Volume 6 • Issue 3 • June 2012

INTERNATIONAL JOURNAL OF

COMPUTER SCIENCE AND SECURITY (IJCSS)

ISSN : 1985-1553

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS

http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

VOLUME 6, ISSUE 3, 2012

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-1553

International Journal of Computer Science and Security is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCSS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND SECURITY (IJCSS)

Book: Volume 6, Issue 3, June 2012
Publishing Date: 20 - 06- 2012
ISSN (Online): 1985 -1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2012

EDITORIAL PREFACE

This is third issue of volume six of the International Journal of Computer Science and Security (IJCSS). IJCSS is an International refereed journal for publication of current research in computer science and computer security technologies. IJCSS publishes research papers dealing primarily with the technological aspects of computer science in general and computer security in particular. Publications of IJCSS are beneficial for researchers, academics, scholars, advanced students, practitioners, and those seeking an update on current experience, state of the art research theories and future prospects in relation to computer science in general but specific to computer security studies. Some important topics cover by IJCSS are databases, electronic commerce, multimedia, bioinformatics, signal processing, image processing, access control, computer security, cryptography, communications and data security, etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

This journal publishes new dissertations and state of the art research to target its readership that not only includes researchers, industrialists and scientist but also advanced students and practitioners. The aim of IJCSS is to publish research which is not only technically proficient, but contains innovation or information for our international readers. In order to position IJCSS as one of the top International journal in computer science and security, a group of highly valuable and senior International scholars are serving its Editorial Board who ensures that each issue must publish qualitative research articles from International research communities relevant to Computer science and security fields.

IJCSS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCSS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Science and Security (IJCSS)

EDITORIAL BOARD

Dr. Parvinder Singh
University of Sc. & Tech
India

Assistant Professor Vishal Bharti
Maharishi Dayanand University,
India

TABLE OF CONTENTS

Volume 6, Issue 3, June 2012

Pages

Performance Evaluation of Mini-sinks Mobility Using Multiple Paths in Wireless Sensor Networks

David Fotue *david.fotue@uni.lu*
Interdisciplinary Centre for Security
Reliability and Trust (SnT)
6, rue Richard Coudenhove-Kalergi, L-1359, Luxembourg

Houda Labiod *houda.labiod@telecom-paristech.fr*
Informatique Réseaux et Sécurité (INFRES)
Télécom ParisTech
46 rue Barrault, 75013, France

Thomas Engel *thomas.engel@uni.lu*
Interdisciplinary Centre for Security
Reliability and Trust (SnT)
6, rue Richard Coudenhove-Kalergi, L-1359, Luxembourg

Abstract

This paper presents a new approach based on the use of many data collectors, which we designate Mini-Sinks (MSs), instead of a single sink to collect the data in order to improve Wireless Sensor Network (WSN) performance. One or mode MS are mobile and move according to a controlled arbitrary mobility inside the sensor field in order to maintain a fully-connected network topology, collecting data within their coverage areas and forwarding it towards the single main sink. Energy Conserving Routing Protocol (ECRP), based on route diversity, is implemented in MSs and sensors in order to optimize the transmission cost of the forwarding scheme. A set of multiple routing paths between MSs and sensors is generated to distribute the global traffic over the entire network. Simulations were performed in order to validate the performance of our new approach. We compare the results obtained with those for a single static sink and mobile sink, and show that our approach can achieve better performances such as packet delivery ratio, throughput, end-to-end delay, network lifetime, residual energy, energy and routing diversity overhead.

Keywords: Wireless Sensor Network, Mini-sink Mobility, Multiple Paths, Congestion, Network Performance.

1. INTRODUCTION

The advances in micro-electro-mechanical technologies bring significant advantages to the development of low-cost sensors equipped with storage, computing and communication capabilities. Wireless Sensor Networks (WSNs) are ad hoc wireless networks that consist of a large number of small devices, known as sensors, scattered over a particular geographical area [1]. As an emerging technology, they have gained much attention in a large range of technical fields such as industrial, biological, medical, military, nuclear science, forest fire detection, air pollution monitoring etc. The lack of a predefined communication infrastructure increases the challenge in the design of communication techniques for these networks, especially in hostile environments, where it is often difficult to replace sensor batteries after deployment and where communication infrastructures are not accessible or available.

In WSNs, all sensor nodes send their data towards the central sink, which is the final recipient of the sensed information. It is typically connected to conventional computing equipment for complex processing of the accumulated readings. Each sensor is equipped with a limited amount

of storage capacity and energy, and is able to communicate with its neighbours over wireless connections. Thus, the sensor energy is the main impediment to improve overall network performance. Self-configuration is mandated to give all sensors the possibility of efficiently forwarding data towards the sink for improving network performance [3].

In this paper, we evaluate network performance [2] such as Packet Delivery Ratio (PDR), Throughput, End-to-End-Delay (E_2ED_{elay}), Network Lifetime (NL), Residual Energy (RE), Energy Overhead (EO) and Routing Diversity Overhead (RDO). In a nutshell, the main contributions of this paper are as follows:

• The use of several MSs instead of a single sink, for collecting the data, in order to improve overall network performance.
• Sensors and the main sink are fixed, but MSs are mobile. The MSs move inside the sensor field according to a controlled arbitrary mobility model in order to maintain a fully-connected network topology, collecting data within their coverage areas and forwarding it towards the sink.
• Energy Conserving Routing Protocol (ECRP), based on route diversity, is implemented in MSs and sensors in order to optimize the transmission cost of forwarding [4].
• A set of multiple routing paths between MSs and sensors is generated to distribute the global traffic over the entire network. Thus, network performance can be improved significantly.

Extensive simulations have been performed in order to validate the performance of our approach. We compare the results obtained with those for a single and mobile sink [5] by taking PDR, Throughput, E_2ED_{elay}, NL, RE, EO and RDO as performance criteria. We show that our new approach can achieve better results.

The remainder of this paper is organized as follows: Section 2 outlines related work. Section 3 formulates the problem and presents our Mini-Sink mobility model. Section 4 discusses our proposed approach. Section5 presents performance metrics. Section 6 presents analysis and performance results and Section 7 concludes the paper.

2. RELATED WORK

In the past, many works have been proposed using the mobility of the sink for collecting the data. The sink mobility can be classified into mobile base station, mobile data collector and rendezvous-based taking into account the movement pattern of mobile sinks and the manner the data are collected [6]. We focus on the deployment of many mobile data collectors for decreasing the load in order to improve overall network performance.

In the mobile data collector, many mobile data collectors are used to collect the sensed data from fixed sensors. According to the sink mobility pattern, we can classify into random, predictable and controlled mobility [7]. In random mobility, mobile data collectors move along a random path inside the sensor field and implement a technique for collecting the data from fixed sensors. But random mobility does not guarantee the collection of data from all sensors and need a high delay to deliver the data. In predictable mobility, the mobile data collector moves along a predefined or a fixed path for improving network performance. In this case, all sensors should know the movement of data collectors in order to predict the forwarding time, helping to improve overall network performance. In controlled mobility, the mobility of data collectors is controlled. The approach presented in this paper is based on an arbitrary mobility of MSs for maintaining a fully-connected network, collecting the sensed data from fixed sensors not in arbitrary manner, but controlled based on ECRP.

We describe now some recent works investigating the use of mobile sinks or mobile data collectors for increasing WSN performances.

Vecchio et al. [8] propose density-based proactive techniques that do not impose any restrictions on mobility of the sink. They approach combines a probabilistic flooding and storing scheme for

collecting data. Hamida et al. [9] explore recent data dissemination protocols using mobile sinks and analyze the mobility impact on energy consumption and the network lifetime. Marta et al. [10] propose an approach in which mobile sinks change their location when energy of sensors nearby mobile sinks is depleted. The new location of mobile sinks follows the path with the maximum energy of sensors for improving network lifetime. Yang et al. [11] propose the using of mobile sinks to route data towards the destination via the shortest paths. The residual energy is taking into account in the shortest paths calculation in order to maximize network lifetime and overhead. Li et al. [12] study the theoretical aspects of the uneven energy depletion phenomenon around a sink, and address the problem of energy-efficient data gathering by mobile sinks. Cuomo et al. [13] study the effects of sensor node mobility on network formation according to IEEE 802.15.4/ZigBee. They focus on single-sink and multi-sink configurations to analyze network performance as a function of the number of sinks. Vlajic et al. [14] propose the evaluation of various deployment strategies involving sink mobility in the real world in order to reduce energy consumption and propagation delay while increasing network lifetime. Maria et al. [15] propose a novel linear programming model for network lifetime maximization by determining the movement of the sink rather than minimizing the energy consumption at the nodes. Their proposed model results in a fair balancing of energy depletion among the network nodes. Luo et al. [16] propose a model that uses the mobility of the sink in such a way that the sensor nodes located in the vicinity of the sink change over time. They show that combining the mobility of the sink with routing protocols helps to balance the load and so optimizes network lifetime. Ioannis et al. [5] propose the use of random sink mobility to reduce data latency and increase WSNs lifetime, although random sink mobility is not sufficient to guarantee the collection of data from all sensors.

Our approach presented in this paper is close to [5]. One difference is that, we propose a new approach in which a set of multiple paths using ECRP between the closest MSs and sensors is generated in order to optimize the transmission cost of the forwarding scheme. The forwarding scheme is controlled based on ECRP. Such a method has the advantage of distributing the global traffic over the entire network topology.

To the best of our knowledge, there is no previous study that investigates the use of multiple paths between sensors and MSs for improving WSN performances. In this paper, we use the terms multiple paths and route diversity interchangeably.

3. PROBLEM STATEMENT AND PROPOSITION

In this section, we formulate the problem addressed in this paper and outline our Mini-Sink mobility model.

3.1 Problem Statement

As already presented in our previous work [17], the main cause of decreasing network performance in WSNs is the transmission of data from all sensor nodes towards a single sink. One of the main disadvantages of this communication model is increasing of congestion in the network. Congestion may occur in a WSN for two major reasons: 1) Due to the short wireless communication range of sensors, the sink can only communicate with a limited number of sensors, namely the sensors in the vicinity of the sink. It may happen that some sensors in the vicinity of the sink collect more data because they are aggregating the data from other sensors. Thus, congestion starts to build up on these sensors, and the residual energy in these sensors quickly becomes depleted, so are more prone to shutdown [18]. 2) Since each sensor is equipped with a limited amount of storage capacity and energy supply, at any given moment, some routing sensors fail to transmit or receive the data because the amount of data collected becomes greater than the amount of data that can be forwarded, causing the emergence of local congestion at these routing sensors, so impacting network performance.

3.2 Proposition

To address these problems, we propose that, instead of having a central sink responsible for all data collection, we introduce many data collectors, which we designate Mini Sinks (MSs). These

MSs move in the sensor field according to a controlled arbitrary mobility model in order to maintain a fully-connected network topology, collecting data within their coverage areas and forwarding it towards the sink. Thus, the overall network performance as PDR, Throughput, E_2ED_{elay}, NL, RE, EO and RDO can be improved significantly.

3.3 Network Architecture and Assumptions

Our network architecture consists of three classes of nodes:

- MSs are special nodes equipped with unlimited energy and storage capacity.
- Sensor nodes are responsible for sensing their nearby environment.
- A single sink provides a gateway to conventional computing equipment.

We assume in our new approach that:

- Sensors and MSs are deployed in an area L.
- Sensors are homogeneous and fixed.
- Each sensor maintains a list of the identities (Id) of its neighbours.
- Links between two adjacent sensor nodes are always bidirectional.
- Each sensor takes readings at a fixed rate and forwards them to the most accessible MS.
- MSs are mobile and can return to a recharging point when their energy reserves have been depleted.
- MSs are responsible for collecting the data from sensors and forwarding it towards the sink.
- A single sink is the final recipient of all the sensed data.

3.4 Mini-Sink Mobility Model

In our new approach, the MSs move according to a controlled arbitrary mobility model inside the sensor field as shown in Figure 1.

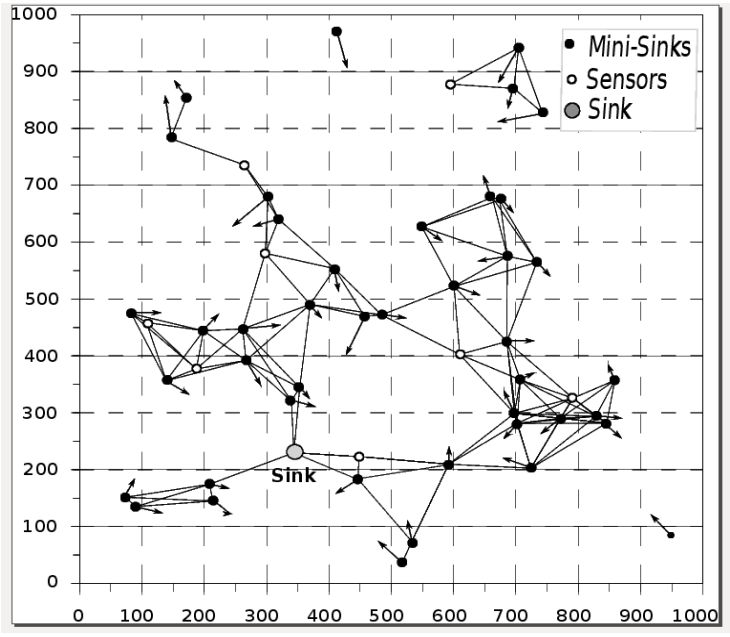


FIGURE 1: Network with mobile mini-sinks.

The geographic network area is a square of side L = 1000m x 1000m.N MSs are randomly placed in this area. Each MS Ni is defined in respect of its coordinates (x, y), and moves from a given position (x_i, y_i)to a new position (xd_i, yd_i) with a velocity [v_{min}, v_{max}], in the range [0...2π].Each MS moves with a different velocity represented in the Figure by differing dashed line styles. When a

MS reaches the locality radius of the sink, it stays there for a time t_i selected in the range $[t_{min}...,t_{max}]$, in order to forward the data that it has collected based on the controlled ECRP towards the sink. After this interval, the MS restarts its displacement process by selecting a new position, and so on.

In the following Section, we outline our Energy Conserving Routing Protocol (ECRP), which has already been presented in [4].

4. ECRP OVERVIEW

The ECRP protocol has been designed to optimize the cost of the forwarding scheme, postpone the onset of congestion and to counteract the high traffic variability in WSNs [19]. The route discovery approach derives directly from the Dijkstra's algorithm. Macgregor et al. [20] present the Meta Dijkstra's algorithm, consisting of iterative applications of Dijkstra's algorithm in a changing topology. Once a path is discovered, its links are deleted from the topology and the performance of the new shortest path in the current graph is evaluated, and so on until a set of maximal paths is found. Unfortunately, such deletion may be too restrictive as it can reject the neighbourhood of the source node from the remaining topology. In other words, it can lead to create a disconnected graph in which the source and destination nodes are not connected together [21, 22, 23].In our new approach, we prefer changing the current topology by adding limited weights to all discovered shortest path edges. We recall that the Meta Dijkstra algorithm corresponds to a particular case of the modified Dijkstra's algorithm where infinite weights are used.

Here briefly is how ECRP works.

Consider a simple topology, as shown in Figure 2. In this topology, we want to extract a set of maximal paths between the transmission nodes S_1 and S_7 randomly chosen. The initial weight of links corresponds to the values seen in the real topology T_0.The modified Dijkstra's algorithm is executed, providing the lowest cost path P_0= $S_1S_6S_7$ between the transmission sensor nodes S_1 and S_7.Thereafter we increase each link weight in P_0; by adding a constant value C, greater than or equal to the locality radius, the probability of having the same lowest cost path P_0 in the calculation of the new lowest path remains low.

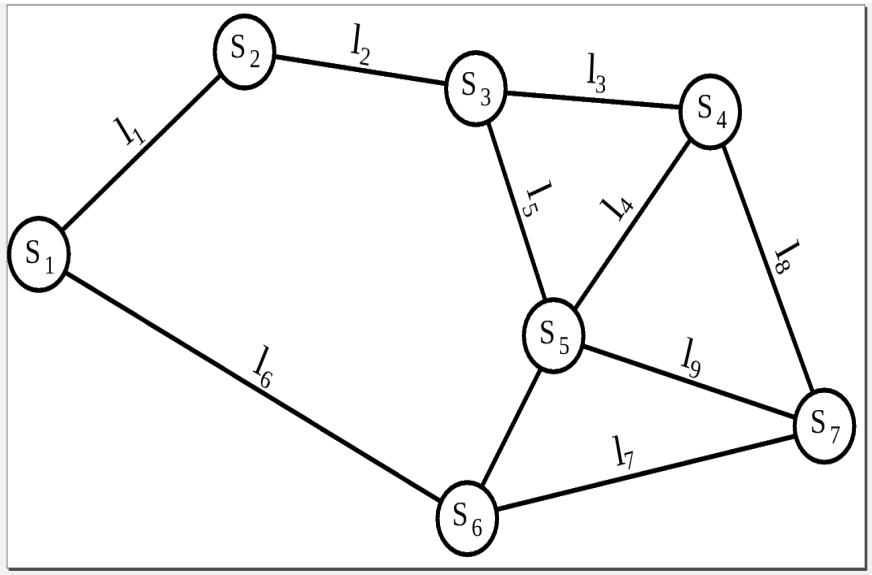


FIGURE 2: Network topology.

Thus, the topology is now described by T_1. We discover the lowest cost path P_1 between the same connection nodes, but now we take the current topology T_1 into account for the calculation. We then increase each link weight in P_1. The topology is now described by T_2. We iterate this process in order to extract a set of maximal routing paths between S_1 and S_7.This iterative process obtains the required maximum number of paths between S_1 and S_7as shown in Table 1.

Paths	Connection links	Hop count
P_1	$S_1S_6S_7$	2
P_2	$S_1S_2S_3S_5S_7$	4
P_3	$S_1S_6S_5S_4S_7$	4
P_4	$S_1S_2S_3S_4S_7$	4

TABLE 1: Paths discovery between sensors S_1 and S_7.

