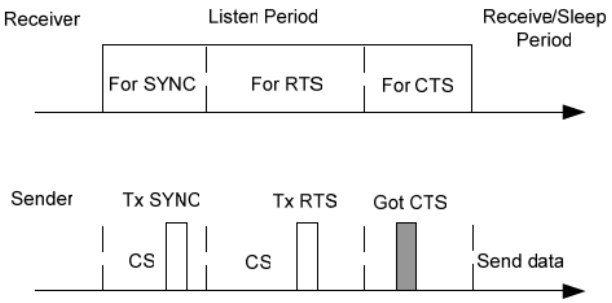


Figure 2.5: S-MAC Messaging Scenario.

Time Out MAC (T-MAC)

S-MAC has some disadvantages such as :

a) Broadcasting data packets do not use RTS/CTS which can enhances collision probability.

b) Idle listening has a fixed duty cycle which wastes energy when traffic is low while duty cycle is tuned for high traffic and it also reduces the throughputs when traffic is high while duty cycle is made for low traffic.

c) When the packet is not addressed to the listening node, sleep and listen periods are constant, which reduces the performance of the algorithm.

T-MAC is designed to solve aforementioned problems by employing adaptive duty cycle. In case of no movement in its adjacency, the sensor node goes to sleep mode. But, this protocol consumes more energy in variable traffic when compared to S-MAC.

Figure 2.6 represents the procedures of S-MAC and T-MAC in which S-MAC has fixed active windows while adaptive T-MAC has variable active windows that prolong as long as messages are received or other activation events occur.

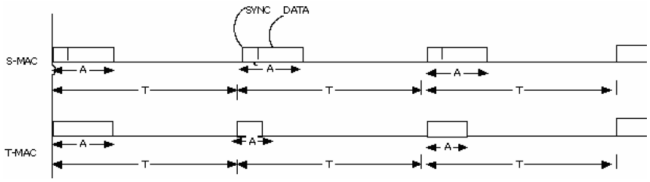


Figure 2.6: The scheme of S-MAC and T-MAC.

3. ENERGY SAVING IN WSN

3.1 Energy Saving at Node Level

In this section, the basic components of sensor node, and the node structure are explored.

In principle, energy saving methods can be categorised in two levels:

Device Level

At this level, the component of hardware is determined and then the required configuration is assigned, to achieve the longest possible lifetime which is the minimum energy consumption in a sensor node.

Network Level

At this level, routing techniques, communication methods and protocols to save energy consumption is chosen.

Generally, a sensor node is described in three parts, *processor, sensor and power unit*.

Overall Design:

A sensor node is composed of four primary parts: *power, transceiver, sensing and processing units*. The basic block diagram of wireless sensor node is shown in Figure 3.1.

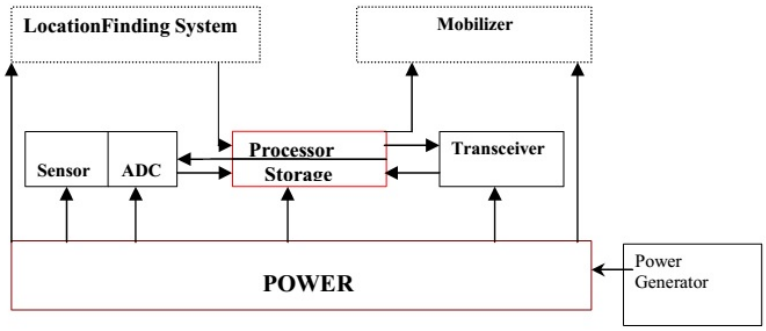


Figure 3.1: The basic block diagram of the WSN.

Processing Unit:

This unit which is resided on the micro-controller, is used for reading sensory data and makes them ready for transmission. The main functionality of this part as is clear from its name, is for computation in sensor node. Other responsibilities of this part are: *Regulation of task scheduling, energy computation, determination of communication protocols, data manipulation, per se*. Hence, this part plays a significant role in sensor nodes in which necessitates selection of an appropriate energy-efficient processor for our network system.

The energy consumption of processor depends on the operating voltage, duty-cycle internal logic and basically relies with the time it stays at sleep mode. Since, the sleep mode has direct connection with the operation of node.

There exists different micro-controllers which each one has a different property and distinctive features such as operating voltage, channel, RAM, Bits, Flash, and energy consumption (Idle, active, and power down mode). In the literature, micro-controllers and a comparison of some of them are studied in[21,22].

Sensor:

Sensor unit is the channel to communicate between the physical environment and the processing unit. This unit is one of the significant parts of WSNs. It collects sensory data such as humidity or temperature by sensing of environment, and sends this data to the processor unit. Then, processor unit checks the received data and decides where it has to go. According to the routing protocols, forwards data to other sensor nodes or transmits the data directly to the base station. Sensor performs as a transducer and changes over energy from one format to another format. Sensor can be recognized in view of what kind of energy they identify or transmit to the system.

Radio and Transceiver:

This part uses the most energy consumption in the WSNs. Energy conservation usually uses three methods to minimize data packet overhead in wireless sensor networks [5, 27], namely *duty cycling, data-driven, and mobility based* techniques.

Duty Cycling:

This method uses two various and supportive techniques as illustrated in Figure 3.2. It is possible to use node redundancy and adaptively choose just a minimum subset of nodes to stay in active mode for prolonging the connectivity in the network system. Sensor nodes with no need to be connected can switch to sleep mode which saves energy. Here, finding minimum subset of nodes that also ensures the connectivity, is the responsibility of topology control. Active nodes which are elected by the topology control protocol, as they do not need to be connected and also do not need to preserve their radio ceaseless on, they switch off their radios (*i.e.*, put it in the low-power sleep mode) when network activity does not exist in the network system, thus, interchanging between sleep and active modes. All over, we mention to duty cycling

performed on active nodes as power management. Consequently, topology control and power management act as interrelated methods in which roughly effectuate duty cycling. Power management protocols can be executed as *sleep/active protocols (i.e., sleep/wake-up protocols) or MAC protocols with low duty-cycle*.

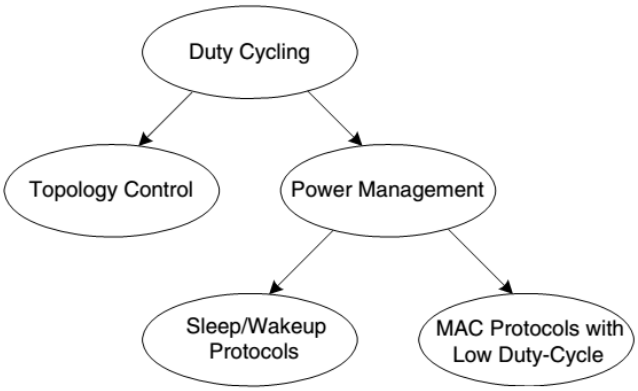


Figure 3.2: Duty cycling scheme.