The set of maximal paths extracted is directly applied between sensors and MSs in such a way that, for a transmission between sensors and MSs, the defined traffic is not all carried on a single path, but it is spread over multiple paths. This results in a fair balancing of the energy depletion in order to increase overall network performance. The onset of the global congestion is delayed, as the route diversity modifies the probability of taking a path according to its load. This dynamic path selection implies that the traffic remains more regular for the sensor nodes involved in the routing path. Thus, route diversity appears to be a promising solution for coping with high traffic variability and improving network performance.

We consider in our approach three communication modes while MSs are mobile:

• Multi-MS Mode: each sensor is allowed to connect itself simultaneously to several MSs in order to increase its connectivity capabilities.
The sensor node under consideration stores and updates the lowest cost path towards each accessible MS.
• Multiple routing paths MS mode: each sensor is only interested in the closest MS, although multiple paths are used between a sensor and the closest MSs. These paths are discovered using ECRP.
• MS Point-to-point mode: two MSs want to establish a connection with each other. The lowest cost path is discovered and updated when the network topology changes. In this mode, packets always follow a single path if the topology stays stable. However, the path is updated when the topology change occurs.

4.1 Network Topology

The proposed WSN can be modelled as a connected graph G = (S, E), where S is the set of n stationary sensors, and each E □ SxS is the set of wireless links that communicate between any two sensor nodes. We use the locality model suggested by Zegura et al. [24] into determine network connectivity. The probability of a link between two sensor nodes S_i and S_j is given by:

$$P = \begin{cases} \alpha \ if \ d \leq R \\ \beta \ if \ d > R \end{cases} \quad (1)$$

$$1 = \alpha + \beta \quad (2)$$

Where d is the Euclidean distance between the sensors $S_i$and S_j. R is a model parameter that defines the locality radius. We visualize R as a value that provides a relationship between physical distance and connection probability. α and β are in [0,1]. In this paper, we select α=1 and β=0.Thus, if $d(S_i, S_j) \leq R$, a bidirectional link is possible between them. This model is relevant to the design of WSNs made up of sensors that have a bounded communication range.

The goal of our approach is to study overall network performance resulting from the mobility of MSs. We also aim to measure the effectiveness of multiple routing path propagation on changing topologies.

4.2 Data Forwarding Procedures

As MSs are mobile, the network topology must be computed in real time in order to see its behaviour. Consider the network topology shown in Figure 1. MSs are represented by black disks with a velocity vector that points to their destination. Sensor nodes are represented by white disks. Arrow length is proportional to the velocity. While each MS is moving, it broadcasts a packet to all sensors in its locality radius in order to inform them that it is a MS. The packet contains the hop count, which is initialized to 1, the identity Id of the MS and the type of sensed data. During the sensing activity of sensors, it may happen that some sensors are connected to many MSs due to their mobility. In order to know which MS is most suitable and presents the lowest cost for transferring the data, each sensor in direct communication with MSs calculates the lowest cost path using ECRP before sending the data to the best MS. During mobility, when each MS arrives at the locality radius of the sink, it stays at the same position for a time t_i, which is as long as is necessary to transfer the data to the sink. During this time, the MS also plays the role of a relay point for its neighboring MSs. The time needed for each MS depends on the amount of data to be transferred to the sink.

5. PERFORMANCE METRICS

The following metrics are used to evaluate our approach:

5.1 Packet Delivery Ratio (PDR)

PDR is the ratio of packets that are received by the sink to the total packets generated by sensors.

$$PDR = \frac{P_{Received} * 100}{\sum_{i=1}^{n} P_{Generated_i}} \qquad (3)$$

PReceived is the total number of data packets received by the sink, PGenerated the total number of data packets generated by sensors and n the number of sensors.

5.2 Throughput

Throughput is the total number of data packets received by the sink in a period of time.

$$Throughput = \frac{\sum_{i=1}^{n} P_{Received_i} * P_{Length}}{SIMU_{Time}} \qquad (4)$$

P*Length* the length of a packet, SIMUTime the simulation time.With higher PDR and throughput being more desirable.

5.3 E_2ED_{elay}

$E_2ED_{elay}$is the average sum of the difference delay of each data packet is received by the sink and the time a data packet is sent by sensors to MSs.

$$E_2E_{Delay} = \frac{\sum_{i=1}^{P_{Received}} (T_{Received_i} - T_{Ransmission_i})}{P_{Received}} \qquad (5)$$

TReceived is the reception time by the sink, TTransmission the transmission time by each sensor.Smallest is this value indicates the promptness of data delivered to the sink.

5.4 Routing Diversity Overhead (RDO)

We have seen in subsection 4.2 that, while each MS is moving, it broadcasts a beacon message to all sensors in its locality radius in order to inform them that it is a MS. We consider in our experiments that the beacon message exchanged to find the routing paths is a data packet.
We evaluate RDO per sensor due to discover, establish, update and maintain multiple routing paths between sensors and MSs. RDO is the percentage of the total number of packets

exchanged (to calculate, update and maintain multiple paths by each sensor) to the total number of packets that are received by the sink.

$$RDO = \frac{\sum_{i=1}^{n} PExchanged * 100}{PReceived} \quad (6)$$

PExchanged is the total number of packets exchanged by sensors.

5.5 Energy Model

In WSNs, sensors use batteries as their source of energy. In a very large sensor network, sensors are often deployed in a hostile environment where replacing the batteries is not possible. Since sensors are battery-driven, a good choice of energy model is essential to optimize sensor lifetime. It is well-known that data transmission consumes more energy than other activities in WSNs [25]. Our approach considers that sensors are in the active mode and can turn on sleeping mode. In this paper, the energy model used is the same as in [26]. For each pair of sensors (S_i, S_j), the energy consumed when sending a data packet of m bits over one-hop wireless link d can be obtained as:

Sensor sender energy consumption:

$$ETi(m,d) = Eelec * m + Eamp * m * d^2 \quad (7)$$

Sensor receiver energy consumption:

$$ERi(m,d) = Eelec * m \quad (8)$$

The total energy consumed by each pair (S_i, S_j) is:

$$ET(m,d) = ETi(m,d) + ERi(m,d) \quad (9)$$

When a packet is sent along a path P_i ($_i$=1....,q), we must perform an energy decrease operation on each sensor along the path except for the destination sensor. Thus, after a data packet is sent by a sensor, the energy level of that sensor is decremented by the amount of energyrequired to send the data packet. Thus, the RE of a sensor is a fraction of its initial energy value.

RE is the difference between the initial energy and the energy consumed by a sensor:

$$RE = E - ET(m,d) \quad (10)$$

EO is the ratio of the total energy exchanged (to discover, establish, update and maintain multiple routing paths)to the total energy consumed to transfer the data by each sensor to MSs.

$$EO = \frac{\sum_{i=1}^{n} E_{Exchanged_i} * 100}{E_T(m,d)} \quad (11)$$

ET_i is the energy consumed for a packet's transmission by the source S_i, ER_j the energy consumed for a packet's reception S_j (1-hop neighbors), Eelec the energy consumed to run the transmitter and receiver circuitry, Eamp the energy of the amplifier, EExchanged to calculate, maintain multiple paths, d the Euclidean distance between (S_i, S_j).

5.6 Network Lifetime (NL)

NL, as the total number of packets that can be transferred in the network before the link between sensors and MSs is disconnected due to the energy depletion. We have seen in that, when a

packet is sent along a path P_i ($_i$=1....,q), we must perform an energy decrease operation on each sensor along the path except for the destination sensor. Let T_1 is the real topology of the graph G. After executing ECRP in T_1providing the lowest cost path P_1. After the decreasing operation along the path P_1, we obtain a new topology T_2, in which RE of sensors and link weights are different. If after the decrease operation, RE of a sensor becomes 0, the sensor under consideration and its corresponding links are removed from the new topology. We iterate the procedure of extracting the paths until we obtain the required number of routing paths to transmit the maximum number of data packets to MS. Suppose that P(S_i, MS) is the path between a given sensor S_i and a destination MS, and m bits to be transferred. NL is obtains by maximizing the RE of the path P(S_i, MS).

$$NL = Max \sum_{i=1}^{q} RE\left(P(Si, MS)\right) \qquad (12)$$

6. ANALYSIS AND PERFORMANCE

6.1 Analysis

We implemented our network topology using Qualnet. A topology is totally described by the number of stationary sensor nodes n belonging to the network, their locations, and the link characteristics (l direct edges between sensor nodes).A link is defined by a starting node (head), a finishing node (tail) and a weight (w) needed in the path discovery between sensor nodes. The parameters of analysis are described in Table 2.

Parameters	Description	Value
E	Full Energy of sensor	10000 J
Eelec	Energy to run transceiver/receiver	50 nJ/bit
Eamp	Energy of amplifier	100 pJ/bit
L	Simulation area (m)	1000 x 1000
Packet	Packet length	2 Kbits
Traffic rate	UDP traffic	6 packets/sec
Slength	Session length	[1…60]
B	Bandwidth	250 kbps
R	Locality radius	50m
Movement	Random Way Point	
Routing	Routing protocol	ECRP
V_{max}	Maximum velocity	10mps
SIMUTime	Simulation time	1000s
t_i	Time needed	[0…3]s
n	Number of sensors	[25…100]
N	Number of Mini-Sinks	30

TABLE 2: Simulation parameters.

In all our analysis, we deploy 100 fixed sensor nodes inside a square area L that defines network coordinate bounds. The sink is placed at the corner of the square area L. Each sensor is able to transmit to its lowest cost MS a certain number of packets before its energy is depleted. We analyzed for 30 MSs, since we have showed in our previous work [17] that, using 30 MSs can achieve a fully-connected network. MSs move with a velocity in the range [0…10mps].During the execution of our simulations, a given source and destination pair remains in the evaluated set until communication between them fails due to energy depletion. We repeated 100 times the experiments for the same topology, and then we took the average value of these 100 runs. Initially, each sensor is charged with energy of 10000 Joules. A sensor node was considered non-functional if its energy reached the value 0.

6.2 Performance Results

For the defined network topology, ECRP is applied between a selected sensor and the closest MS. As a consequence, packets can be transmitted over multiple routing paths until the network topology changes to a new configuration. We recall that in the case of a single sink and the mobile sink [5], a single packet is transmitted between each pair (S_i, S_j). In our approach, as multiple routing paths are used between sensors and MSs, we assume that many packets are transmitted between each pair (S_i, S_j).

We used simulations to investigate:

- The PDR and Throughput due to the use of MSs.
- The E_2ED_{elay} due to the mobility of MSs.
- The effect of session length (k) on overall NL and RE.
- The effect of locality radius (R) on overall NL and RE.
- The effect of network density on overall NL and RE.
- The EO and RDO due to calculate and maintain multiple routing paths.

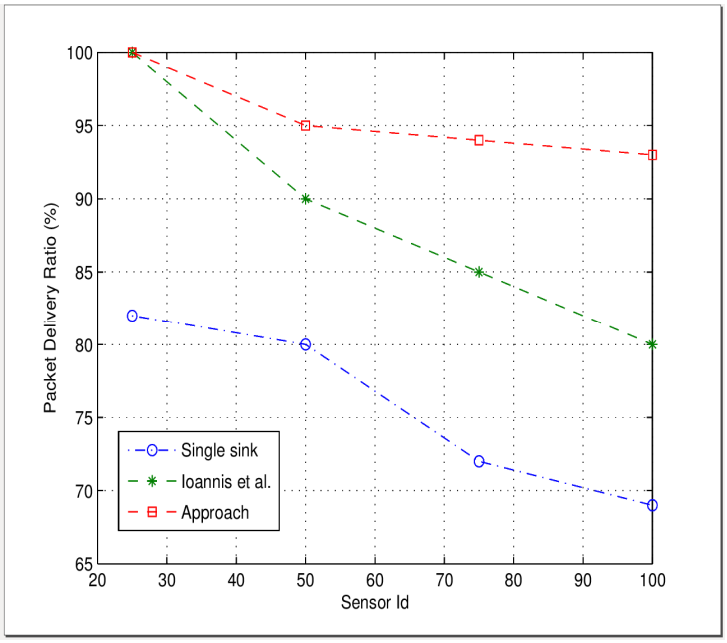


FIGURE 3: PDR vs. Number of sensors.

Figure 3 shows the results of PDR as a function of the sensor Ids. We observe from Figure 3 that, we have the same PDR as Ioannis et al. [5] with 25 sensors. When the number of sensors varies between [25...100], the single static single presents a small percentage of PDR. Hence, Ioannis et al. achieve a higher PDR than the case of a single static sink. In all cases, our Mini-Sink approach achieves the better PDR with an average of 95.5%, compared to 88.55% for Ioannis et al. and 75.75% for the single static sink.

Figure 4 shows the results of throughput as a function of the velocity. We recall that the throughput depends on the velocity of MSs. It can be observed from Figure 4 that, the throughput decreases with increase velocity. We can see that the maximum throughput is achieved with the velocity of 2.5mps. When the velocity varies between [2.5 - 10]mps, our approach outperforms Ioannis et al. and the single sink with an average of 11.24% and 35.94% respectively. We can conclude that, increasing the velocity of MSs degrades the throughput since some sensors may not able to transfer the data to MSs on time.

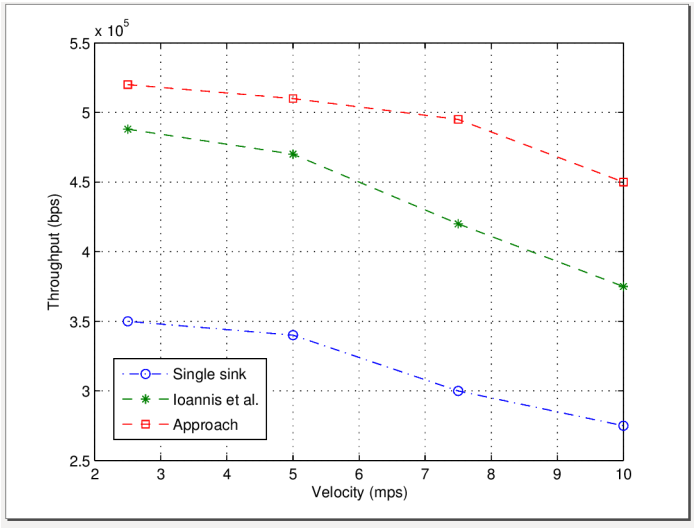


FIGURE 4: Throughput vs. Velocity.

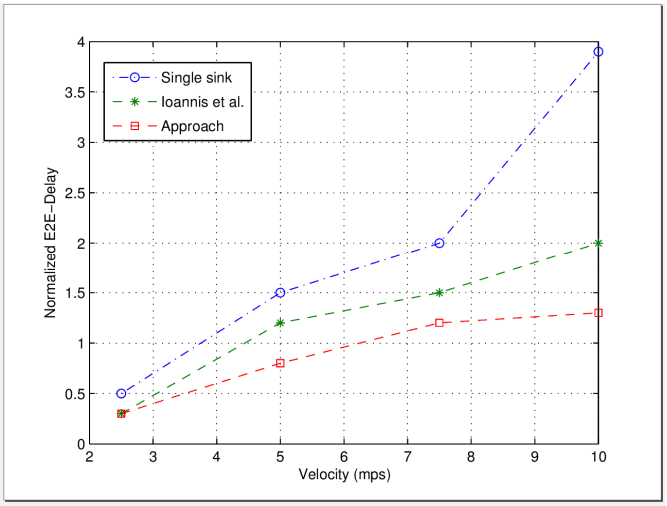


FIGURE 5: E_2ED_{elay} vs. Velocity.

Figure 5 shows the normalized E_2ED_{elay} as a function of the velocity of MSs. We can see that the single static sink presents the large E_2ED_{elay}.That is due to the fact that whenever a sensor wants to send the data, a sensor performs a route discovery process which takes more time. Every sensor extracts and records information before forwarding towards the sink via intermediate sensors instead of MSs as in our approach. Ioannis et al. present the lowest E_2ED_{elay}compared to the single static sink. Figure 5 shows that with the increasing velocity of MSs, our approach achieves the smallest E_2ED_{elay} than Ioannis et al. and the single static sink.

We evaluate now the overall NL. In the single and mobile sink [5], a single packet is transmitted in Session length (Slength) between each pair (S_i, S_j). We assume that k packets are transmitted in each Slength between each pair (S_i, S_j).We then vary the value of k in order to observe the behaviour of our approach and the techniques implemented.

Figure 6 shows the results of NL as a function of Slength. We send k packets at a time for each Slength. We observe from Figure 6 that, when we vary Slength between [1...60], Ioannis et al. achieve better NL than the case of a single static sink. In all cases, our Mini-Sink approach outperforms Ioannis et al. by around 16% and the single static sink by around 40%.

Figure 7 shows the impact of the locality radius on NL. We can see that when the locality radius is less or equal to 35m,the single static sink improves NL than Ioannis et al. and our approach by around 14% and 5% respectively. While, when the locality radius varies between [40...100]m, our approach significantly outperforms Ioannis et al. and the single static sink by around 5% and 20% respectively.

Figure 8 shows the results of the RE vs. Slength. We see that in all the three algorithms, RE increases with increasing Slength. In the case of a single static sink, the forwarding scheme uses multi-hop along the shortest path towards the sink. We observe that Ioannis et al. improve RE than the single static sink by around 20%. Our approach still outperforms Ioannis et al. in terms of RE by around 15% and the single static sink by around 31%.