Sleep/Active protocol:

This part is performing on the top of a MAC protocol and resided on the network or application layer. It allows more flexibility to adopt itself when needed to the application necessity, and, in general, can be employed with any MAC protocol.

MAC with low duty-cycle:

This method allows to optimize medium access approaches regarding to the particular sleep/active pattern applied for power management.

Data-driven Methods:

This part involves *data reduction and energy efficient data acquisition*.

Data reduction:

This technique as shown in Figure 3.3 divided into three subsets as *in-network processing, data compression, and data prediction.* The objective of these methods is minimizing the amount of data routing to the base station (*i.e.*, sink node).

Data compression:

This model can be used to decrease the amount of data packet transmitted by source nodes. This frame incorporates encoding all generated data at source nodes, and also decoding it at the base station. There exist various techniques to compress data which is studied in [35, 42, 45, 46]. Since these compressing techniques are not only related to the WSNs, we do not go to the details of this concept.

In-network processing:

In-network processing model has an essential feature in operating data aggregation (*e.g.*, calculating average of some data values) at intermediate nodes between the source nodes and the base station. In this case, the amount of data packet routing towards the base station will be decreased, and also the communication cost will be decreased. Since data aggregation is known as an application-specific, we will not talk about it in the remaining of this work. The concerned reader can see in [23] for a detail.

Data prediction:

Data prediction places both at sensor nodes and the base station. It roles in creating an evaluated data summary based on the sensory data. This technique uses sensor nodes to predicts the values of sensory data that is gathered from monitoring area. In general, this model reduces the required energy of communication in the network and also minimizes the amount of data which is transmitted by source nodes.

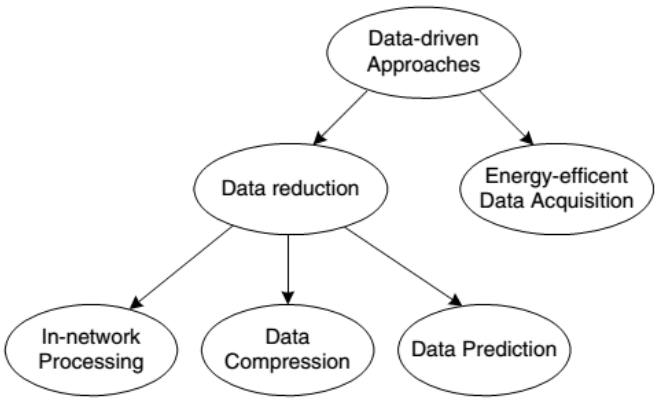


Figure 3.3: Data-driven methods to energy conservation.

Mobility-based scheme:

This model as can be seen in 3.4 is composed of two sub-models as *mobile-sink and mobile-relay*. The significant point when studying mobility scheme, is the kind of

control that the designer of wireless sensor network has on the mobility of nodes. In this case, controlling the environment would be more difficult. With following a specific plan such as public transportation, it can be predictable mobility. In other case, it might exist a random behavior which makes the prediction of the mobility untrustworthy. Eventually, the last case is neighter predictable nor random. Since in our work we are not interested in the mobility scheme, the interested readers can find further information in [6, 28]

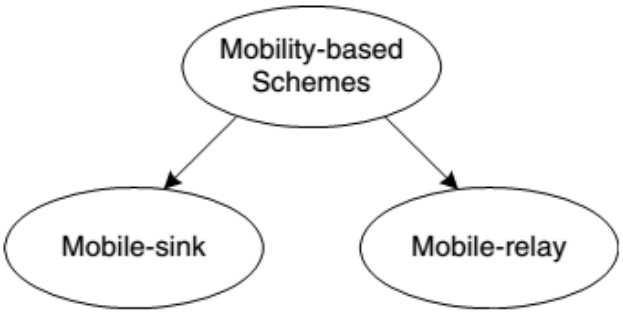


Figure 3.4: Mobility-based energy conservation schemes.

3.2 Energy Efficient of MAC Protocols

Medium Access Control (MAC) provides channel access control that enables sensor nodes to communicate in a shared network medium. The MAC layer is one of two sublayers that performs as an interface between the data link layer and the physical layer of the network. It uses MAC protocols to guarantee of no collision in the network for the signals transmitted from different sources upon the same channel. Moreover, it is responsible for coordinating adjacent nodes in WSNs, and making energy usage of network more efficient. Major amount of energy can be both saved or wasted regarding to the performance of this layer.

Collision

IF a collision happens in the network, it necessitates re-sending for those collided data packets, which causes an extra energy consumption. This event can be avoided before happening so that saving energy in the network system.

Idle listening

Duration of time where transceiver is active, but, neither data transmitted nor received by a sensor node. At this mode, node still attempts to monitor sensory data which is wasting of energy. To save the energy consumption, a sensor node should turn off its radio as long as possible.

Control - packet overhead

The operations of transmission, reception and listening of network overhead packets entail energy consumption. To save energy, the amount of these packets should be minimized.

Overhearing

This mode mostly appears when there exists high traffic in network and sensor node receives a data packet which does not belong to that node and is marked to some other sensor nodes in WSNs. This event leads wasting energy due to extra operations that have.

All above mentioned points can be considered by an energy aware MAC protocol to save the energy consumption in WSN.

4. PROPOSED APPROACH

We utilized a novel mathematical optimization technique to model the impact of critical node elimination attacks on WSNs and explored the parameter space through numerical evaluations of the LP model. Since the lifetime of network is one of the most significant performance indicators in WSNs, and the possibility of decreasing this metric through various attacks by removal of a specific subset of nodes makes it possible for the adversaries to impede the performance of WSNs with a low risk of detection; we designed two algorithms to investigate the impact of elimination of these particular groups on the lifetime of WSNs. Sequential Algorithm in which we eliminate nodes sequentially, and Bulk Algorithm in which a subset of nodes will be removed all together. In Section 4.3.3 we will describe the details of each algorithms and their impacts on the performance of WSNs.

4.1 System Parameters

In our system we have used the following parameters:

Table 4.1: List of parameters employed in our system model

Variable	Description
N	Number of nodes
f_{ij}	Flow from node-i to node-j
s_i	Data generated at node-i at each round
E_{rx}	Energy consumption for receiving one bit of data
E_{tx}	Energy consumption for transmitting one bit of data
d_{ij}	Distance between node-i and node-j
$G = (V, E)$	Directed graph that represents network topology
V	Set of nodes, including the base station
W	Set of nodes, except the base station
E	Set of edges
e_i	Battery energy of node-i
t	lifetime of network at each round
$R_{max}^{(l)}$	maximum transmission range at power level-l
$R_{max}^{(l-max)}$	maximum transmission range at maximum power level

In WSNs there is a restricted computational capabilities in the WSN node due to the limited energy resources. In our system model, the greatest part of energy consumption of sensor nodes is spent by communication energy. Hence, we ignore the sensing and computation energy dissipations [10, 25] each sensor node is initialized with the constant amount of energy.

The nodes we are dealing with, are acting as either sensors or relays, the key parameters of energy consumption are the energy required to sense a bit (E_{sens}), receive a bit (E_{rx}) and transmit one bit of data (E_{tx}) over a distance of d. Due to main part of this energy consumption is spent for transmission and reception, we ignore the sensing energy in our system model. Furthermore, additional energy is spent in transmission when compared to the reception of one bit data [36].

Although, the amount of consumption of energy for transmission is roughly the same as that spent for computation of thousand functions in a sensor node [5, 34]. To extend lifetime of a sensor network, various protocols and routing techniques such as duty-cycling, data-driven, and mobility are introduced [4]. However, to achieve the longest possible lifetime for WSNs, nodes should cooperate in relaying the data acquired from the circumstances. In such environments, it is possible to design a novel attack type to reduce the lifetime of sensor nodes by incapacitating a specific group of sensor nodes that are critical in achieving optimal energy balancing. Further information about aforementioned energy factors will be discussed in 4.3.

4.1.1 Overhead in WSNs

In wireless sensor networks, a data packet generated by sensor node(s) must be transmitted to the base station either directly or through intermediate nodes. There will be a problem in this communication when some nodes fail to relay and route the received data packets due to insufficient energy in a sensor node or because of other attacks which make a node inoperable.

To increase the reliability of the network system, there is a solution of introducing multiple paths for routing the same data packet via each of them which adds more traffic on our network system [30]. This method has been introduced in [24] which presents a novel technique to discover multiple paths from source to destination with efficient energy. In [19] a novel model of data separation to subdue overhead problem in WSNs is proposed. This methodology tries to regulate the trade-off between reliability and traffic of network system. It helps to reduce the data traffic overhead, but still has weakness in the reliability. In the following we will analyse the data overhead with multiple contributing factors in WSNs:

Scalability and Reliability

Wireless network system which is usually built with random distribution (without any predetermined topology), each node is in quest of communicating with other sensor nodes which might injects more data packets than required. These additional packets known as "network overhead" or "control packet". Routing protocols are examples of the overhead. In such networks systems, with increasing number of nodes, the network overhead raises too, and building a secure and reliable network

becomes more complex. Furthermore, communication links are more exposed to be broken in routing paths of large networks, which in turn leads to inject more network overhead packets, thus, increasing overhead.

Quick Responsiveness and Reliability

Responsiveness is the capability of the network in which network is flexible enough to adjust itself along with changing topology. To obtain this ability as high as possible, it necessitates more control packets in the network system which increases overhead.

Mobility and Reliability

Mobility in WSNs involves mobile nodes and entails high responsiveness to handle the mobility. As it seems, building a large mobile wireless networks would require high amounts of control packets, thereby, increasing overhead.

Power Efficiency and Reliability

Building energy efficient WSNs is another technique to decrease duty cycle of each node. In this method, to save more energy, sensor nodes remain more than usual in the sleep mode, this reduces the chance of successful communication among sensor nodes.

In our work we considered WSNs as consisting of stationary sensor nodes, and dissimilar to mobile networks (MANETs) changes are not happening frequently [9].

4.2 Attacks and Countermeasures in WSN

In WSNs, many vulnerabilities exist and sensor nodes are prone to various types of attacks including physical attacks of jamming and tampering of nodes; attacks on secrecy and authentication such as eavesdropping, packet replay attacks, and modification or spoofing of packets link attacks of collision, unfairness, and misdirection; attacks on network availability which are often referred as DoS attacks.

Denial of Sleep (DS) attacks as a specific type of denial-of-service (DoS) attack that targets a battery of nodes in the network in order to exhaust the limited energy of node resource which may reduce the sensor node's lifetime from years to days [12]. Cryptographic solutions such as authentication and encryption solutions have been proposed to protect the network from DoS attacks [20, 38]. Moreover, there are also other possibilities of attacks and vulnerabilities, such as physical destruction, natural threats like earthquakes, landslides and many other unconsidered risks, which can target on sensor nodes and make them unusable or perhaps permanently out of service.

Considering all types of these attacks and solutions against these attacks, many existing defence strategies are not adequate against these compromising attacks, and sensor nodes are still vulnerable to the specific upcoming attacks. Such an attack has the potential to reduce the network lifetime disproportionately with the number of sensor nodes eliminated.

Elimination of nodes can be achieved through physical destruction of a limited number of critical sensor nodes or remote node capture attacks by adversaries. Furthermore, it is also possible that critical sensor nodes incapacitated due to natural risks such as landslides. Note that the definition of critical nodes in our study is different from the general use in WSN literature where elimination of critical nodes results in network disconnection [16] whereas in our case, we assume that the network is strongly connected, therefore, incapacitation of a few nodes do not result in network partitioning.

Reduction in network lifetime due to the elimination of a subset of nodes critical in achieving maximal network lifetime is an important research topic left uninvestigated in the literature. The only study on the impact of node elimination attacks on WSN lifetime is [49], which explored the effects of eliminating a single node only (*i.e.*, not a group of nodes). To analyse this problem under optimal operating conditions we construct a novel Linear Programming (LP) framework and designed two algorithms based on the LP model. We do not make any assumptions on the causes of the elimination of critical nodes and focus on the impact of the incapacitation of the critical nodes on WSN lifetime, per se.

4.3 System Model

In this section, first, the research problem will be proposed. Then, the LP optimization formula will be introduced in the following context.

4.3.1 Problem definition

During lifetime of our network system, sensor nodes are responsible for sensing environment to produce meaningful data and forwarding this information toward the base station. In other words, sensor nodes are capable of transmitting their own generated data, and also forwarding data from other sensor nodes to the base station as a relay node.