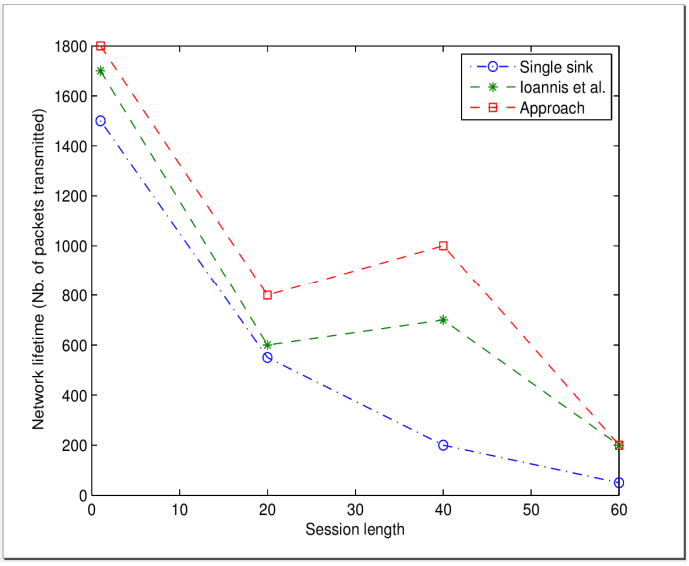


FIGURE 6: Network lifetime vs. Session length.

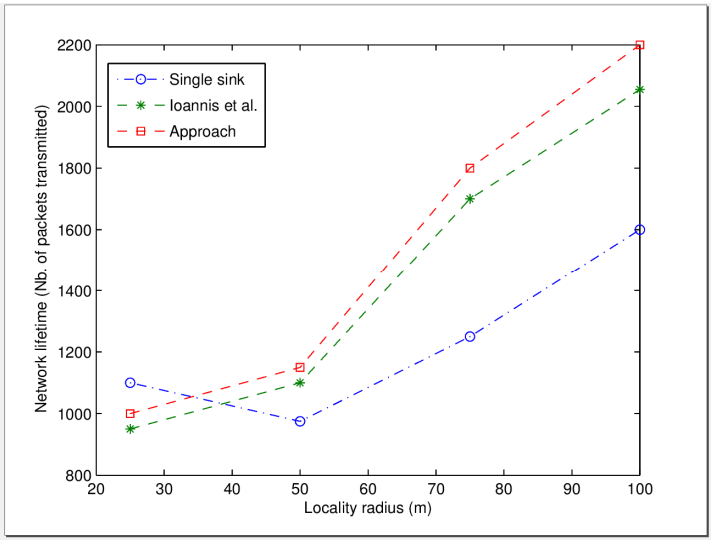


FIGURE 7: Network lifetime vs. Locality radius.

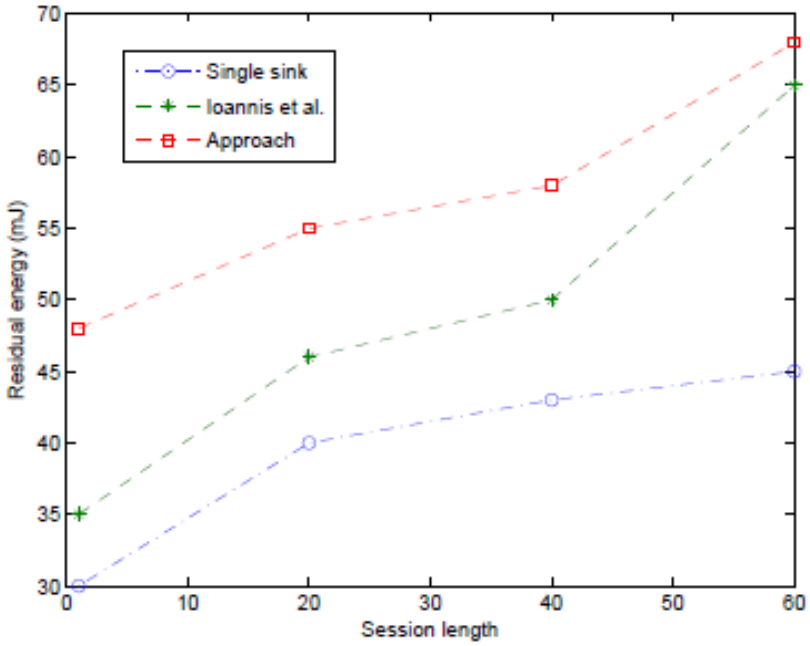


FIGURE 8: Residual energy vs. Session length.

Figure 9 depicts the impact of the locality radius on RE. We see that, as the locality radius varies between [25...100]m, the RE of all the three techniques decreases considerably. That means the locality radius has a strong impact on the RE. In all the cases, our approach outperforms Ioannis et al. and the single static sink by around 36% and 50% respectively.

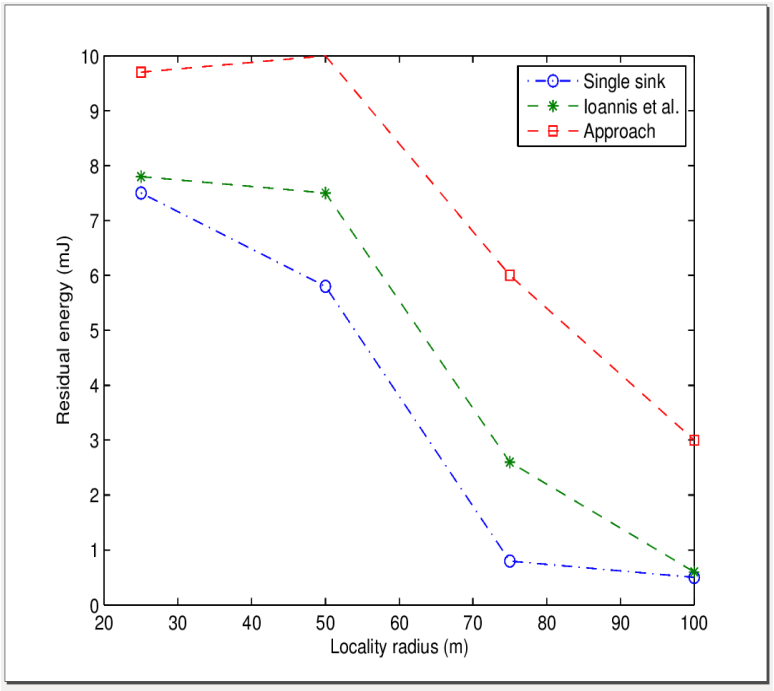


FIGURE 9: Residual energy vs. Locality radius.

In order to understand the behaviour of our approach, we evaluate our algorithm between [100...300] sensors. Figure 10 and Figure 11 depict the average NL and RE as a function of network density. We observe that, when we increase the number of sensors by keeping the locality radius constant, the results obtained by Ioannis et al. are very close to our approach in terms of NL as shown in Figure 10.Ioannis et al. perform better than the case of a single static sink. In terms of the maximal RE as shown in Figure 11, our approach still outperforms Ioannis et al. and the single static sink by around 45% and 63% respectively.

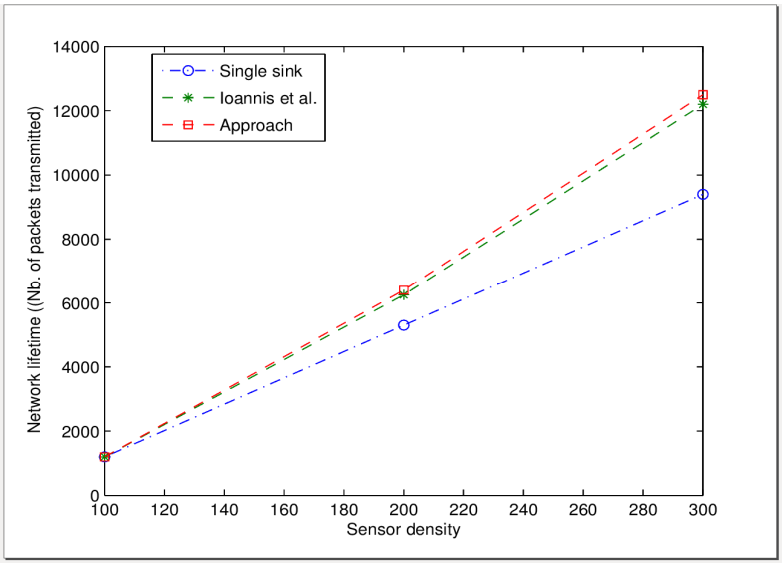


FIGURE 10: Network lifetime vs. Network density.

Figure 12 and Figure 13 show the evolution of EO and RDO as a function of sensor Ids. We can see from Figure 12 that, our approach performs better Ioannis et al. and the single sink in terms of the maximum EO by each sensor with around 11%, 20% and 35% respectively. For the average EO, our approach presents an average EO with around 7.75%, Ioannis et al. around 12.25% and the single sink around 21.75%.Statistically, our approach outperforms Ioannis et al.

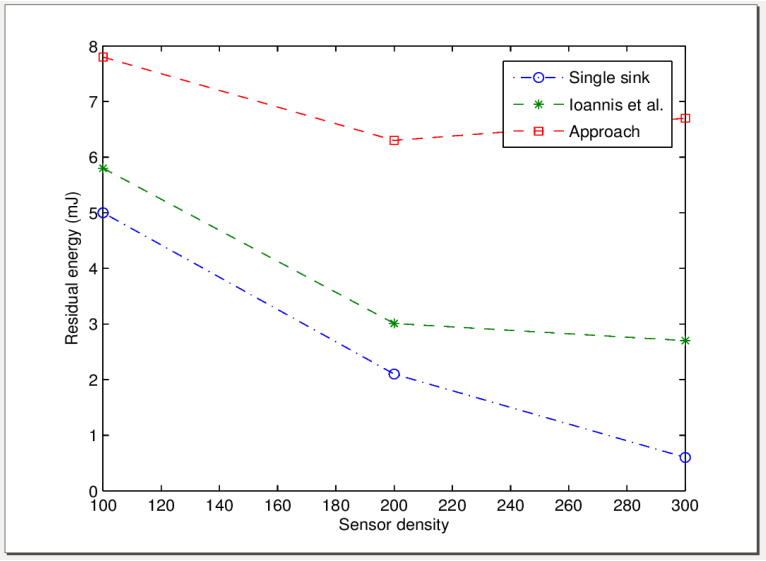


FIGURE 11: Residual energy vs. Network density.

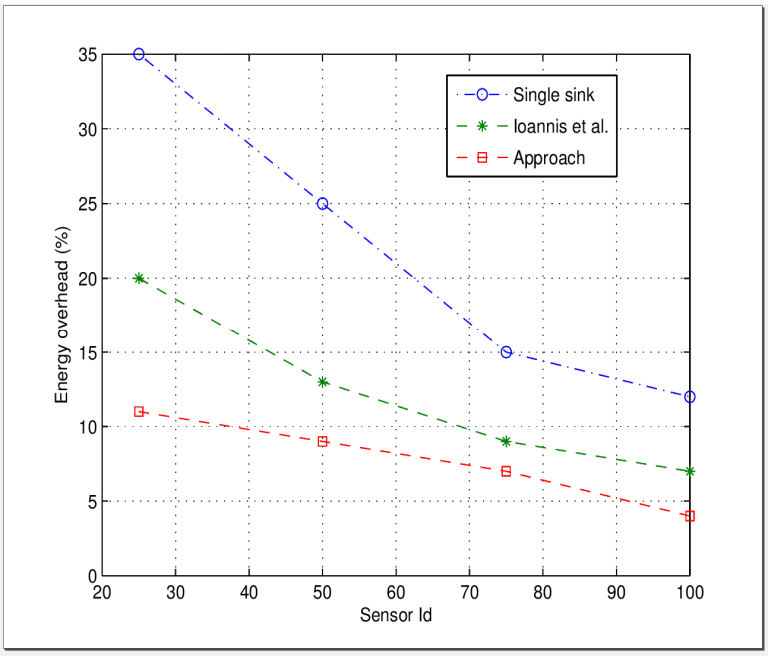


FIGURE 12: Energy overhead vs. Sensor Id.

and the single sink with around 58% and 180% respectively. In Figure 13, we observe that our approach and Ioannis et al. used the lowest beacon packets to find the routing paths compared to the single static sink. That is due to the fact that the single static sink uses the simple flooding in the route discovery process, and needs a higher number of beacon messages if the battery fails. Our approach improves RDO than Ioannis et al. and the single sink with an average of around 14.75% and 78.51% respectively. This happens because our approach needs less beacon messages to discover and maintain multiple routing paths to MSs.

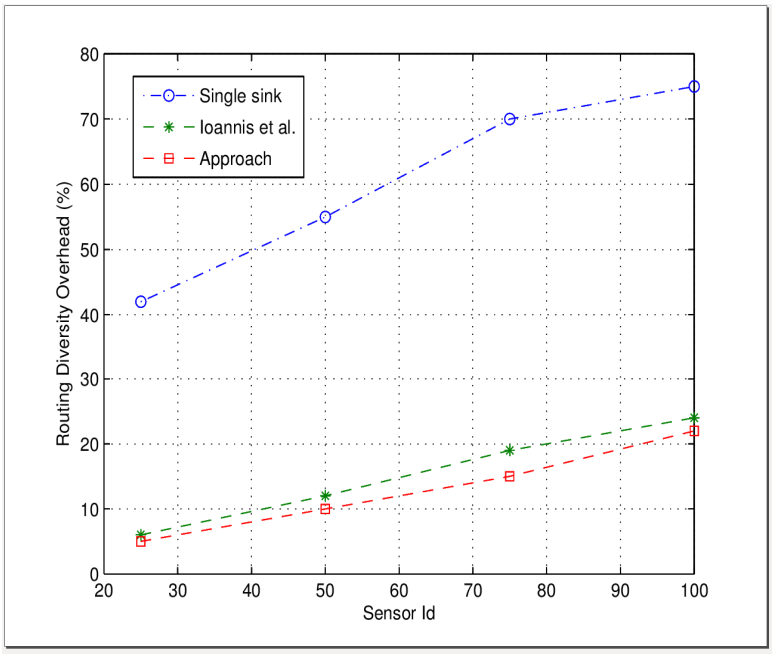


FIGURE 13: RDO vs. Sensor Id.

7. CONCLUSION

In this paper, we propose the use of many MSs, instead of a single sink for collecting data in order to improve WSN performance. One or more MSs are mobile and move according to a controlled arbitrary mobility model inside the sensor field in order to collect data within their coverage areas and forward it towards the sink. ECRP, based on route diversity, is implemented in MSs and sensors in order to optimize the transmission cost of the forwarding scheme. A set of multiple routing paths between MSs and sensors is generated to distribute the global traffic over the entire network. We compare the results obtained with those for a single and mobile sink, and show that our solution can achieve better network performances as PDR, Throughput, E_2ED_{elay}, NL, RE, EO and RDO.

In future works, we will define aggregation mechanisms on sensors and evaluate the impact of interference between sensors and MSs.

8. REFERENCES

[1] P. Wang, R. Dai and I. Akyildiz. "Collaborative Data Compression Using Clustered Source Coding for Wireless Multimedia Sensor Networks," in Proc. the 29th IEEE INFOCOM, 2010, pp. 2106-2114.

[2] D. Kandris, M. Tsagkaropoulos, I. Politis, A. Tzes and S. Kotsopoulos. "Energy efficient and perceived QoS aware video routing over Wireless Multimedia Sensor Networks." Ad Hoc networks Journal, vol. 9, no. 4, pp. 591-607, 2011.

[3] J.H. Chang and L. Tassiulas. "Maximum lifetime routing in wireless sensor networks." IEEE/ACM Transactions on Networking, vol. 12, pp. 609-619, 2004.

[4] D. Fotue, F. Melakessou, H. Labiod and T. Engel. "Design of an Enhanced Energy Conserving Routing Protocol based on Route Diversity in Wireless Sensor Networks." In Proc. of the 9th IEEE/IFIP Annual Mediterranean Ad Hoc Networking Workshop, 2010, pp. 1-7.

[5] I. Chatzigiannakis, A. Kinalis and S. Nikoletseas. "Sink mobility protocols for data collection in wireless sensor networks." In Proc. of the Forth ACM International Workshop on Mobility Management and Wireless Access (MOBIWAC), 2006, pp.52-59.

[6] Q. Dong and W. Dargie. "A Survey on Mobility and Mobility-Aware MAC Protocols in Wireless Sensor Networks." IEEE Communications Surveys and Tutorials, pp. 1-13, 2011.

[7] M.S.G. Premi and K.S. Shaji. "Impact of Mobility Models on MMS Routing in Wireless Sensor Networks." International Journal of Computer Applications (IJCA), vol. 22, No 9, pp. 47-51, 2011.

[8] M. Vecchio, A.C. Viana, A. Ziviani and R. Friedman. "DEEP: Density-based proactive data dissemination protocol for wireless sensor networks with uncontrolled sink mobility." Computer Communications journal (ComCom), vol. 33, Issue 8, pp. 929-939, 2010.

[9] E.B. Hamida and G. Chelius. "Strategies for data dissemination to mobile sinks in wireless sensor networks." IEEE Wireless Communications Magazine, vol. 15, Issue 6, pp. 31-37, 2008.

[10] M. Marta and M. Cardei. "Improved sensor network lifetime with multiple mobile sinks." Pervasive and Mobile Computing Journal, vol. 5, Issue 5, pp. 542-555, 2009.

[11] H. Yang, F. Ye and B. Sikdar. “SIMPLE: Using Swarm Intelligence Methodology to Design Data Acquisition Protocol in Sensor Networks with Mobile Sinks.” in Proc. of INFOCOM, 2006.

[12] X. Li, A. Nayak and I. Stojmenovic. “Exploiting Actuator Mobility for Energy-Efficient Data Collection in Delay-Tolerant Wireless Sensor Networks.” in Proc. of the IEEE Fifth International Conference on Networking and Services (ICNS), 2009.

[13] F. Cuomo, E. Cipollone and A. Abbagnale. “Performance analysis of IEEE 802.15.4 wireless sensor networks: An insight into the topology formation process.” Computer Networks Journal (Elsevier), vol. 53, Issue 18, pp. 3057-3075, December 2009.

[14] N. Vlajic and D. Stevanovic. “Sink mobility in wireless sensor networks: When theory meets reality.” in Proc. of the IEEE Sarnoff Symposium (SARNOFF), 2009, pp. 1-8.

[15] Z.M. Wang, S. Basagni, E. Melachrinoudis and C. Petrioli. “Exploiting Sink Mobility for Maximizing Sensor Networks Lifetime.” in Proc. of the 38thAnnual Hawaii International Conference on System Sciences (HICSS),2005.

[16] J. Luo and J.P. Hubaux. “Joint mobility and routing for lifetime elongation in wireless sensor networks.” in Proc. of the 24thINFOCOM, 2005, pp. 1735-1746.

[17] D. Fotue, F. Melakessou, H. Labiod and T. Engel. “Mini-Sink Mobility on Route Diversity-Based Congestion Reduction and Low Latency in Wireless Sensor Networks.” in Proc. of the 8thACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks (PE-WASUN), 2011, pp. 1-7.

[18] W. Alsalih, S. Akl and H. Hassanein. “Placement of multiple mobile base stations in wireless sensor networks.” in Proc. of the IEEE International Symposium on Signal Processing and Information Technology, 2007, pp. 229-233.

[19] K. P. Sushil and A. Dhawan. “Distributed Algorithms for Lifetime of Wireless Sensor NetworksBased on Dependencies Among Cover Sets.” in Proc. of the 14thInternational Conference on High Performance Computing (HiPC), 2007, pp. 381-392.

[20] M. MacGregor and W. Grover. “Optimized k-Shortest-Paths Algorithm for Facility Restoration.”Software Practice and Experience journal,vol. 24, no. 9, pp. 823-834, 1994.

[21] M. Tariquea, K. Tepeb, S. Adibic and S. Erfanib. “Survey of multipath routing protocols for mobile ad hoc networks.” Journal of Network and Computer Applications, vol. 32, pp. 1125-1143, 2009.

[22] S. Li, X. Ma, X. Wang and M. Tan.“Energy-efficient multipath routing in wireless sensor networks considering wireless interference.” Journal of Control Theory and Applications, vol. 9, pp. 127-132, 2011.

[23] B. Yahya and J. Ben-Othman. “REER: Robust and energy efficient multipath routing protocol for wireless sensor networks.” in Proc. of the IEEE Global Telecommunications Conference (GLOBECOM), 2009, pp. 1-7.

[24] E. Zegura, K. Calvert, and M. Donahoo. “A Quantitative Comparison of Graph-based Models for Internet Topology.” IEEE Transactions on Networking, 1997.

[25] W. Ye, J. Heidemann and D. Estrin. “An energy efficient MAC protocol for wireless sensor networks.” in Proc. of the IEEE INFOCOM, 2005.
March, 2005.

[26] Z. Cheng, M. Perillo and W. Heinzelman. “General network lifetime and cost models for evaluating sensor network deployment strategies.” IEEE Transactions on Mobile Computing, vol. 7, pp. 484-497, 2008.

Image Steganography Techniques: An Overview

Nagham Hamid
University Malaysia Perils (UniMAP) *nagham_fawa@yahoo.com*
School of Communication and Computer Engineering
Penang, Malaysia

Abid Yahya
University Malaysia Perlis (UniMAP)
School of Communication and Computer Engineering
Perlis, Malaysia

R. Badlishah Ahmad
University Malaysia Perlis (UniMAP)
School of Communication and Computer Engineering
Perlis, Malaysia

Osamah M. Al-Qershi
School of Electrical & Electronic Engineering
University of Science Malaysia (USM)
Penang, Malaysia

Abstract

Steganography is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. In this way, if successfully it is achieved, the message does not attract attention from eavesdroppers and attackers. Using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files. The focus in this paper is on the use of an image file as a carrier, and hence, the taxonomy of current steganographic techniques for image files has been presented. These techniques are analyzed and discussed not only in terms of their ability to hide information in image files but also according to how much information can be hidden, and the robustness to different image processing attacks.

Keywords: Adaptive Steganography, Current Techniques, Image Files, Overview, Steganography, Taxonomy.

1. INTRODUCTION

In this modern era, computers and the internet are major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security, particularly when it is combined with encryption [1].

Steganography differs from cryptography. The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is.. In some cases, sending encrypted information may draw attention, while invisible information will not. Accordingly, cryptography is not the best solution for secure communication; it is only part of the solution. Both sciences can

be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well [2].

Watermarking and fingerprinting, among technologies related to steganography, are basically used for intellectual property protection [3]. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. Though this method keeps the data accessible, but it is permanently marked [4]. The hidden information in a watermarked object is a signature referring to the origin or true ownership of the data in order to ensure copyright protection. In the case of fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [5]. Consider Fig. 1, which illustrates the types of steganography.

The performance of a steganographic system can be measured using several properties. The most important property is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associated measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects [6], and robustness, which refers to how well the steganographic system resists the extraction of hidden data.

Nearly all digital file formats, with a high degree of redundancy, are known for their being used for steganography, the redundant parts refer to those parts capable of change without any possibility to detect the alteration. Image and audio files satisfy this requirement particularly well [3]. In fact, digital images are the most used carrier file formats owing to their popularity on the internet. There are a number of steganographic techniques that enable one to hide a secret message in an image file, all of which have corresponding strong and weak points. Different steganographic techniques are used for different applications. Modern steganography categorizes two main classificatory schemes for the taxonomy of algorithms. The first distinguished algorithm is based on file type. The second is a more widely used scheme, where its categorization is based on an embedding technique, which is the main focus of this paper.

This paper is organized as follows. Section 2 presents a brief description of image files and some related concepts. Section 3 describes the most common examples of older steganographic techniques. Section 4 gives an overview of steganographic techniques applicable to specific image formats, including a taxonomy that classifies the techniques depending on the approach used to hide information. Section 5 describes a performance measure for the distortion caused by embedding data in an image. The steganography techniques are compared and evaluated in Section 6. Finally, Section 7 highlights and discusses the arrived at conclusions.

2. IMAGE STEGANOGRAPHY

As stated previously, images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS).

2.1 Image Files

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image [7]. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel [3]. Moreover, the smallest bit depth in the color

scheme is 8, i.e., 8 bits are utilized to represent the color of each pixel. Both Monochrome and gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that digital color images are known for being saved in 24-bit files and for utilizing the RGB color model. Almost all the color variations for the pixels of a 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8 bits [7]. Thus, in any given pixel, the number of different shades of red, green, and blue can reach 256 that adding up to more than 16 million combinations that finally result in more than 16 million colors. The most prominent image formats, exclusively on the internet, are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, and to a lesser degree, the portable network graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure [8, 9].

2.2 General Concepts

- Lossless compression is known for being preferable when the original data should stay in its entirety. In this manner, the original image information will never be removed, and this makes it possible the reconstruction of the original data from the compressed data. This is typical of images in GIF and BMP [7].

- Lossy compression saves storage space by discarding the points the human eyes find difficult to identify. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. JPEG compression uses this technique. A cover image is the image designated to carry the embedded bits or secret information [8].

- A stego image refers to the image carrying the hidden message.

- A stegokey is secret information necessary to get the hidden message from the stego image [9].

3. STEGANOGRAPHY HISTORY

Throughout history, people have hidden information in different ways. The word 'steganography' was basically derived from the Greek words with the meaning “covered writing”. Soon after, researchers used it for thousands of years in various manners [10]. During the 5th century BCE, the Greek tyrant Histiaeus was taken as a prisoner by King Darius in Susa. Histiaeus needed to send an abstruse message to his son-in-law, Aristagoras, who was in Miletus and in order to do this, Histiaeus shaved a slave’s head and tattooed the message on his scalp. As soon as the slave’s hair grew sufficiently to conceal the tattoo, he was sent to Miletus with the message [11].In ancient Greece, another method was to peal the wax off a wax-covered tablet, then write a message and to have the application of the wax again. The one in charge to receive the message would simply need to get rid of the wax from the tablet to see the message. Invisible ink was another popular form of steganography. Ancient Romans had their way in writing between the lines by using invisible ink, and by using substances such as fruit juice, urine, and milk. Using Invisible ink, though seems harmless, a letter might reflect a very different message written between the lines. Invisible ink was used as recently as World War II [12].

In addition to invisible ink, the Germans used the Microdot technique during the Second World War. Information, particularly photographs, was made so small that they were very difficult to detect [13].

In 1550, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user of such papers all what he needs is to write his secret message in such holes after placing the mask over a blank sheet of paper. The next step is to

remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text [14].

This technique, steganography, is now highly used in computers files with digital data as the carrier and networks are considered as high-speed dispatch channels. The sections that follow illustrate the taxonomy of steganographic techniques for image files, including an overview of the most important steganographic techniques for digital images.

4. TAXONOMY OF STEGANOGRAPHIC TECHNIQUES

There are quite a lot of approaches in classifying steganographic techniques. These approaches can be classified in accordance with the type of covers used with secret communications. Another possibility is done via sorting such approaches depending on the type of cover modification already applied in the process of embedding. The second approach is adopted in this work, although in some cases an exact classification is not possible. In general, the process of embedding can be defined as follows:

Let C denote the cover carrier, and $\tilde{C}$ the stego-image. Let K represent an optional key (as a seed used to encrypt the message or to generate a pseudo-random noise, which can be set to $\{\phi\}$ for simplicity), and let M be the message to be sent. Then, Em represents an embedded message and Ex represents the extracted message. Therefore,

$$Em : C \oplus K \oplus M \rightarrow \tilde{C} \quad (1)$$

$$\therefore Ex(Em(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M \quad (2)$$

To distinguish between different steganographic techniques in a wide sense, one must take into consideration both the methods that modify the image and those that modify the image file format. However, the modifications to the file format are less robust [15]. The important issue to mention here is the main role compression usually plays when it comes to deciding which steganographic algorithm is better. Though lossy compression methods result in smaller image file sizes, they increase the possibility of the partial loss of an embedded message because surplus image data is to be eliminated in these techniques. Lossless compression does not compress the image file as much [16]. As a result, researchers have come up with different steganographic algorithms that suit such compression types. Steganographic techniques that modify image files for hiding information include the following:

- Spatial domain;
- Transform domain;
- Spread spectrum;
- Statistical methods; and
- Distortion techniques.

Steganographic techniques that modify the image file format involve file embedding and palette embedding. In addition, there are techniques that modify the elements in the visual image including:

The image generation technique; and the image element modification technique.

Finally, there is a special type of the spatial and transform domain techniques called the adaptive steganography technique, which we also describe for completeness. The next section explains each steganographic approach in more detail.

4.1 Spatial Domain Technique

Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which

changes are likely to be a bit scant when compared to the human visual system (HVS).One of the ways to do so is to hide information in the least significant bit (LSB) of the image data [15].
This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image [17].
The embedding operation of LSB steganography is described by the following equation:

$$Yi = 2\left|\frac{x_i}{2}\right| + m_i \quad (3)$$

where m_i, x_i, and y_i are the i-th message bit, and the i-th selected pixel value before and after embedding, respectively. Steghide, S-tools, Steganos, and other tools using LSB-based steganographic are available in [18].

Let $\{P_x(x=0), P_x(x=1)\}$ denote the distribution of the least significant bits of the cover image, and $\{P_m(m=0), P_m(m=1)\}$ denote the distribution of the secret binary message bits.

The message is to be compressed or encrypted before being embedded just to protect its secrecy. According to this, the distribution of the message may be assumed to equal an averaged distribution, such that $\{P_m(m=0) \approx P_m(m=1) \approx 1/2\}$.

In addition, the cover image and the message may also be assumed to be independent. Therefore, the noise introduced into the image may be modeled as:

$$P_{+1} = \frac{P}{2}P_x(x=0),\ P_0 = 1-\frac{P}{2},\ P_{-1} = \frac{P}{2}P_x(x=1) \quad (4)$$

Where P is the embedding rate, measured in bits per pixel (bpp). The embedding process described above, makes it clear to what extent it is possible to extract the secret message bits directly from the LSBs of these pixels already selected during this process [19].

When hiding the message bits in the image using LSB algorithms, there are two schemes, namely sequential and scattered. The LSBs of the image, in the sequential embedding scheme are replaced by the message bits, whereas in the case of the scattered embedding scheme, the message bits are randomly scattered throughout the image using a random sequence to control the embedding sequence [20].

The well-known steganographic tools based on LSB embedding are different as far as the way they hide information is concerned. Some of them change the LSB of pixels randomly, others modify pixels not in the whole image but in selected areas of it, and still others increase or decrease the pixel value of the LSB, rather than change the value [8].

Katzenbeisser and Petitcolas [21] describe several variations on the basic LSB techniques. They also describe a substitution technique for embedding a secret message into the LSB bits of the palette of GIF or BMP image format using steganography.

Bailey and Curran provide an evaluation of various techniques concerning spatial steganographic and such techniques can principally apply to GIF images [22]. From the above, we conclude that the resulting changes to the cover image using LSB techniques are very difficult to be recognized by the human eye due their being too small. Moreover, such techniques are simple and popular. The disadvantage of this technique is that it uses each pixel in the image. As a result, if lossy compression is used, some of the hidden information might be lost [23].

4.2 Transform Domain Techniques

Transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. It is worth saying that most of the strong steganographic systems today operate within the transform domain [21].

Transform domain techniques have an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions [15]. The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it.

4.2.1 JPEG Compression

If an image is to compress into JPEG format, the RGB color space is first turned into a YUV representation. Through this representation, the Y component represents brightness (or luminance) and the U and V components stand for color (or chrominance). It is known that the human eye is more sensitive to changes in the brightness of a pixel than to changes in its color [24]. Down sampling the color information is taken as an advantage of the JPEG to reduce the size of the file Where the color components (U and V) are splitted in the horizontal and vertical directions and consequently reducing the file size by a factor of 2 [37].

Then, the image is transformed. For JPEG images, the discrete cosine transform (DCT) is used; the pixels can be converted with such mathematical processing by simply “spreading” the position of the pixel values over the image or part of it [17]. With DCT transformation, a signal is transformed from the representation of an image into the frequency domain, this is done by sorting the pixels into (8 × 8) pixel blocks and transforming these blocks into 64-DCT coefficients which are affected by any modification of a single DCT coefficient.

The quantization phase of the compression is counted as the next step. Besides it is considered as biological property where the human eye is imposed. Basically, the human eye is known for being capable of identifying small differences in brightness over a relatively large area. The same does not apply when considering the distinction between different strengths in high-frequency brightness [3]. Consequently, the strength of higher frequencies can be reduced without any change in the image appearance. The JPEG format is done by dividing all the values in a block via a quantization coefficient, so the results are made approximate to integer values. The last point is to encode the coefficients by using Huffman coding just to reduce the size.

4.2.2 JPEG steganography

Previously, it was believed that steganography could not be used with JPEG images owing to the lossy compression, which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise. Data in most of the steganographic systems seems to be embedded into the non-zero discrete cosine transform (DCT) coefficients of JPEG images. The major JPEG steganographic methods can be described as follows:

- JSteg/JPHide. Jsteg and JPHide are two classic JPEG steganographic tools that employ the LSB embedding technique [21]. JSteg functions to hide the secret data in a cover image by simply exchanging the LSBs of non-zero quantized DCT coefficients with secret message bits. The quantized DCT coefficients, already used to conceal secret message bits in JPHide, are selected randomly by a pseudo-random number generator. JPHide, on the other hand, tends not only to modify the LSBs of the selected coefficients, but it can also switch to a process where bits of the second least-significant bit-plane are likely to be worked out [8].

- F5. The F5 steganographic algorithm was introduced by Westfeld [25]. Rather than replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is reduced by the F5 algorithm by one if it needs modification. Due to the author's argument, the use the chi-square attack can never detect this type of embedding [26]. In addition to embedding message bits into randomly chosen DCT coefficients, the F5 algorithm employs matrix embedding that reduces the number of changes necessary for hiding a message of a certain length. Both, the message length and the number of non-zero coefficients are required in the embedding process to determine the matrix embedding needed to decrease the number of modifications required in the cover image [18].

- OutGuess. OutGuess is provided by Provos as a UNIX source code for which there are two widely known released versions [27]. The first one is the OutGuess-0.13b, which is exposed to statistical analysis, and the second is OutGuess-0.2, which includes the ability to safeguard statistical properties. Hereafter, OutGuess refers to OutGuess-0.2. There are two stages representing the embedding process of OutGuess. The first of which is that OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0s and 1s.Soon after modifications are made to the coefficients already left during embedding to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be subjected to a chi-square attack [18, 26].

- MB. Model-based steganography (MB) can be defined as a general framework for conducting both steganography and steganalysis by simply using a statistical model of the cover media [28]. The MB method for JPEG images is capable of having high message capacity while remaining secure against many first-order statistical attacks [18].

- YASS. Yet another steganographic scheme (YASS) belongs to JPEG steganography, but does not conceal data in JPEG DCT coefficients directly [29]. Instead, an input image in the spatial domain is divided into blocks with a fixed large size, called big blocks (or B-blocks). A later stage is to randomly select within each B-block, an 8 × 8 sub-block known as embedding host block (or H-block). Then via using error correction codes, secret data is encoded and embedded in the DCT coefficients of the H-blocks. Finally, the entire image is compressed and distributed as a JPEG image after inversing DCT on the H-blocks [18].

4.2.3 Wavelet Transform Technique

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. The discrete wavelet transform (DWT) method is favored over the discrete cosine transform (DCT) method, owing to the resolution that the WT provides to the image at various levels [30].

Wavelets are mathematical functions that divide data into frequency components, which makes them ideal for image compression. In contrast with the JPEG format, they are far better at approximating data with sharp discontinuities [15].