During sensing, a node collects events that are happening in the environment (*e.g.*, temperature, humidity, pressure) and then transmits this sensory data to the base station either by relying or directly. Since sensor nodes are self-organized, they decide whether to send data directly or forward via intermediate nodes to the base station, according to the distance of the current node and its remainder energy. During this communication, sensor nodes are more exposed to the possible threats which try to make some nodes incapable in the network. Meantime, physical destruction can be made or even some node may exhaust all of its battery power due to the external attacks or threats like landslide. In this case, the remaining nodes taking over the responsibility of the inoperable nodes, to perform their tasks.

In our network model, there exists a single base station at the center of the disc shaped network deployment area and multiple sensor nodes (*i.e.*, N_S sensor nodes), which are randomly distributed at the disk shaped network. Each sensor node-i generates s_i amount of data periodically and all generated data terminates at the base

station. All sensor nodes are able to relay the data on behalf of other nodes towards the base station.

The network topology is represented by a directed graph, $G = (V, E)$, where V is the set of all sensor nodes and the base station is defined as node n_1. We also define a set W , which includes all nodes except node-1 ($W = V \setminus \{n_1\}$). E= $\{(i, j) : i \in W, j \in V - i\}$ is the set of links. Note that by definition no node sends data to itself. The objective function is the maximization of t (the minimum lifetime of all sensor nodes). We adopt the network lifetime definition given in [14], which is the time when the first sensor node exhausts all of its battery power.

Since the objective is maximization of the lifetime which is common for all nodes, all sensor nodes cooperate to extend the lifetime as much as possible through network wide energy balancing, hence, all nodes deplete their batteries at the end of the network lifetime.

4.3.2 LP model

Linear programming (LP) is an optimization technique to achieve the best results in a mathematical model [1]. LP has a linear objective function (or multiple linear objective functions) , linear equality and inequality constraints whose solutions can be found by employing popular and well known available software [32]. In this work, we present the LP framework with an objective function of maximization in WSNs to model the impact of critical node elimination attacks on WSNs and explore the parameter space through numerical evaluations.

Maximize $\sum_{i \in W} S_i t$

Subject to:

$$f_{ij} \geq 0 \; \forall (i, j) \in E \tag{4.1}$$

$$\sum_{j \in V} f_{ij} - \sum_{j \in W} f_{ji} = s_i t \; \forall i \in W \tag{4.2}$$

$$\sum_{j \in V} E^{opt}_{tx,ij} f_{ij} + E_{rx} \sum_{j \in W} f_{ji} \leq e_i \; \forall i \in W \tag{4.3}$$

$$e_i = \varepsilon \; \forall i \in W \tag{4.4}$$

Equation 4.1 states that all flows are non-negative. Equation 4.2 is the flow balancing constraint and states that for all nodes except the base station, the difference between the amount of data flowing out of node-i and the amount of data flowing into node-i is equal to the amount of total data generated by node-i.

Furthermore, all generated data by the sensor nodes terminate at the base station (incoming flow plus self produced data must be equal to the outgoing flow).
Equation 3 presents the energy dissipation constraint for sensor nodes. The amount of energy dissipated on transmission and reception is limited by the initial energy of sensor nodes (e_i).

Table 4.2: Transmission energy consumption ($E_{tx}(l)$ – nJ/bit) and transmission range ($R_{max}(l)$ – m) at each power level (l) for the Mica2 motes as a function of power level [48]. Energy dissipation for reception of data is constant ($E_{rx} =$ 922 nJ/bit).

l	$E_{tx}(l)$	$R_{max}(l)$	l	$E_{tx}(l)$	$R_{max}(l)$
1 (l_{min})	671.88	19.3	14	843.75	41.19
2	687.50	20.46	15	867.19	43.67
3	703.13	21.69	16	1078.13	46.29
4	705.73	22.69	17	1132.81	49.07
5	710.94	24.38	18	1135.42	52.01
6	723.96	25.84	19	1179.69	55.13
7	726.56	27.39	20	1234.38	58.44
8	742.19	29.03	21	1312.50	61.95
9	757.81	30.78	22	1343.75	65.67
10	773.44	32.62	23	1445.31	69.61
11	789.06	34.58	24	1500.01	73.79
12	812.50	36.66	25	1664.06	78.22
13	828.13	38.86	26 (l_{max})	1984.38	82.92

Furthermore, each sensor node is assigned with equal initial energy at the beginning of the network operation (*i.e.*, ($\varepsilon = 3J$) as stated in Equation 4. The optimal amount of energy to transmit one bit of data over a distance (d_{ij} , the distance between node-i and node-j) is represented by $E^{opt}_{tx,ij}$ and the energy to receive one bit of data is represented by E_{rx} . Experimentally determined energy dissipation and transmission ranges for Mica2 mote platform are presented in Table 4.2 [9] where energy consumption for transmission power level-l is denoted as $E_{tx}(l)$ and the maximum transmission range at this level is indicated as $R_{max}(l)$.

Note that, transmission power takes a value from a finite set denoted as S_L (*i.e.*, there are 26 power levels to choose). While the energy required for transmitting one bit depends on the distance between source and destination, the energy required for receiving does not and it has a constant value ($E_{rx} = 0.922J/bit$). If d_{ij} is greater than maximum transmission range (*i.e.*, $R_{max}(26) = 82.92m$), no data can be sent from node-i to node-j. Each sensor node chooses its optimal transmission energy for each outgoing link as presented in Equation 5.

$$E^{opt}_{tx,ij} = \begin{Bmatrix} E^{(l-1)}_{tx} \; if \; d_{ij} \leq R^{(l-1)}_{max} \\ \infty \; else \; if \; d_{ij} > R^{(l-26)}_{max} \\ E^{(l+1)}_{tx} \; else \; if \; R^{(l)}_{max} < d_{ij} \leq R^{(l+1)}_{max} \end{Bmatrix} \tag{4.5}$$

4.3.3 Algorithm model

After formulation of an LP model for the maximization of network lifetime, the next step is to build an algorithm for determining the most critical nodes in the network which removal of these nodes from the network topology will reduce the network lifetime the most. Note that we assume the network is strongly connected and elimination of nodes (up to a certain limit) will not result in network partitioning. If we want to determine a single critical node which reduces the network lifetime the most, we can run the LP model for the given network topology with $(N_S - 1)$ sensor nodes for N_S times (*i.e.*, one node at a time is removed from the network and the lifetime is computed). Thus, the most critical node will be the node that gives the lowest lifetime when removed. Furthermore, removal of certain nodes will not reduce the network lifetime at all.