In [31, 32], a group of writers discuss a steganography technique, based on wavelet compression techniques, that attaches attribute information to images in order to reduce the amount of information stored in a database of images. They use the homogenous connected region interested ordered transmission (HCRIOT) wavelet algorithm for image encoding and compression. This technique embeds secret information in the edge and detail regions of the image where the human eye is less sensitive to the noise generated by the technique. In general, the human eye is more sensitive to noise in the smooth regions of an image.

In the project described in [33], researchers use vector quantization, called Linde-Buzo-Gray (LBG), associated with block codes, known as BCH codes, and one-stage discrete Haar wavelet transforms. They emphasize that modifying data by using a wavelet transformation produces good quality with few perceptual artifacts.

A group of scientists at Iowa State University are developing an advanced application called artificial neural network technology for steganography (ANNTS), with the aim of detecting all current steganography methods, which include DCT, DWT, and DFT. They found that the inverse discrete Fourier transform (IDFT) includes a rounding error that makes DFT inappropriate for steganography applications [34].

The research discussed in [35] proposes, a data hiding technique in the DWT domain. DWT with the first level is used to decompose both secret and cover images, where each is broken into disjoint (4 × 4) blocks. Then a comparison is made between the blocks of the secret image and the cover blocks to determine the best match. Later, error blocks are produced and embedded into the coefficients of the best matched blocks in the HL part of the cover image.

In [30], the authors proposed high capacity and high security steganography using the discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and the payload are merged into a single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to minimize the pixel range to ensure accurate recovery of the payload at the receiving end. The capacity of the proposed algorithm is increased as only the approximation band of the payload is considered. The entropy, mean square error (MSE) and capacity are improved with an acceptable peak signal to noise ratio (PSNR).

4.3 Spread Spectrum Technique

Spread spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image. Cover image as noise

A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub images [15].

When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum steganography. When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum steganography. These techniques require searching the image for the carrier in order to then retrieve the data. These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier. In this case, after the carrier is created, and before the message is added, the carrier is compressed using JPEG compression and decompression such that it will be unaffected by later JPEG compression of the cover image [36]. The capacity can be traded directly for robustness, and it depends greatly on the image.

- Pseudo-noise

This technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect [37]. Spread spectrum image steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error control coding, and image processing to hide information in images, is an example of this technique [38]. The general additive embedding scheme can be described as follows:

$$Y_i = X_i + \gamma W_i \quad \text{For } i = 1, 2, ..., N \tag{5}$$

Where X_i is a sequence of the original data from the cover,

W_i is a pseudo-random sequence generated from a pseudo-random number generator (PRNG) initialized by a secret stego key,

γ is an embedding strength parameter (gain factor), and Y_i is a sequence of possibly altered data.

In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible not only to the human eye but also through computer analysis without access to the original image.
The last few years witnessed the development of several steganography techniques one of which is spread spectrum steganography. In 1996, Smith and Comiskey described three schemes, namely direct sequence, frequency hopping, and chirp [36]. In image steganography, it is noticed that high frequencies usually aid the invisibility of the hidden information, but at the same time, they are not efficient as far as robustness is concerned. In contrast, low frequencies are better with respect to robustness, but are far too visible to be useful. Such conflicting points are reconciled by the spread spectrum technique via allowing the embedding of a low-energy signal in each one of the frequency bands, and as illustrated in [21].

Instead of using direct sequences, two new processing methods are proposed and shown in [39].Such methods include block spread spectrum and duplicate spreading. Spread spectrum techniques are capable of being combined with transform embedding by using transformation techniques in order to get the payload capacity increased. In [40][5], the authors introduce a technique based on discrete Fourier transform (DFT) that can significantly increase the number of transform coefficients that can transmit hidden information. A blind image steganography, based on a hybrid direct sequence/frequency hopping (DS/FH) technique, is described in [41], in which the system retrieves the hidden message without needing the original image. The authors in [42] found that using a signature vector, when embedding a spread spectrum (SS) message, maximizes the signal-to-interference-plus-noise ratio (SINR) at the output of the corresponding maximum-SINR linear filter.

The research in [43] describes the benefits of combining the spread spectrum technique with the advantages of error correction coding and DFT simply to the robustness of the system increased.
Finally, an analysis is presented in [44] proposes using a code division multiple access (CDMA) spread spectrum for both the spatial domain and the transform domain for image steganography in MMS. Their experimental results reveal that the spread spectrum detection method is highly robust for normal signal manipulation.

4.4 Statistical Methods

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [17].

Statistical steganographic techniques exploit the existence of a "1-bit", where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a "1" is transmitted, otherwise it is left unchanged [45]. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message [15].

Another technique, called data masking, has been proposed in [46]. According to this technique, the message signal is processed such that it views the properties of an arbitrary cover signal.
In work [28], the authors propose a method where the transformed image coefficients are broken down into two parts to allow the coded message signal to replace the perceptually insignificant component. Hence, the statistics of the quantized (non-zero) AC DCT coefficients are modified taking into consideration the parametric density function. This process requires a low precision histogram of each frequency channel in addition to matching the model with each histogram by deciding the corresponding model parameters.

However, statistical steganographic methods in their simplest form, for which sub-images are simply sub-rectangles of the original image, are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. To counter these attacks, the sub-images could be selected based on picture elements, for example, the faces in a crowd, and error correction coding could be utilized within the message. These defenses can make the statistical steganographic method approximately as robust as the underlying watermarking scheme [15].

4.5 Distortion Techniques

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image [46]. So, information is described as being stored by signal distortion [30].

Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit [45].

The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, then the message bit is a "1." Otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such manner that the statistical properties of the image are not affected (which is different from many LSB methods). However, the need for sending the cover image limits the benefits of this technique. As in any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, rotating, or scaling, the receiver can easily detect the modification. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be fully recovered [15].

An early approach to hiding information was to do so in text. Most text-based hiding techniques are of the distortion type. For example, the layout of a document or the arrangement of words might show or reflect the presence of information. Considering one of these techniques, can show the adjustment of the positions of lines and words where spaces and "invisible" characters are added to the text, providing a method of sending hidden information [45].

4.6 File Embedding

Different image file formats are known for having different header file structures. In addition to the data values, such as pixels, palette, and DCT coefficients, secret information can also be hidden in either a header structure or at the end of the file [47]. For example, the comment fields in the header of JPEG images usually contain data hidden by the invisible Secrets and Steganozorus. Camouflage, JpegX, PGE10, and PGE20 add data to the end of a JPEG image.

Image storage formats such as TIFF, GIF, PNG, and WMF have a file header that can be exploited to hide arbitrary information. In this case, that arbitrary data may be a secret message. It is possible to append data to many image storage formats without affecting the image. When the image is processed for display, the image user will decode the image size from the file header, and any tracking information attached to the end of the file will be ignored. Using this technique, it is possible to attach a message of any size to a cover image. However, the message could be removed from the cover image by simply resaving the image in the same file format [15]. The limitations of this method are that despite the large payload, it is not that difficult to identify and defeat, it is weak when lossy compression and image filtering are concerned, and the resaving of the image implies complete loss of hidden data [48].

4.7 Pallet Embedding

In a palette-based image, what matters is the fact that only a subset of colors from a particular color space is used to colorize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colors as a list of indexed pairs (i, c_i), assigning a color vector c_i to every index i, and the actual image data, which specifies a palette index for each pixel, rather than the color value itself. The file size gets decreased via this approach when only a limited number of color values are used in the image. Two of the most popular formats are the graphics interchange format (GIF) and the bitmap format (BMP). However, owing to the availability of advanced compression techniques, their use has diminished [21].

In some cases, the palette itself can be used to hide secret information. Because the order of the colors in the palette usually does not matter, the ordering of colors can be used to transfer information. In essence, a hidden message can be embedded using the difference between two colors in the palette (i.e., one secret message bit for every two colors in the palette). Color palettes are used to minimize the amount of information images that are used to represent colors [15].

Since steganographic message within the bits of the palette and/or the indices is embedded in the palette-based steganography, one must be careful not to exceed the maximum number of colors [49, 50].

4.8 Image Generation Technique

Many techniques have been proposed that encrypt messages so that they are unreadable or as secret as possible. Big Play Maker hides information by converting the secret text message into a larger and a slightly manipulated text format. The same principle can be employed in image creation, in which a message is converted to picture elements and then collected into a complete stego-image. This method cannot be broken by rotating or scaling the image, or by lossy compression. Parts of the message may be destroyed or lost because of cropping, but it is still possible to recover other parts of the message by encoding the message with error correcting information.

Generally, this technique uses pseudo-random images, because if a malicious third party detects a group of images passing through a network without any reason for them being there (i.e., random images), he or she may suspect that the images contain secret information and block their transmission [15].

4.9 Image Element Modification Techniques

Some steganographic techniques do not try to hide information using the actual elements of the image. Instead, they adjust the image elements in completely undetectable ways, for example, by modifying the eye color or hair color of some person in a photograph. These modifications can then be used to carry the hidden information. In addition, this information will survive rotations, scaling, and lossy compression.

The feasibility of modifying objects within images as a tactic for hiding information has been discussed by [51]. It is important to keep in mind that when this method is used, the same cover image must not be used more than once, because the elements used will become apparent. This technique can be achieved manually with any photo editing software. With the advent of computer vision systems that identify objects within pictures, these methods have become more viable.

4.10 Adaptive Steganography

Adaptive steganography is a special case of the spatial and transform techniques. Moreover, it is introduced as statistics-aware embedding and masking. Global statistical characteristics of the image are basically used before any attempt to deal with its frequency transformed coefficients. These statistics decide what changes can be made. A random adaptive selection of pixels actually characterizes this method, relying on the cover image and the selection of pixels in a block with a large standard deviation (STD). The latter is intended to avoid areas of uniform color, such as smooth areas. This technique is known for exploiting images with existing or deliberately added noise and with images that show color complexity [52, 53, 54, 55].

An adaptive technique applied to the LSB substitution method has been proposed in [56]. The idea behind this method is to make use of the correlation between neighboring pixels so as to calculate the degree of smoothness. The researchers shed light on the options of having two-, three-, and four-sided matches. The payload (embedding capacity) they were able to obtain was high.

A technique called the “adaptive more surrounding pixels using” (A-MSPU) technique, which improves the imperceptibility problems of multiple base notational systems (MBNS), has been discussed in [57]. This technique pays attention to the edge areas of a cover image while re-expressing the secret bits in multiple base notational systems. The suggested approach uses the same probability parameter to get the secret bits scattered and it also uses surrounding pixels with the maximum number to determine the capacity of every target pixel. Most steganographic techniques use either three or four adjacent pixels of a target pixel. The proposed technique is able to utilize all eight adjacent neighbors, which improves the imperceptibility value.

5. PERFORMANCE MEASURE

As a performance measure for image distortion due to embedding, the well-known peak-signal-to-noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images [55]. It is defined as:

$$PSNR = 10\log(\frac{C_{\max}^{\ 2}}{MSE}) \tag{6}$$

where MSE denotes the mean square error, which is given as

$$MSE = \frac{I}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \tag{7}$$

Here, $C_{\max}$ indicates the maximum value in the image, for example:

$$C_{\max} \leq \begin{cases} 1 & in\ double\ precision\ images \\ 255 & in\ 8-bit\ unsigned\ \text{int}\ eger\ images \end{cases}$$

In addition, x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the resultant stego image, and C_{xy} is the cover image. In [58, 59], C_{xy} is set to 255, as an agreed default value for 8-bit images. It can be that an image has only up to 253, or fewer, gray colors. Having $C_{\max}$ is raised to the power of 2 results in a strong change to the PSNR value. For this reason, $C_{\max}$ is considered as the actual maximum value rather than the largest possible value [48]. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is clear). A high-quality stego image should strive for a PSNR of 40 dB, or higher.

6. EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. Fridrich in Fig. 2 shows the relationship between three parameters [60]. These parameters are as follows:

- Undetectability (imperceptibility): this parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.
- Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique (out of the scope of this paper).
- Payload capacity: it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests.

The following paragraphs compare the previously mentioned steganographic techniques in terms of the competing parameters.

- LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression [7]. Although LSB techniques can hide large quantities of information i.e., high payload capacity, they often compensate the statistical properties of the image and thus indicate a low robustness against statistical attacks as well as image manipulation.

- The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms [8]. The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers' attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival [8].

- Spread spectrum techniques are generally quite robust against statistical attacks, since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction [9].

- The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. Defenses could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depends on the cover image selected.

- Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS.

- Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data [48].

- Hiding information via steganographic techniques that modify the elements in the visual image results in a stegoimage that will survive rotation, scaling and much lossy compression like JPEG. A reasonable payload capacity can be achieved with this technique as well. Table 1 summarizes the evaluation of the mentioned techniques through this paper.

	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet Embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

TABLE 1: A comparison of Image Steganography Techniques

*: Indicates dependency on the used cover image

7. CONCLUSION

This paper reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and robustness). From TABLE 1, one can deduce that while one technique may lack in payload capacity, another may lack in robustness. For example, file formatting techniques can store large amounts of information, but they are easily detected and attacked. Likewise, LSB techniques in a spatial domain have a high payload capacity, but they often fail to prevent statistical attacks and are thus easily detected. It is important to notice that the hiding capacity in LSB technique depends on the cover image being used. LSB in BMP images is capable of hiding relatively a large message, but large amount of altered bits results in a larger possibility of detection by human eye. While LSB in GIF images is approximately the same as that of using LSB in BMP images. The only difference is related to the structure of the GIF images, since they only have a bit depth of 8. Thus, the amount of hidden information is less than with BMP. In addition, LSB in GIF is mainly dependent on the file format and the image itself. Incorrect choice of cover image could result in visible message.

Besides, file and spatial domain approaches are considered not to be robust against lossy compression and filtering. Transform domain techniques are considered more robust for lossy compression image formats, but this advantage is achieved at the expense of payload capacity. However, it is possible to defeat the transform domain techniques, but with some efforts.
For most of steganography applications, JPEG file format can be used, especially for images that have to be communicated over an open systems environment like the Internet

Thus, for an agent to send secret information using steganographic techniques, he or she must select a suitable steganographic algorithm and suitable cover image as well. The required application is the only thing to decide the most appropriate steganographic method among all the present image steganographic techniques.

In short, one must have the determination to compromise on some characteristics to ensure the high performance of other characteristics.

FIGURE 1: Steganography Types

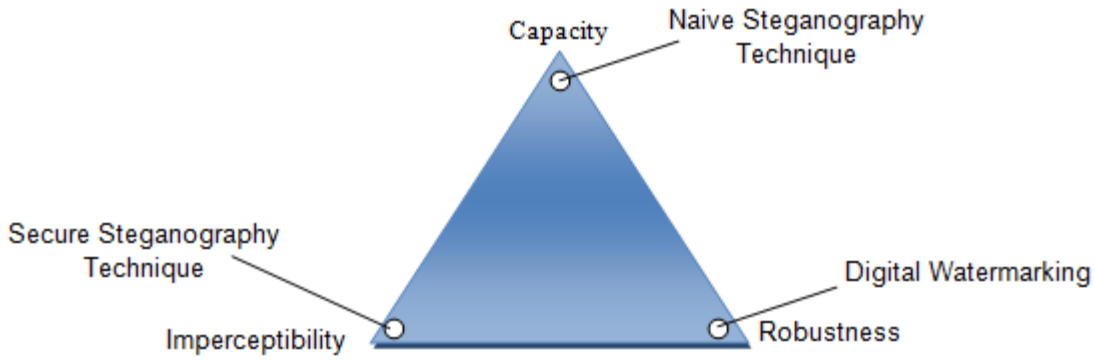


FIGURE 2: Competing factors in steganographic systems [60]

8. REFERENCES

[1] S.A. Halim and M.F.A Sani. "Embedding using spread spectrum image steganography with GF (2^m)," in Proc. IMT-GT-ICMSA, 2010, pp. 659-666.

[2] N.N. El-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm." Computer Science. [On-line]. 3(4), pp. 223-232. Available: www.thescipub.com/pdf/10.3844/jcssp.2007.223.232 [Dec., 2011].

[3] T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, 2005, pp. 1-11.

[4] L. Chun-Shien. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. USA: Idea Group Publishing, 2005, pp. 1-253.

[5] R.J. Anderson and F.A.P. Petitcolas. (1998, May). "On the limits of steganography." IEEE Journal of Selected Area in Communications. [On line]. 16(4), pp. 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[6] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert. Digital watermarking and steganography. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[7] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[8] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal. [On line]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[9] M. Fortrini. "Steganography and digital watermarking: A global view." University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf . [June 2011].

[10] N. Provos and P. Honeyman. (2003, Jun.). "Hide and seek: An introduction to steganography." IEEE Security and Privacy Journal. [On line], 1(3), pp. 32-44. Available: http://niels.xtdnet.nl/papers/practical.pdf [Jul., 2011].

[11] N.F. Johnson. (1995, Nov.). "Steganography. Technical report." Available: http://www.jjtc.com/pub/tr_95_11_nfj/ [Sep., 2011].

[12] D. Sellars. "An introduction to steganography. Internet: http://www.cs.uct.ac.za/courses/CS400W/papers99/stego.html [Jul., 2011].

[13] T. Jamil. (1999, Feb.). "Steganography: The art of hiding information in plain sight." IEEE Potentials. [On line], 18(1), pp. 10-12. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=747237 [Sep., 2011].

[14] S.B. Sadkhan. "Cryptography: Current status and future trends." in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.

[15] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

[16] M.S. Prasad, S. Naganjaneyulu, CH.G. Krishna, and C. Nagaraju. (2009, Oct.). "A novel information hiding technique for security by using image steganography." Journal of Theoretical and Applied Informaion Technology. [On line]. 8(1), pp. 35-39. Available: www.jatit.org/volumes/research-papers/Vol8No1/6Vol8No1.pdf [Apr. 2011].

[17] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). "Image steganography: Concepts and practice." WSPC/Lecture Notes Series: 9in x 6in, [On line], pp. 1-49. Available: http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf [Aug. 2011].

[18] B. Li, J. He, J. Huang, and Y.Q. Shi. (2011, Apr.). "A survey on image steganography and steganalysis." Journal of Information Hiding and Multimedia Signal Processing. 2(2), [On line], pp. 142-172. Available: http://bit.kuas.edu.tw/~jihmsp/2011/vol2/JIH-MSP-2011-03-005.pdf [Dec., 2011].

[19] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. (1996). "Techniques for data hiding." IBM System Journal. 35(3/4), [On line], pp. 313-336. Available: http://www.almaden.ibm.com/cs/people/dgruhl/313.pdf [Nov., 2011].

[20] M. Juneja and P.S. Sandhu. "Designing of robust image steganography technique based on LSB insertion and encryption." IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.

[21] N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[22] K. Curran and K. Baily. (2006, Jul.). "An evaluation of image based steganography methods." Multimedia Tools and Applications Journal. [On line]. 30(1), pp. 55-88. Available: http://dl.acm.org/citation.cfm?id=1164470 [May, 2011].

[23] A.R. Naghsh-Nilchi, L. Pourmohammadbagher. (2006, Jun.). "A new approach to steganography using sinc-convolution method." PWASET Journal. [On line]. 14(1), pp. 324-329. Available: http://www.waset.org/journals/waset/v20/v20-4.pdf [May, 2011].

[24] D.L. Currie and C.E. Irvine. "Surmounting the effects of lossy compression on steganography." in Proc. of the 19th National Information Systems Security Conference, 1996, pp. 194-201.

[25] A. Westfeld. "F5-A steganographic algorithm: high capacity despite better steganalysis." in Proc. of the 4th Information Hiding Workshop, LNCS, 2001, pp. 289-302.

[26] A. Westfeld and A. Pfittzmann. "Attacks on steganographic systems- breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned." in Proc. of the 3rd Internet Workshop on Information Hiding, 1999, pp. 61-76.

[27] N. Provos. "Defending against statistical steganalysis." in Proc. of the 10th USENIX Security Symposium, 2001, pp. 323-325.

[28] P. Sallee. "Model-based steganography." in Proc. the 2nd International Workshop on Digital Watermarking, LNCS, 2004. pp. 254-260.

[29] K. Solanki and B.S. Manjunath. "Yass: Yet another steganographic scheme that resists blind steganalysis." in Proc. of the 9th Information Hiding Workshop, LNCS, 2007. pp. 1-16.

[30] H.S. Majunatha Reddy and K.B. Raja. (2009). "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security. [On line]. 3(6), pp. 462-472.
Available:
http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue6/IJCSS-163.pdf [Jun., 2011].

[31] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. "Exploring on steganography for low bit rate Wavelet based coder in image retrieval system." in Proc. of IEEE TENCON, 2000. pp. 250-255.

[32] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. "Steganography for low bit-rate Wavelet based image coder." in Proc. of IEEE ICIP, 2000. pp. 597-600.

[33] N.K. Abdulaziz and K.K. Pang. "Robust data hiding for images." in Proc. of IEEE International Conference on Communication Technology, 2000. pp. 380-383.

[34] L.D. Paulson. (2006, Aug.). "New system fights steganography. News briefs." IEEE Computer Society. [On line]. 39(8), pp. 25-27.
Available:
http://journals2.scholarsportal.info/details.xqy?uri=/00189162/v39i0008/25_nsfs.xml [Jul., 2011].

[35] A.A. Abdelwahab and L.A. Hasan. "A discrete Wavelet Transform based technique for image data hiding." in Proc. of 25th National Radio Science Conference, 2008. pp. 1-9.

[36] J.R. Smith and B.O. Comiskey. "Modulation and information hiding in images." in Proc. of the 1st Information Hiding Workshop, 1996. pp. 207-226.

[37] H. Wang and S. Wang. (2004, Oct.). "Cyber Warfare: steganography vs. steganalysis." Communications of the ACM. [On line]. 47(10), pp. 76-82.
Available: www.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf [Mar., 2011].

[38] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. (1999). "Spread spectrum image steganography." IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083. Available: http://www.mendeley.com/research/spread-spectrum-image-steganography-1/ [Apr., 2011].

[39] C.L. Tsai, K.C. Fan, and C.D. Chung. "Secure information by using digital data embedding and spread spectrum techniques." IEEE 35th International Carnahan Conference on Security Technology, 2001. pp. 156-162.

[40] F. Alturki and R. Merserau. "Secure blind image steganographic technique using Discrete Fourier Transform." in Proc. IEEE International Conference on Image Processing, 2001. pp. 16-162.

[41] K.C. Widadi, P.H. C.C. Wah. "Blind steganography using direct sequence/frequency hopping spread spectrum technique. in : Information, Communications and Signal Processing, 5th International Conference, 2006. pp. 1125-1129.

[42] M. Gkizeli, D.A., and M.J. Medley. (2007, Feb.). "Optimal signature design for spread-spectrum steganography." IEEE Signal Processing Society. [On line]. 16(2), pp. 391-405. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4060938 [Oct. 2011].

[43] R.S. Youail, A.-K.A.-R. Khadhim, and V.W. Samawi. "Improved stegosystem using DFT with combined error correction and spread spectrum." in 2nd IEEE ICIEA, 2007. pp. 1832-1836.

[44] R.S. Singh, M.A. Khani, and N. Singh. (2010, Dec.). "Spread spectrum image steganography in multimedia messaging service of mobile phones." International Journal of Electronics Engineering. [On line]. 2(2), pp. 365 – 369. Available: http://www.csjournals.com/IJEE/PDF%202-2/Article_29.pdf [Oct., 2011].

[45] S.C. Katzenbeisser. "Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[46] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. "Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.

[47] Y.O. Yildiz, K. Panetta, and S. Agaian. (2007, Apr.). "New quantization matrices for jpeg steganography." International Society for Optical Engineering. [On line]. 6579(1), pp. 6579OD. Available: link.aip.org/link/?PSISDG/6579/65790D/1 [Nov., 2011].

[48] A. Shaddad, J. Condell, K. Curran, and P. Mckevitt. "Enhancing steganography in digital images." IEEE Canadian Conference on Computer and Robot Vision, 2008. pp. 326-332.

[49] S.S. Agaian, B.M. Rodriguez, and J.P. Perez. "Palette-based steganography used for secure digital image archiving." IS&T Archiving Conference, 2005. pp. 159- 164.

[50] C.H. Tzeng, Z.F. Yang, and W.H. Tsai. (2004, May). "Adaptive data hiding in palette images by color ordering and mapping with security protection." IEEE Trans. on Communications. [On line]. 52(5), pp. 791-800. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1299069 [Dec., 2011].

[51] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb. (2000, Jul.). "Applications for data hiding." IBM Systems Journal. [On line]. 39(3&4), pp. 447- 568. Available: http://www.almaden.ibm.com/cs/people/dgruhl/afdh.pdf [Dec., 2011].

[52] E. Franz and A. Schneidewind. "Adaptive steganography based on dithering." in Proc. of the 2004 workshop on Multimedia and Security, 2004. pp. 56-62.

[53] R. Bohm and A. Westfeld. "Breaking cauchy model-based JPEG steganography with first order statistics." In Proc. of ESORICS'2004, 2004. pp. 125-140.

[54] A.M. Fard, M. Akbarzadeh-R., and F. Varasteh-A. "A new genetic algorithm approach for secure JPEG steganography." in Proc. of IEEE International Conference on Engineering of Intelligent Systems ICEIS, 2006. pp. 216-219.

[55] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt. "Biometric inspired digital image steganography." In Proc. of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008. Pp. 159-168.

[56] C.C. Chang, P. Tsai, and M.H. Lin. "An adaptive steganography for index- based images using code word grouping." Lecture Notes in Computer Science, 2004. pp. 731-738.

[57] M. Afrakhteh and S. Ibrahem. "Adaptive steganography scheme using more surrounding pixels." IEEE International Conference on Computer Design and Applications, 2010. pp. 225-229.

[58] Z.Z Kermani and M. Jamzad. "A robust steganography algorithm based on texture similarity using Gabor filter." in Proc. of IEEE 5th International Symposium on Signal Processing and Information Technology ISSPIT, 2005. pp. 578-582.

[59] A.I. Hashad, A.S. Madani and A.E.M.A. W ahdan. "A robust steganography technique using Discrete Cosine Transform insertion." In Proc. of IEEE/ITI 3rd International Conference on Information and Communications Technology, 2005. pp. 255-264.

[60] J. Fridrich. "Applications of data hiding in digital images." Tutorial for the ISPACS'98 Conference, 1998.

Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks

R. Murugan *muruganraam75@yahoo.com*
Associate Professor / Department of Computer Applications
Bannari Amman Institute of Technology
Sathyamangalam, 638401, INDIA

A. Shanmugam
Professor / Department of Electronics and Communication Engineering
Bannari Amman Institute of Technology
Sathyamangalam, 638401, INDIA

Abstract

In mobile ad hoc networks, the misbehaving nodes can cause dysfunction in the network resulting in damage of other nodes. In order to establish secure communication with the group members of a network, use of a shared group key for confidentiality and authentication is required. Distributing the shares of secret group key to the group members securely is another challenging task in MANET. In this paper, we propose a Cluster Based Misbehavior Detection and Authentication scheme using threshold cryptography in MANET. For secure data transmission, when any node requests a certificate from a cluster head (CH), it utilizes a threshold cryptographic technique to issue the certificate to the requested node for authentication. The certificate of a node is renewed or rejected by CH, based on its trust counter value. An acknowledgement scheme is also included to detect and isolate the misbehaving nodes. By simulation results, we show that the proposed approach reduces the overhead.

Keywords: Clustering Technique, Misbehaving Nodes, Trust Count, Threshold Cryptography, Key Share

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of dynamic, independent, wireless devices that groups a communications network, devoid of any backing of a permanent infrastructure. The eventual goal of designing a MANET is to make available a self-protecting, "dynamic, self-forming, and self-healing network" for the dynamic and non-predictive topological network [1]. According to the positions and transmission range, every node in MANET acts as a router and tends to move arbitrary and dynamically connected to form network. The topology of the ad hoc network is mainly interdependent on two factors; the transmission power of the nodes and the Mobile Node location, which are never fixed along the time period [2].

Ad hoc networks excel from the traditional networks in many factors like; easy and swift installation and trouble-free reconfiguration, which transform them into circumstances, where deployment of a network infrastructure is too expensive or too susceptible [5]. MANETs have applicability in several areas like in military applications where cadets relaying important data of situational awareness on the battleground, in corporate houses where employees or associates sharing information inside the company premises or in a meeting hall; attendees using wireless gadgets participating in an interactive conference, critical mission programmer for relief matters in any disaster events like large scale mishaps like war or terrorist attacks, natural disasters and all. They are also been used up in private area and home networking, "location-based" services, sensor networks and many more adds up as services based on MANET [4]. The three major

drawback related to the quality of service in MANET are bandwidth limitations, vibrant and non-predictive topology and the limited processing and minimum storage of mobile nodes [3].

1.1 Misbehaving Nodes in MANETs

The misbehaving nodes or critical nodes are defined as the nodes that cause malfunction in network and damage other nodes [6].

1. Malfunctioning nodes: These causes hardware failures or software errors in the network.

2. Selfish nodes: These nodes refuse to forward or drop data packets
The three categories of selfish nodes are:
i) Node will take active participation in the route discovery and route maintenance; however will refuse to forward data packets in order to save its resources.

ii) Node will not participate in route discovery phase as well as data forwarding phase but only use their resources for transmission of their own packets.

iii) Nodes behaves in proper manner if its energy level lies between full energy-level and certain threshold T_1. Here, there are two cases.

- If energy level lies between T_1 and T_2, this node performs as type ii
- If energy level falls below T_2, this node performs as type i.

3. Malicious nodes: The nodes with the help their own resources try to lessen the strength of other nodes or networks by taking part in all established routes, thus compelling other node to use a malicious route which is under their control. When they are selected in requested route, they result in serious attacks by dropping all received packets similar to black hole attack or by selecting dropping packets in the similar manner as Gray hole attack [7].

1.2 Threshold Cryptography

The Shamir's algorithm offers the threshold cryptography technique. In this scheme, the authentication protocol necessitates a node to get adequate partial signatures from one-authenticated node to construct a full signature. Initially a node forwards a Certification Request Message (C_{REQ}) and those nodes that receives the request after processing sends reply as a partial signature (C_{REP}). The node that sent the request gathers entire C_{REP} for generating a legitimate full signature on availability of adequate replies within assured time duration [8].

The means of providing the shared key to the node without key infrastructure assistance is provided by threshold cryptographic approach and this scheme is appropriate for secret key sharing in MANET. Though only t or more shares are provided in (n, t) threshold cryptography, the secret S can be obtained. With the lack of share refresh scheme and with never-ending time duration, a malicious node can compromise minimum t shares holder nodes to get secret key. In order to refresh the share in secured manner, a proactive secret sharing scheme (PSS) is deployed along with the threshold cryptography. This scheme permits refreshment of all shares by generating new group of shares of the similar secret key from the old shares excluding the reconstruction of the secret key [9].

1.3 Problem Identification

In [14], a cluster based authentication technique is proposed for mitigating the internal attacks. The entire network is divided into hierarchical group of clusters. The entire network is divided into hierarchical group of clusters, each cluster having a fully trusted cluster head. Each node holds a certificate issued by an offline certificate authority (CA). The Trust Count (TC) for each of the nodes can be estimated periodically for every trust evaluation interval (TEI), based on their

access policy (AP). The certificate of a node is renewed or rejected by the cluster head, based on its trust counter value.

In [15], an efficient timer based acknowledgement technique is proposed that allows the detection and isolation of the misbehavior nodes and can even find a possible alternate route in case of current route failure. This involves a detection timer and forward counter that help to reduce the number of acknowledgements thus reducing the delay and overhead. This approach is keenly focusing on acknowledgement of nodes regarding the misbehaviors so that the source takes the corresponding action.

In this paper, we propose a new approach called threshold cryptography coupled acknowledgement scheme for attack detection in MANET.

2. RELATED WORKS

Hitoshi Asaeda et al [9] proposed a Proactive Secret Sharing (PSS) scheme in mobile ad hoc networks. The proposed scheme is related to threshold cryptography along with the methods to bootstrap secret group key. In this scheme, all shareholder nodes coordinates the PSS procedure in a well-managed fashion to maintain the reliability of the protocol.

GSR Emil Selvan et al [10] proposed a compromised node detection scheme in ad hoc networks. The proposed approach is based on threshold cryptography and Chinese remainder theorem. All nodes concerned with the transmission process are authenticated. Then, threshold cryptography is used to share the message and Chinese remainder theorem for routing verification and to validate whether the node is authenticated or not. The problem of compromised nodes such as message dropping, message alteration and routing to wrong destination are addressed.

S.M. Sarwarul Islam Rizvi et al [11] proposed a security module based on threshold cryptography for protecting the mobile agent and agent server in an ad hoc network. The threshold cryptography is a new environment in the cryptographic world where trust is distributed among multiple nodes in the network. The proposed approach offers prime security services like confidentiality, integrity and authenticity.

Sanjay Raghani et al [12] proposed the design of distributed CA based on threshold cryptography for mobile ad hoc networks. The proposed protocol is extended with a set of monitoring protocols by offering dynamic behavior. The protocol allows the distributed CA to dynamically update the threshold value by monitoring the average node degree of the network and thus avoiding the increase in the certification renewal delay.

Keun-ho lee et al [13] proposed authentication protocol based on Hierarchical Clusters in Ad hoc Networks (AHCAN). The proposed scheme designs an end-to-end authentication protocol that relies on mutual trust between nodes in other clusters. It uses certificates containing an asymmetric key using the threshold cryptography scheme. The establishment of secure channels, the detection of reply attacks, mutual end-to-end authentication, prevention of node identity fabrication, and secure distribution of provisional session keys are included using shadow key certification of the threshold key configuration.

3. PROPOSED WORK

3.1 Proactive Secret Sharing Technique

The Threshold cryptography is the technique utilized to share the secret among the nodes. In order to make the sharing scheme more secured, a proactive secret sharing scheme is deployed along with the threshold cryptographic approach. This scheme permits refreshment of all shares by generating a new set of shares for a similar secret key from the old shares exclusive of renovating the secret key [9].

Let K represent the secret group key and k_1, k_2…., k_n represents the sub-shares.

Let the node N_a be the share holder

The proactive secret sharing scheme is described using the following steps.

1) N_a randomly generates its sub-shares (k_{a1}, K_{a2},… K_{an})
2) Every sub-shares k_{ab} (b=1, 2,…n) is distributed to node b through secure link.
3) When b receives the sub-shares (k_{1b}, k_{2b},….. k_{nb}), it calculates a new share from the received sub-shares and old shares using the following equation.

$$K_b' = k_b + \sum_{a=1}^{n} k_{ab} \qquad \text{- (1)}$$

4) Each shares (k_1', k_2'……k_n') is sharing of the secret key K, since $\sum_{b=1}^{n} k_{ab} = 0, \forall a \in \{1,....,n\}$.

3.2 Clustering Technique

The complete set of nodes is divided into a number of groups and the nodes inside each group are subdivided into clusters. Each group has a group leader and cluster is headed by the cluster head. Specifically, one of the nodes in the clusters is head .A set of clusters form a group and each group is headed by a group leader. The nodes contained in a cluster are physical neighbors, and they use contributory key agreement, and they further contribute their shares in arriving at the group key. When there is change in membership, the neighbor node initiates the re-keying operation, thus reducing the burden on the cluster head. The group leader selects a random key to be utilized for encrypting messages exchanged connecting the cluster heads and the network head. It forwards the key to the group leader that is used for communication among the group leaders.

3.2.1 Cluster Formation

Step 1: After deployment, the nodes broadcast their id value to their neighbors along with the HELLO message.