To the contrary, removal of certain nodes will result in a net increase in network lifetime. Although, determining the single most critical node can be done in N_S runs of the LP model, determining a group of critical sensors nodes that reduce the lifetime most is not straightforward. We can use a sequential algorithm (Algorithm 1) to determine N_C critical nodes which determines the most critical node in N_S runs then proceeds with remaining nodes to determine the second most critical node in another $N_S - 1$ runs until N_C most critical nodes are determined in N_C steps in a total of $N_C N_S$ - $\frac{N_C(N_C-1)}{2}$ runs of the LP model.

Alternatively we can determine the most critical N_C nodes by considering their combined impact on network lifetime (Algorithm 2). Therefore, all combinations of N_C nodes among the total N_S nodes should be removed from the network and the lifetime values in the absence of all groups should be computed which necessitates a total of $\binom{N_S}{N_C} = \frac{N_S!}{N_C!(N_S-N_C)!}$ runs of the LP model.

Algorithm 1 takes as input a network topology as a graph of nodes and edges $G = (V, E)$, the number of critical nodes to be found (N_C), and the mode of execution (mod) that determines whether a lifetime minimization or maximization objective is sought. In return Algorithm 1 finds an ordered set of N_C critical nodes (C) and the network lifetimes when each critical node is removed from G in the given order in C. If the mode is 'max' then the network lifetime found is maximum or minimum in the case the mode is 'min'.

The algorithm iterates N_C times (line 1) and in each iteration finds one critical node (line 10-11) that minimizes or maximizes the network lifetime (line 8-9) when it is removed from the network (line 8) by iterating over all nodes (line 7). The algorithm works sequentially, in which the critical nodes found are successively removed one by one from the network and in each case each removal (without replacement) minimizes/maximizes the network lifetime.

Algorithm 2 on the other hand, finds N_C critical nodes at once. In this case, N_C critical nodes are removed from the network altogether (line 8) which minimizes/maximizes the network lifetime.

Algorithm 1: Sequential Critical Node Selection

Input : $G = (V, E)$: a network topology graph
N_C: the number of critical nodes
mod: $'min'$ or $'max'$ for minimizing or maximizing the network lifetime with the removal of critical nodes

Output: $C = \{(v_i, lt_j)$: ordered set of critical nodes
$v_i , v_j \in V$, $1 \leq j \leq n$,
lt: when v_1 to v_j removed from G $\}$

Output: $C = \{(v_j, lt_j)$: ordered set of critical nodes v_j, $v_j \; \varepsilon \; V$, $1 \leq j \leq n$, and the network lifetime lt_j when v_1 to v_j removed from G $\}$

```
for k=1 to n do
    if mod='max' then
        C_k.lifeTime = 0
    else
        C_k.lifeTime = ∞
    end
    foreach v_i ε V for 1 ≤ i ≤ |V| do
        lt_i ← lifeTime(G\v_i)
        if (mod='max' and lt_i > C_k.lifeTime) or (mod='min' and
          lt_i < C_k.lifeTime) then
            C_k.criticalNode = v_i
            C_k.lifeTime = lt_i
        end
    end
                        ▷ remove the critical node from G, removal of which gives
      maximizes/minimizes life time
    G ← G\C_k.criticalNode
end
return C
```

Algorithm 2: Bulk Critical Node Selection

Input : $G = (V, E)$: a network topology graph
N_C: the number of critical nodes
mod: $'min'$ or $'max'$ for minimizing or maximizing the network lifetime with the removal of critical nodes

Output: $C = \{(v_j)\text{: } v_j \; \varepsilon \; V,\ 1 \leq \ j \leq n \; \}$: set of critical nodes
lt: min. or max. lifetime of G after removal of critical nodes C

```
1  C ← φ
2  while tempC=chooseNextNNodes(G,n) do
3      if mod=max then
4          lt = 0
5      else
6          lt = ∞
7      end
8      tempLT ← lifeTime(G\tempC)
9      if (mod=max and tempLT > lt) or (mod=min and tempLT < lt) then
10         C ← tempC
11         lt ← tempLT
12     end
13 end
14 return C, lt
```

5. EXPERIMENTS AND ANALYSIS

In this section, we explore the impact of elimination of the most critical sensor nodes on WSN lifetime through numerical evaluations of the Algorithm 1 and Algorithm 2 which utilize the LP model for lifetime maximization.

We use General Algebraic Modelling System (GAMS) with XPRESS solver for the numerical analysis of the LP problems. We present the averages of 100 runs for statistical significance (*i.e.*, sensor node distributions over the disc shaped network area is regenerated using a uniform random distribution 100 times and the results are averaged).

In Figure 5.1 and 5.2, we present network lifetime change curves as functions of network radius (R_{Net}) when N_S = 50. Negative values indicate decrease in network lifetime when compared to the original network topology (before elimination of any sensor nodes) and positive values indicate increase in network lifetime. Average lifetime decrease by the removal of a single node is denoted as AMD-1 whereas average lifetime decrease due the removal of two nodes are denoted as AMD-2 and so on. Likewise, average lifetime increase due to the removal of one to five sensor nodes are denoted as AMI-1, . . . , AMI-5, respectively. Furthermore, the maximum lifetime decrease due to sensor node removals (*i.e.*, the largest value encountered in all runs) are denoted as MD-X where X is the number of removed sensor nodes. In a similar way, the maximum lifetime increase are denoted as MI-X, respectively.

The impact of elimination of critical nodes is more severe in sparser networks which is manifested by the increase (of absolute values) in all curves as the network radius increase. For example, in Figure 5.1 when N_C = 2 average network lifetime decreases (i.e., AMD-2) are 6.9%, 24.6%, and 35.1% for networks with radii 100 m, 150 m, and 200 m, respectively.

The average decrease in network lifetime can be as high as 20.2% (AMD-1) and 64.0% (AMD-5) when R_{Net} = 200 m. As expected, as the number of critical nodes increase the impact on the lifetime also increases. For example, average lifetime decreases with 200 m radius are 20.2%, 48.6%, and 64.0% for N_C = 1, 3, and 5, respectively. The maximum decrease for a given parameter set is much higher than the average decrease value throughout the parameter space. For example, the maximum reduction in network lifetime with 200 m radius and N_C = 2 (*i.e.*, MD-2) is 72.8% whereas the average decrease for the same network is 35.1%.