Step 2: When all the nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors is selected as the cluster head. Other nodes become members of the cluster or local nodes. The nodes update the status values accordingly.

Step 3: The cluster head broadcasts the message “CLHEAD” so as to know its members.

Step 4: The members reply with the message “CLMEMBER” and in this way clusters are formed in the network.

Step 5: If a node receives more than one “CLHEAD” messages, it becomes Gateway which acts as a mediator between two clusters.

In this manner clusters are formed in the network. The cluster heads broadcast the message, “CLHEAD EXCHANGE” so as to know each other. The cluster head with the least id is chosen as the leader of the cluster heads which is representative of the group termed as group leader. Each CH maintains a list of IP addresses of all other CH in the network. The group leaders will be in contact with other group leaders in similar way, and one among the group leader is selected as the leader for entire network.

3.2.2 Key Sharing Scheme

Step 1

Each group (G) holds a group key (or secret key) K and respective group leader (GL) splits K into equal shares which is represented as $\{k_1, k_2, k_3, \ldots\ldots, k_n\}$

Step 2

G distributes the shares among the clusters in the group and the number of shares received by the cluster is based on the following condition.

The number of shares received by each cluster = $\frac{Total\_number\_of\_shares}{number\_of\_clusters}$

Step 3

Upon receiving the shares, the cluster heads starts distributing the shares to its member nodes.

Step 4

Every member node that receives the share generates the sub-shares and exchanges the sub-shares with all other member nodes. Then each node computes the new share value with the old share and received sub-share.

New share = old share + $\sum$new sub-share received by the node

Step 5

Every node transmits its new share value to respective CH. Further, CH updates the new share of its member nodes.

Step 6

When any node requests a certificate from CH, CH broadcasts certification request (C_{REQ}) message to its neighbor CHs within the group.

Step 7

Every CH that receives the $C_{REQ,}$ replies with certificate reply (C_{REP}) message that contains the latest group key shares of each member.

Step 8

CH gathers the entire share and if the required amount of share is obtained (using (n, t) threshold cryptography described in section 1.4), a valid certificate is generated with the group key and the CH sends it to the requested node.

Figure 1 represents the group G comprising three clusters. G possess the group key K and GL splits the key into shares as per existing number of cluster within the group. K is split into 12 shares (i.e. n=12) which is represented as $\{k_1, k_2, \ldots, k_{12}\}$ and distributed among the clusters as per following condition.

The number of shares received by each cluster = $\frac{total\_number\_of\_shares}{number\_of\_clusters}$

$$= \frac{12}{3} = 4$$

Thus each cluster receives 4 key shares, randomly.

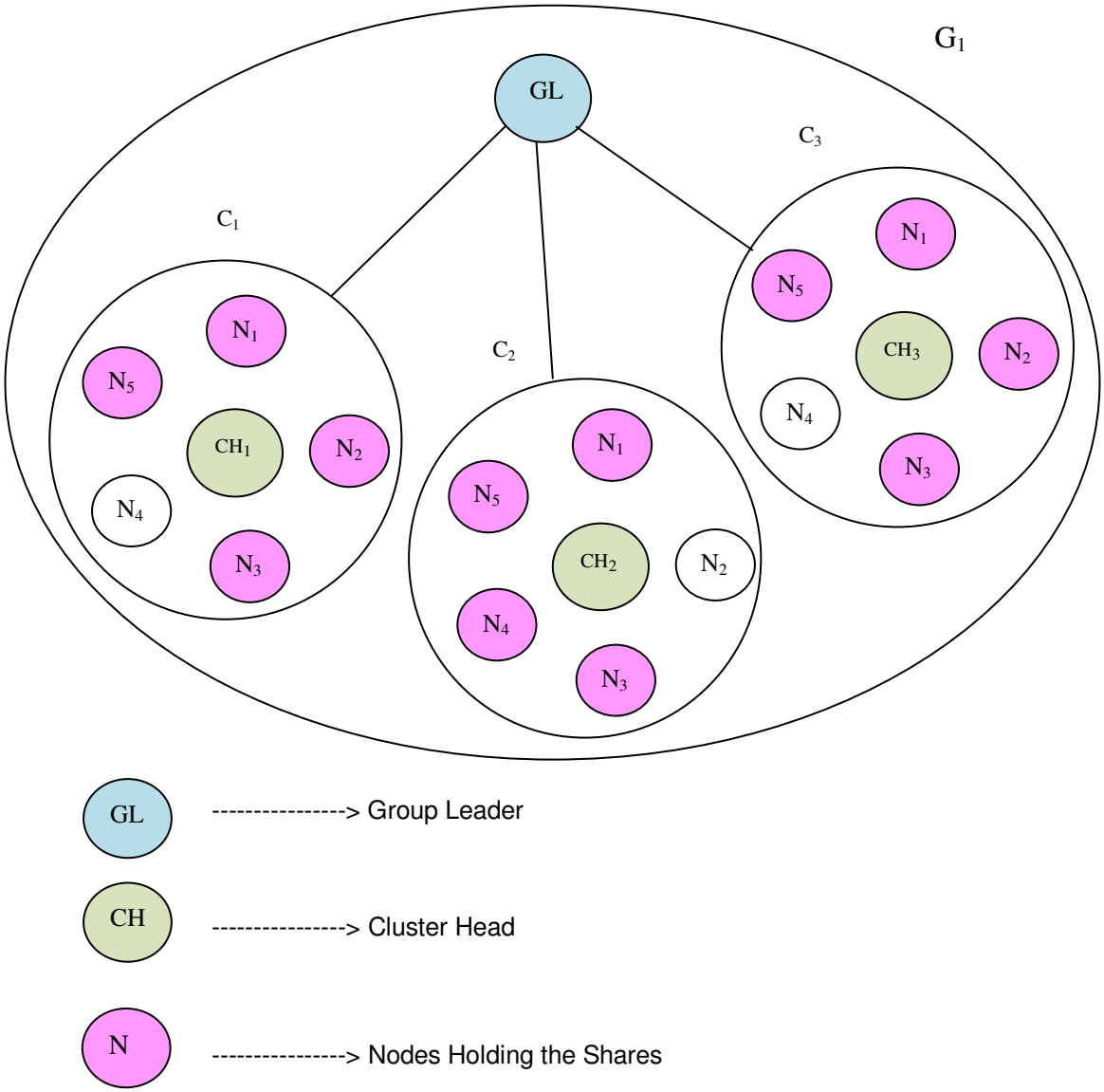


FIGURE1: Key Sharing Scheme

C_1 receives 4 key shares i.e k_1, k_2, k_3 and k_4. The node 1, 2, 3 and 5 within the C_1 receives these shares and these nodes generate the sub-shares. Table 1 represents the node list and its corresponding shares and sub-shares.

Node	Key shares	Sub–shares
Node 1	k1	$k_{11},k_{12},k_{13},k_{15}$
Node 2	k2	$K_{21},k_{22},k_{23},k_{25}$
Node 3	k3	$K_{31},k_{32},k_{33},k_{35}$
Node 5	k4	$k_{51},k_{52},k_{53},k_{55}$

TABLE 1: Nodes and its Shares

Node 1 exchanges its sub-share with all other share holders and generates a new shares.

New share of node 1, k_1"= old share + sum of newly received sub-share

$$= k_1 + (k_{21} + k_{31} + k_{51})$$

Similarly, new share by node 2, 3 and 5 are as follows.

$k_2" = k_2 + (k_{32}+k_{12}+k_{52})$

$k_3"= k_3 + (k_{13}+k_{23}+k_{53})$

$k_5"= k_4 + (k_{15}+k_{35}+k_{25})$

The node 1, 2, 3, and 5 transfers their respective new shares k_1", k_2", k_3" and k_5" to CH_1.
Similarly, the above process is performed in clusters C_2 and C_3 in the group G.

In case, node 2 requests a certificate from CH_1, then CH_1 sends the C_{REQ} to its neighbor cluster heads CH_2 and CH_3. These CHs reply CH_1 with C_{REP} message that contains their respective shares of the group key K. CH_1 collects entire shares obtained from CH_2 and CH_3 along with its own shares. If it contains atleast 8 shares out of 12 shares (n, t threshold cryptography), then a certificate can be generated. CH_1 sign the certificate with group key K and it is forwarded to the requested node 2.

The merit of this approach is that it allows a set of nodes holding shares to refresh all shares by generating a new set of shares for the same secret key from the old shares without reconstructing the secret key.

3.3 Packet Transmission

Let S and D be the source and destination node respectively.
Let N_i be the intermediate nodes where i = {1, 2,…. N}
Let DP represent the data packet and it includes packet identifier PI, the IP address of the destination node (IP_D), a certificate K_n, and expiration time t.

We assume TC_i to be the initial trust counter for all the nodes with a minimum threshold value (TC_{th}).

1) On request, S starts transmitting DP towards the destination via intermediate nodes in hop by hop manner.
It will be in the following form.

$$S \rightarrow \text{Transmit: } [PI, IP_D, k_S, t] K_{Pr}$$

The TC_i for all the nodes is estimated periodically for every trust evaluation interval (TEI)

2) When N_1 receives DP, it uses S's public key extracted from the S's certificate to authenticate the signature and to validate that S's certificate has not expired. Else, the node proceeds by signing the contents of the messages, appends its own certificate, and sends the message to its next hop. Alterations of data or integrity attacks are prevented by signature.
The DP from N_i is transmitted in the following format.

$$N_1 \rightarrow \text{Transmit: } [[DP, IP_D, k_S, t] K_{Pr}] K_{pr\,(N1)}, k_{N1}$$

3) Upon receiving the DP, N_1's neighbor N_2 validates the signature with the given certificate N_2, and then removes N_1's certificate & signature, records N_1 as its predecessor, signs the content of the message originally sent by S, appends its own certificate and forward the message. N_2 then re-transmits the DP.

$$N_2 \rightarrow \text{Transmit: } [[DP, IPD, k_S, t] K_{Pr}] Kpr_{(N2)}, kN_2.$$

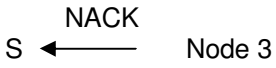
4) Each node along the path repeats these steps of validating the previous node's signature, removing the previous node's certificate and signature, recording the previous node's IP address, signing the original contents of the message, appending its own certificate and forwards the message till DP reaches the destination.
5) All the member nodes send their TC_i value to its cluster head CH. If the CH detects any node with TC_i less than TC_{th}, then the CH adds the corresponding N_i in its local CRL (Certificate Revocation List).
6) When CH receives a renewal request from its cluster member N_i, it verifies whether N_i is in CRL. If it exists, its request is rejected. Otherwise, it sends a certificate renewal reply to Ni with its signature.

3.4 Detecting the Misbehaving Nodes

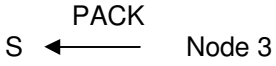
Let N_k is the intermediate node with k=3, 6, 9, …
Let NACK and PACK be the negative and positive acknowledgment respectively.
Let FC be the forward count
Let FC_{Th} represent pre-defined threshold value of FC.

1) S starts forwarding the packet upon request.
2) FC gets incremented during the packet entry and gets decremented during the packet exit.
3) When DP reaches N_k, Fc is verified.
4) When FC is below the FC_{Th}, N_k informs S with NACK. If not, S is informed with PACK.
S transfers the data packet on request. When DP reaches node 3, FC is verified.

If $FC < FC_{Th}$, then



If $FC > FC_{Th}$, then



Similarly, the above process continues for every 3 hops till the packet reaches D.
5) If S receives PACK Then
The route is considered as normal
Else
6) If S receives the NACK, then the following events are carried out

Event 1
The source node counts the NACK sent by every k-hop neighbors,
Event 2
If $NACK_c > NACK_{cmax}$, then the node is considered as misbehaving and this information is broadcasted to all other nodes in the route.
Event 3
From the broadcast information, the destination node checks the number of misbehaving nodes along the route and this information is sent as a feedback to the source node.
Event 4
If the source node finds that only limited number of misbehaving nodes (say 2) in the route, then that particular nodes are marked as rejected and bypass route is established excluding those nodes.
Event 5
When the number of misbehaving nodes exceeds the minimum count, then the entire route is treated as misbehaving and an alternate route is established for further transmission, by the source.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

We use Network Simulator (NS2) [16] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 2.

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
Misbehaving Nodes along the route	1,2,3,4

TABLE 2: Simulation Settings

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Control overhead: The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.
Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.
Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.
Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

4.3 Results

Case 1

In our first experiment, we have taken a scenario for a given source and destination pair (25, 89). We gradually increase the number of misbehaving nodes along the established path for this pair. When the number of misbehaving nodes are more than 2, (minimum count), our proposed CBMDA scheme determines alternate path and reroutes the entire traffic through that path.