The maximum reduction in network lifetime increases as N_C increases (up to 86.4%). It is also possible to have increment in the network lifetime after removal of some of the nodes from the network. The reason for such behavior is that certain relay nodes dissipate unproportionately high energy to relay data and when these nodes are eliminated the burden of relaying on some relay nodes are lightened. Average increase in network lifetime can be extended from 3.1% (AMI-5 with R_{Net} =125 m) to

Table 5.1: Execution time

N_C	Execution time to find critical nodes	
	1 iteration	All topologies with confidence interval
1 Seq and Bulk	$\simeq$ 1 min	100 min ±10 sec
2 Seq	$\simeq$ 2 min	200 min ±20 sec
2 Bulk	$\simeq$ 11 min	1100 min ±50 sec
3 Seq	$\simeq$ 4 min	400 min ±25 sec
4 Seq	$\simeq$ 5 min	500 min ±35 sec
5 Seq	$\simeq$ 7 min	700 min ±40 sec

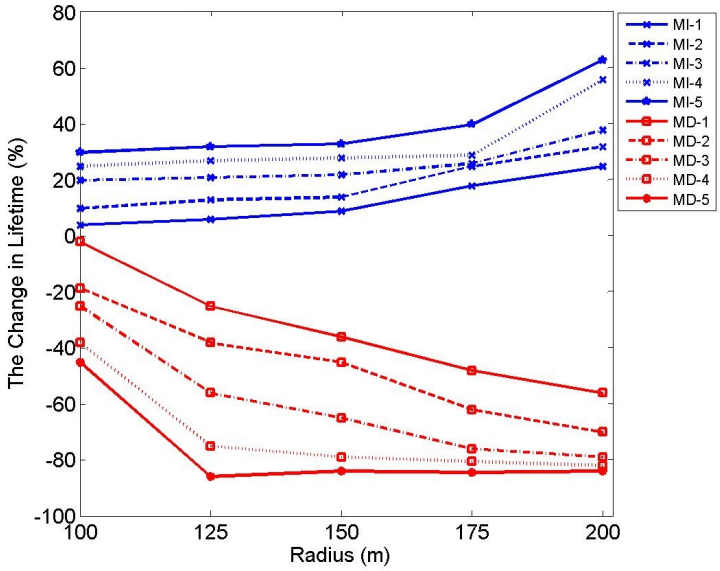
18.1% (AMI-5 with R_{Net} = 200 m).

On the other hand, the maximum increment in the lifetime is not high as the maximum decrements in the lifetime case. Our results reveal that the maximum increase in the network lifetime can be as high as 61.1% (AMI-5 with R_{Net} = 200 m).

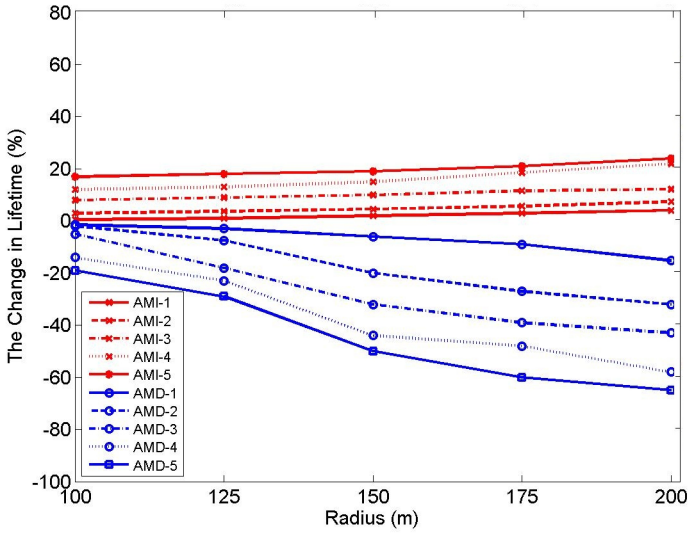
In Figure 5.2 we present the results for Algorithm 2 when N_C = 1 and 2 with the same network radii and N_S values. We cannot present the results of Algorithm 2 for N_C > 2 due to the prohibitively high computational complexity. For all of the numerical evaluations, we found that Algorithm 1 and Algorithm 2 give very close results. The difference between these two algorithms are upper bounded by 0.1% (AMD-2 with R_{Net} = 175 m). Hence, utilization of the sequential search algorithm is preferable over the bulk search algorithm because computational complexity of the bulk search is much higher higher than the sequential search algorithm.

In Table 5.1, we provide the execution time for evaluating the criticality of multiple critical nodes (1 iteration in the procedure), and the confidence interval using sequential and bulk search algorithm. We can see that the running time for a topology of N_S = 50 nodes is 50 second which means for finding one critical node among all combinations of N_S we need about 100 minutes (±10 seconds) to run either using sequential search algorithm or bulk algorithm. This execution time gets higher with increasing the number of critical nodes to be found. The execution times to find the second, third, forth, and five critical nodes among all sensor nodes are represented, respectively. Indeed finding the second critical node using bulk algorithm takes long time in which finding next critical node is not possible to find in a limited time.

We investigate the features of critical nodes (*e.g.*, proximity to the base station, number of neighbors, number of active links, amount of relayed data, and energy dissipated on relaying) which can be used to identify them when the network is deployed over a predetermined sensing area. We found that the probability of a node closer to the base station to be a critical node is higher than a farther away node, however, such a measure is not decisive (*i.e.*, although nodes closer to the network periphery has a lower probability of being a critical node, this probability is still well above zero). Likewise, all the aforementioned features fail to identify critical nodes without a non-negligible level of ambiguity.



(a)



(b)

Figure 5.1: Sequential Algorithm.

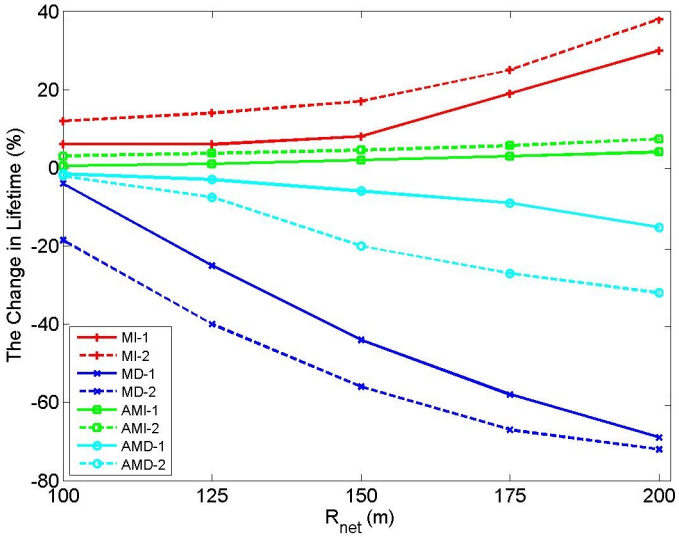


Figure 5.2: Bulk Algorithm.

6. CONCLUSIONS

In WSNs, sensor nodes are prone to sensor node failures due to many reasons such as security threats, natural hazards, hardware/software errors. Although there are some defensive strategies against these threats, yet they may not guarantee the security of all sensor nodes as well as the performance objectives of the entire WSN. Incapacitation of a group of sensor nodes can reduce the network lifetime significantly even such networks are operated by using ideal routing schemes to maximize the network lifetime.

In this study we constructed two algorithms (both based on a novel LP model), namely sequential search algorithm and Bulk search algorithm, to investigate the impact of elimination of critical nodes on WSN lifetime. After the identification of so-called critical nodes, we found that the average network lifetime decrease due to critical node elimination can be as high as 64.0% with a group of five critical nodes. According to our results, the maximum reduction in lifetime of WSNs when five critical nodes are removed is upper bounded by 86.4%.

The presented LP methodology can also be used for non-random deployments, which is the case for many WSN applications, to find the critical nodes and their impact on the overall performance. The results obtained here can be further improved considering another critical metric in WSN, i.e. the latency of WSNs. Future research in this area will focus on this particular case, studying the existing trade-off between latency and lifetime and the impact of critical nodes elimination on both metrics. In addition, we are going to provide some methodologies in a way to reduce the impact of critical nodes on the network performance, adding, for example, spare nodes in strategical positions.

REFERENCES

[1] **A. Abu -Baker, H. Huang, E. Johnson, S. Misra, R. Asorey -Cacheda, and M. Balakrishnan.** Maximizing *α* -lifetime of wireless sensor networks with solar energy sources. In *MILITARY COMMUNICATN CONFERENCE, MILCOM 2010*, pages125–129.IEEE,201.

[2] **K. Akkaya and M. Younis.** A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, 3(3):325–349, 2005.

[3] **I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci.** Wireless sensor networks: a survey. *Computer networks*, 38(4):393–422, 2002.

[4] **J. N. Al-Karaki and A. E. Kamal.** Routing techniques in wireless sensor networks: a survey. *IEEE wireless communications*, 11(6):6–28, 2004.

[5] **G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella.** Energy conservation in wireless sensor networks: A survey. *Ad hoc networks*, 7(3):537–568, 2009.

[6] **G. Anastasi , M. Conti , A. Passarella , and L. Pelusi** . Mobile -relay forwarding in opportunistic networks. *Adaptation and Cross Layer Design in Wireless Networks* , 21:389,2008.

[7] **J.Barcelo -Ordinas ,J.Chanet ,K.-M.Hou,and J.Garca -Vidal.** A survey of wireless sensor technologies applied to precision agriculture .In *Precision agriculture '13*, pages801–808.Springer,2013.

[8] **S. Bartariya and A. Rastogi.** Security in wireless sensor networks: Attacks and solutions. *environment*, 5(3), 2016.

[9] **A. U. Batmaz , H. U. Yildiz , and B. Tavli** . Role of unidirectionality and reverse path length on wireless sensor network lifetime . *IEEE Sensors Journal* ,14(11):3971 – 3982,2014.

[10] **M. Bhardwaj and A. P. Chandrakasan.** Upper bounds on the lifetime of wireless sensor networks. 2001.

[11] **V. Bharghavan , A. Demers , S. Shenker , and L. Zhang** . Macaw : a media access protocol forwireless lan's. *ACM SIGCOMM Computer Communication Review*,24 (4):212–225,1994.

[12] **K.Bicakci and B.Tavli.** Denial-of-service attacks and countermeasures in ieee 802. 11wirelessnetworks. *ComputerStandards&Interfaces*,31(5): 931–941,2009.

[13] **K.-S.Chan,L.K.Yeung,and W.Shao.** Contention-based mac protocols with erasure coding for wireless data networks. *Ad Hoc Networks*, 3(4):495–506,2005.

[14] **Z. Cheng , M. Perillo , and W. B. Heinzelman** . General network lifetime and cost models for evaluating sensor network deployment strategies. *IEEE Transactions on mobile computing*, 7(4):484–497,2008.

[15] **I. C. S. L. M. S. Committee et al.** Wireless lan medium access control (mac) and physical layer (phy) specifications, 1997.

[16] **O.Dagdeviren,K.Erciyes,and S.Tse.**Semi-asynchronous and distributed weighted connected dominating set algorithms for wireless sensor networks . *Computer Standards&Interfaces*, 42:143–156,2015.

[17] **E.Dahlman,P.Beming,J.Knutsson,F.Ovesjo,M.Persson,and C.Roobol.** wcdma-the radio interface for future mobile multimedia communications . *IEEE Transactions on vehicular technology*,47(4):1105–1118,1998.

[18] **I.Demirkol,C.Ersoy,F.Alagoz,et al**. Mac protocols for wireless sensor networks:a survey. *IEEE Communications Magazine*, 44(4):115–121,2006.

[19]**S.Dulman,T.Nieberg,J.Wu,andP.Havinga**.Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks. In *Wireless Communications and Networking,2003.WCNC 2003.2003 IEEE*,volume 3, pages 1918–1922.IEEE,2003.

[20] **D. Eddine et al.** A defense strategy against energy exhausting attacks in wireless sensor networks. 2013.

[21] **F. Electronics.** Motorola's microcontroller mc68hc908.

[22] **F. Electronics.** Types of microcontrollers.

[23] **E.Fasolo,M.Rossi,J.Widmer,and M.Zorzi.** In-network aggregation techniques for wireless sensor networks:asurvey. *IEEE Wireless Communications* ,14(2):70–87, 2007.

[24] **K. Guan and L.-M. He.** A novel energy efficient multi-path routing protocol for wireless sensor networks. In *2010 International Conference on Communications andMobileComputing*,2010.

[25] **W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan.** An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on wireless communications*, 1(4):660–670, 2002.

[26] **E. Hossain, Z. Han, and H. V. Poor.** *Smart grid communications and networking*. Cambridge University Press, 2012.

[27] **S. JAWAD ALI and P. Roy.** Energy saving methods in wireless sensor networks. 2008.

[28] **H. Jun , M . H. Ammar , and E. W . Zegura** . Power management in delay tolerant networks :a framework and knowledge -based mechanisms .In *SECON* ,volume 5, pages418–429,2005.

[29] **L.Kleinrock and F.Tobagi** .Packet switching in radio channels :Part i-carrier sense multiple -access modes and their throughput -delay characteristics . *IEEE transactions on Communications*, 23(12):1400–1416,1975.

[30]**S.P.Kori and R.Baghel.** Evaluation of communication overheads in wireless sensor networks . *International Journal of Engineering Research (ISSN : 2319 -6890) Volume*,(2):167–171.

[31] **C.-T. Li.** *Security of wireless sensor networks: current status and key issues* . INTECH Open Access Publisher, 2010.

[32] **H. Liu and X. Jia.** Linear programming approaches to optimization problems of energy efficiency in wireless ad hoc networks . *Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks* ,200:177–192,2005.

[33] **A. Perrig, J. Stankovic, and D. Wagner.** Security in wireless sensor networks . *Communications of the ACM*, 47(6):53–57, 2004.

[34] **G. J. Pottie and W. J. Kaiser.** Wireless integrated network sensors. . *Communications of the ACM*, 43(5):51–58, 2000.

[35] **S. S. Pradhan and K. Ramchandran** . Distributed source coding using syndromes (discus):Design and construction. *IEEE Transactions on Information Theory*,49(3): 626–643,2003.

[36**] V.Raghunathan,C.Schurgers,S.Park,and M.B.Srivastava.** Energy-aware wireless micro sensor networks. *IEEE Signal processing magazine*, 19(2):40–50,2002.

[37] **V.Rajendran,K.Obraczka,andJ.J.Garcia-Luna-Aceves**. Energy-efficient, collision -free medium access control for wireless sensor networks. *WirelessNetworks*,12(1): 63–78,2006.

[38] **D.R.Raymond,R.C.Marchany,M.I.Brownfield,andS.F**.**Midkiff**. Effects of denial -of-sleep attacks on wireless sensor network mac protocols . *IEEE transactions On vehicular technology*,58(1):367–380,2009.

[39] **L. G. Roberts** . Extensions of packet communication technology to a hand held personal terminal . In *Proceedings of the May 16-18, 1972 , spring joint computer conference*,pages295–298.ACM,1972.

[40] **K. Römer, O. Kasten, and F. Mattern.** Middleware challenges for wireless sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(4):59–61, Oct. 2002.

[41] **E. Shi and A. Perrig.** Designing secure sensor networks. *IEEE Wireless Communications*, 11(6):38–43, 2004.

[42] **C. Tang and C. S. Raghavendra.** Compression techniques for wireless sensor networks. In *Wireless sensor networks*, pages 207–231. Springer, 2004.

[43] **S.Tilak,N.B.Abu-Ghazaleh ,and W.Heinzelman** . A taxonomy of wireless micro-sensor network models . *ACM SIGMOBILE Mobile Computing and Communications Review*,6(2):28–36,2002.

[44]**S.Uludag,M.Karakus,and E.Guler.** Low-complexity 3d target tracking in wireless Aerial sensor networks. In *2014IEEEInternational Conference on Communications (ICC)*,pages373–378.IEEE,2014.

[45**] M.Wu and C.W.Chen.Multiple** Bit stream image transmission over wireless sensor networks. In *Sensors,2003.Proceedings of IEEE*, volume 2,pages 727–731.IEEE, 2003.

[46] **Z. Xiong, A. D. Liveris, and S. Cheng.** Distributed source coding for sensor networks. *IEEE Signal Processing Magazine*, 21(5):80–94, 2004.

[47] **W . Ye , J. Heidemann , and D. Estrin** . Medium access control with coordinated adaptive sleeping for wireless sensor networks . *IEEE /ACM Transactions on networking*,12(3):493–506,2004.

[48] **H.U.Yildiz,B.Tavli,and H.Yanikomeroglu** .Transmission power control for link-level handshaking in wireless sensor networks . *IEEE Sensors Journal* ,16(2):561– 576,2016.

[49]**A.Yuksel,E.Uzun,andB.Tavl**i. The impact of elimination of the most critical node on wireless sensor network lifetime .In *Sensors Applications Symposium (SAS), 2015 IEEE*,pages1–5.IEEE,2015.

[50] **R. Zheng, J. C. Hou, and L. Sha** . Asynchronous wakeup for ad hoc networks. In *Proceedings of the 4thACM international symposium on Mobile ad hoc networking&computing*,pages35–45.ACM,2003.

CURRICULUM VITAE

Given Name-Surname : Behnam Ojaghi Kahjogh

Nationality : Iranian

Date and Place of Birth : 1986- Urmia, Iran

E-Mail : bojaghikahjogh@etu.edu.tr

EDUCATION BACKGROUND:

- **Bachelor of Science** : 2009, Urmia University of Science and Technology , Faculty of Engineering, Department of Computer Engineering
- **Master of Science** : 2017, TOBB ETU, Department of Computer Engineering

FOREIGN LANGUAGES: English, Turkish, Farsi, Arabic

DERIVED PUBLICATIONS AND CONFERENCES FROM THIS THESIS:

- **HU.Yildiz, B.Tavli, BO.Kahjogh**. Assessment of wireless sensor network lifetime reduction due to elimination of critical node sets
  Signal Processing and Communications Applications Conference (SIU)- Antalya, Turkey - 2017
- **HU.Yildiz, B.Tavli, BO.Kahjogh, and E.Dogdu**. The Impact of Incapacitation of Multiple Critical Sensor Nodes on Wireless Sensor Network Lifetime
  IEEE Wireless Communications Letters - 2017

OTHER PUBLICATIONS:

- **BO.Kahjogh, J.Karimov, and E.Dogdu**. EDL:Framework for Entity disambiguation and Linking to knowledge bases.
  IEEE International Conference on Semantic Computing. 2016, California.
- **BO.Kahjogh, I.Demirkol, D.Careglio, and JD.Pascual**. The Impact of Critical Node Elimination on the Latency of Wireless Sensor Network.
  IEEE International Conference on Ubiquitous and Future Networks (ICUFN). 2017, Milan.
- **BO.Kahjogh, G.Bernstein**. Joint Energy and Latency Optimization in Software Defined Wireless Networking.
  IEEE International Conference on Ubiquitous and Future Networks (ICUFN). 2017, Milan.