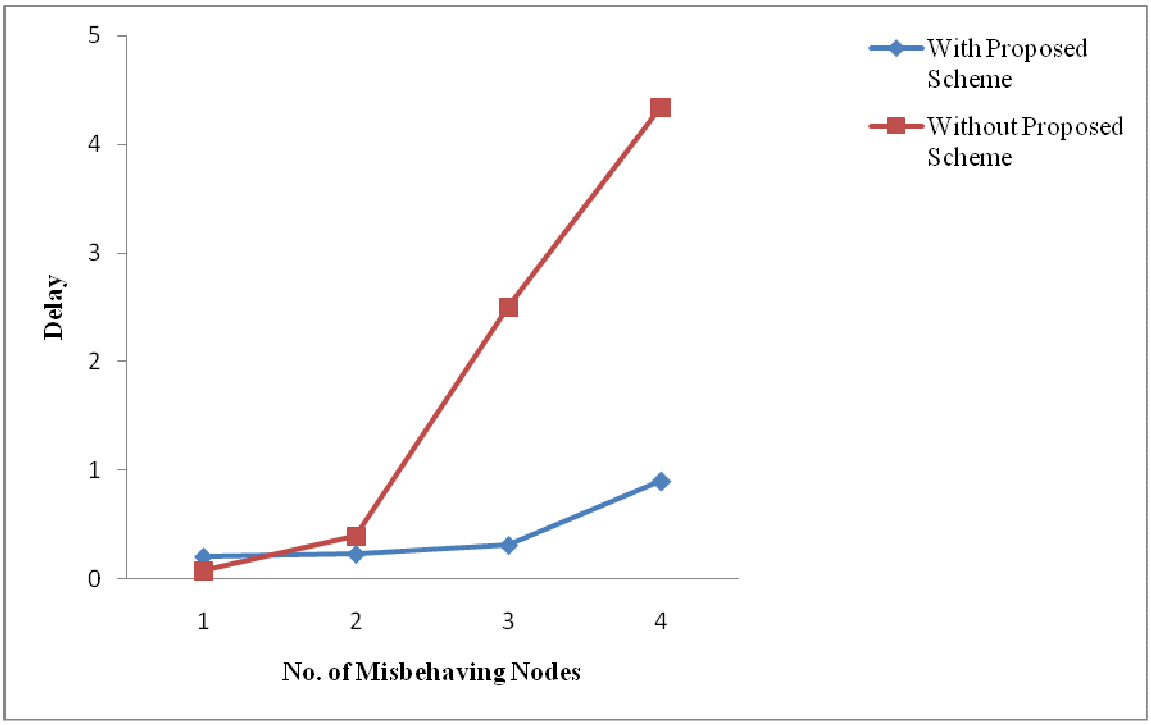


FIGURE 2: Misbehaving Nodes Vs Delay

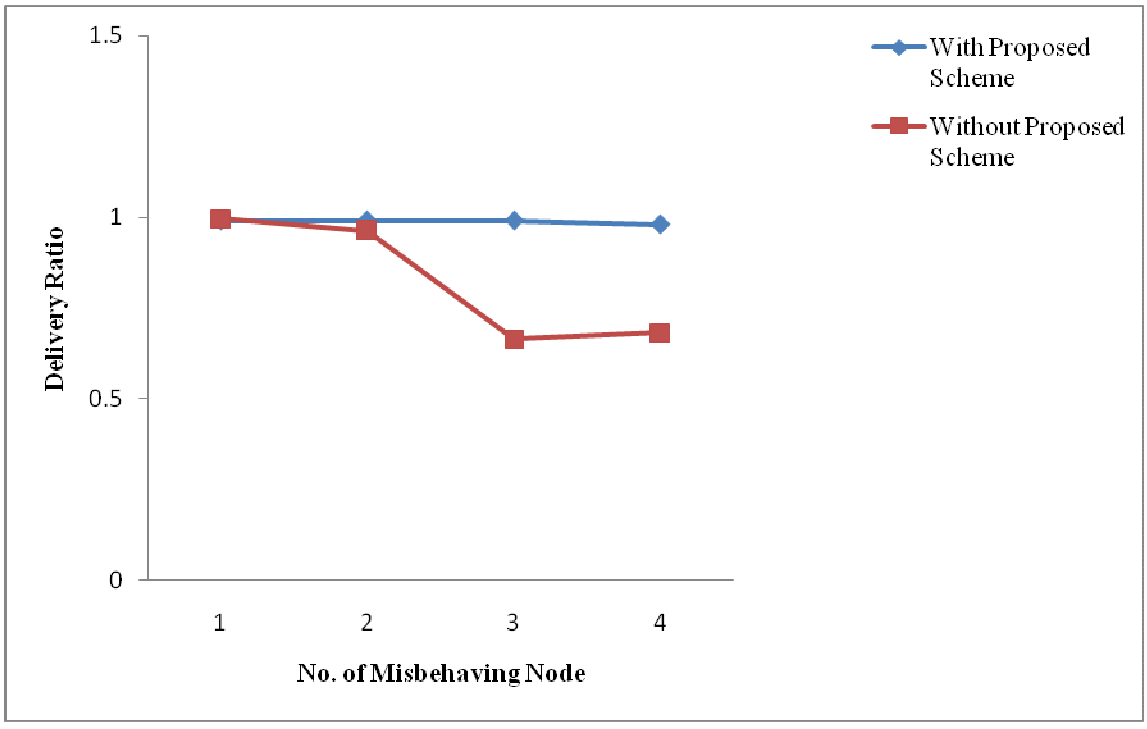


FIGURE 3: Misbehaving Nodes Vs Delivery Ratio

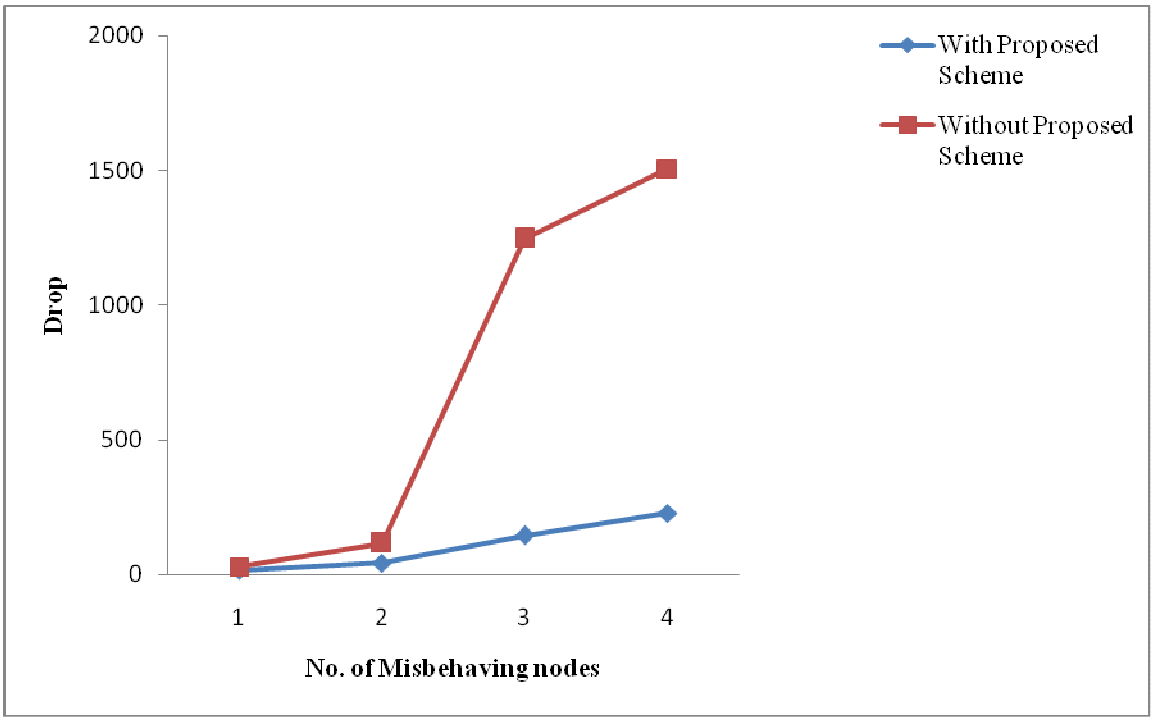


FIGURE 4: Misbehaving Nodes Vs Drop

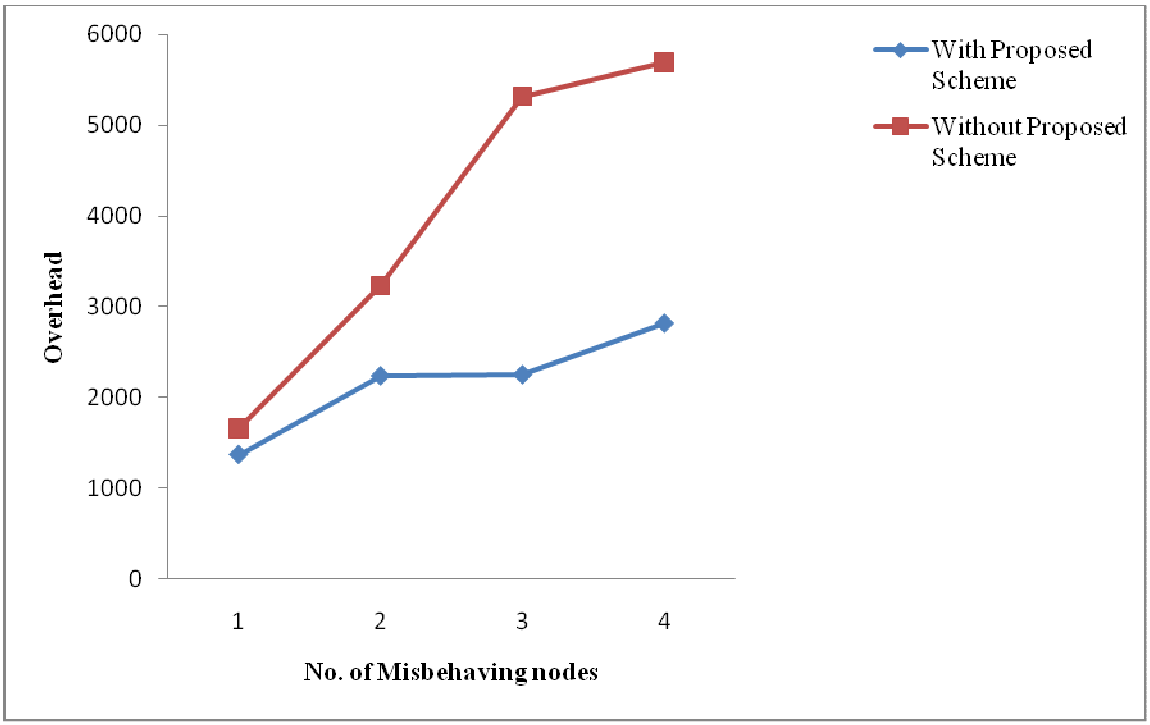


FIGURE 5: Misbehaving Nodes Vs Overhead

Figure 2 shows the results of average end-to-end delay for the increasing misbehaving nodes for both the schemes. We can see that the proposed scheme (CBMDA) has significantly lower delay compared to without proposed scheme since it exchanges less number of acknowledgment

packets. Hence for the same reason, the control overhead involved is also less in the proposed CBMDA scheme, when compared to without proposed scheme as in Figure 5.

When the number of misbehaving nodes is more than two, the packet delivery ratio begins to reduce in case of without proposed scheme, since CBMDA continues the transmission using alternate route, the delivery ratio is unaffected. From Figure 3, we can see that clearly the CBMDA scheme outperforms the without scheme by achieving more delivery ratio. For the same reason, the packet drop is less in CBMDA as shown in figure 4.

Case 2

In our second experiment, we have taken another scenario for a given source and destination pair (13, 99). We gradually increase the number of misbehaving nodes along the established path for this pair.

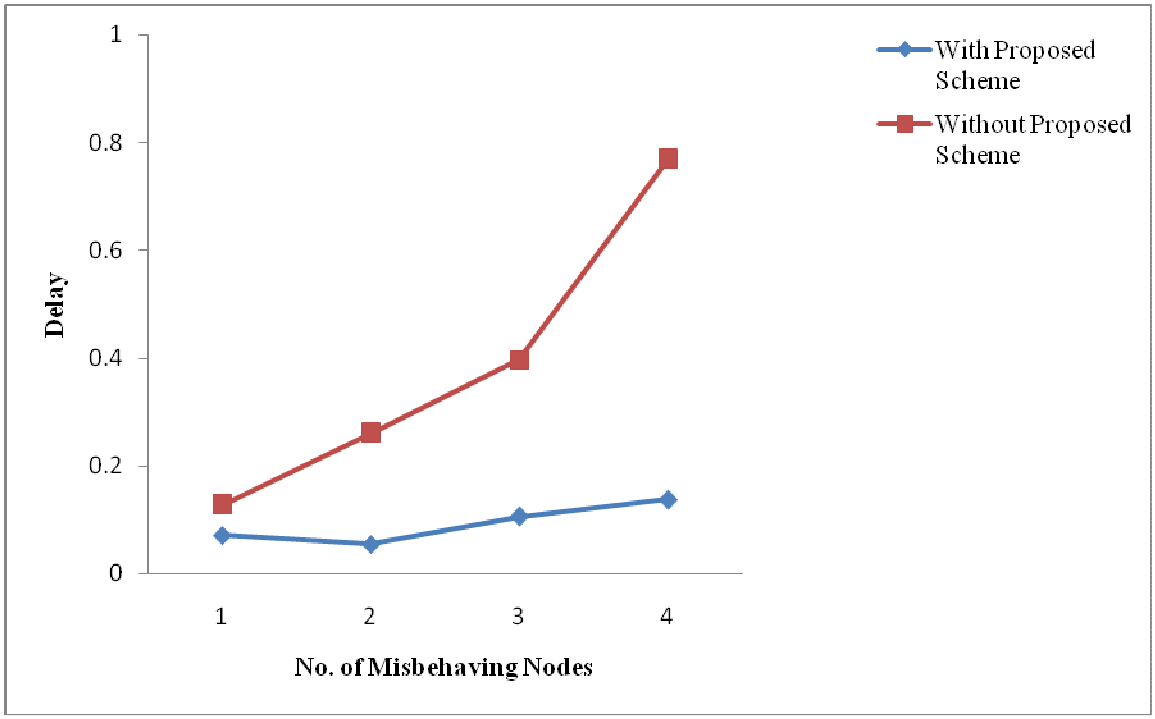


FIGURE 6: Misbehaving Nodes Vs Delay

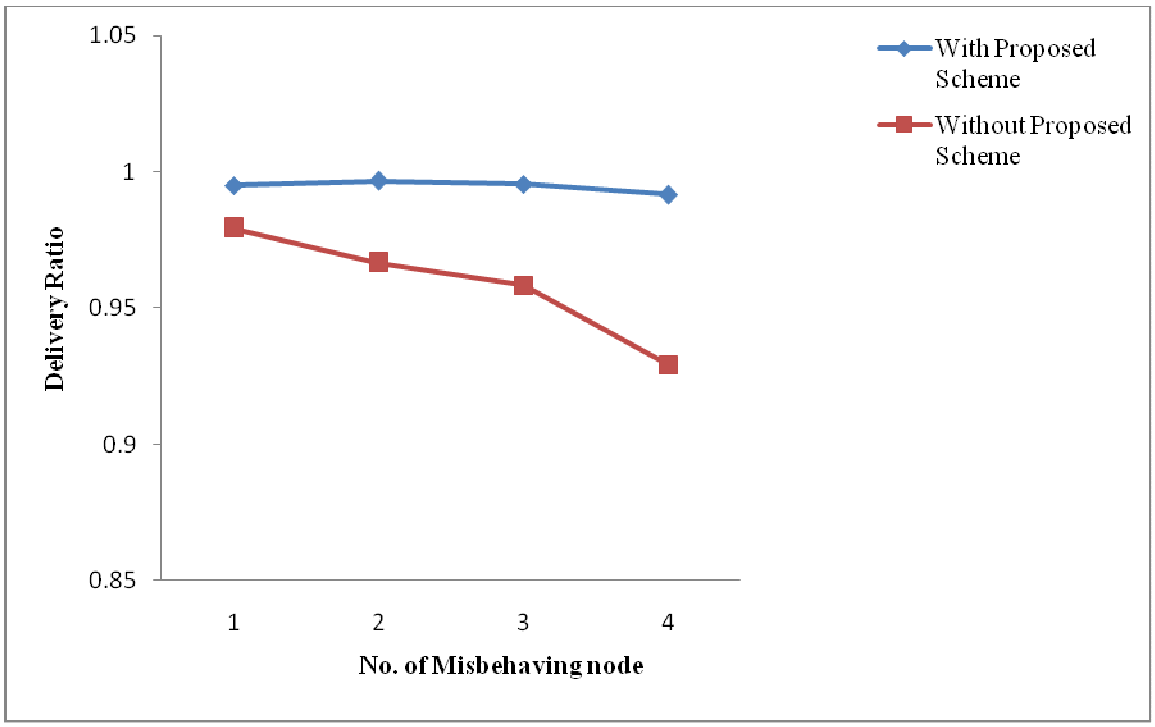


FIGURE 7: Misbehaving Nodes Vs Delivery Ratio

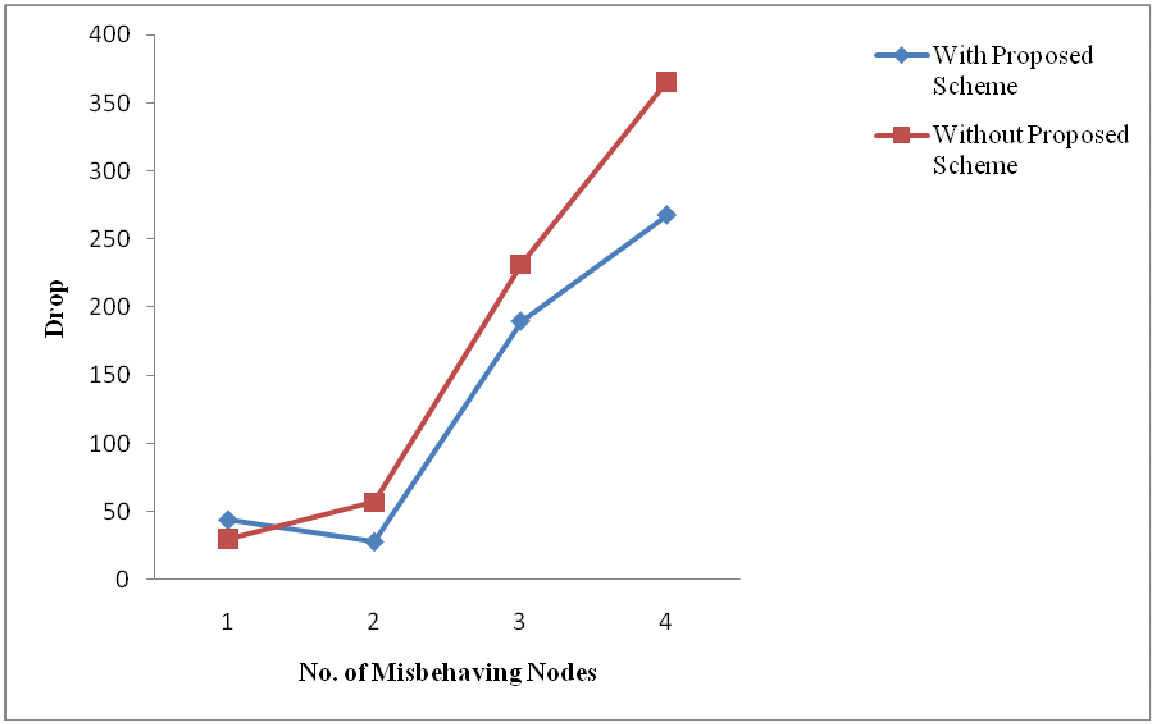


FIGURE 8: Misbehaving Nodes Vs Delivery Ratio

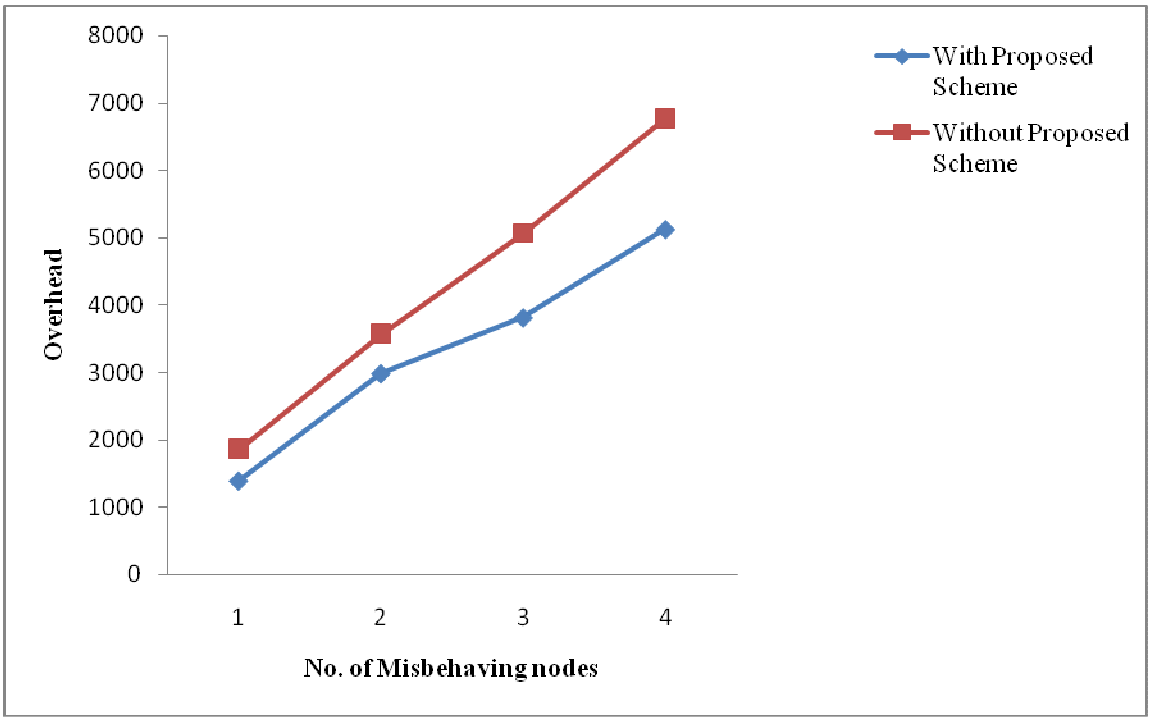


FIGURE 9: Misbehaving Nodes Vs Drop

As we can see from the figures 6, 7, 8, and 9, the results are similar to our previous experiment. (ie) CBMDA has more delivery ratio with reduced delay, drop and overhead when compared to without proposed scheme.

5. CONCLUSION

In this paper, we have developed a threshold cryptography coupled acknowledgement scheme for misbehaving node detection in MANET. Initially clusters are formed in the network and cluster member with the least id is chosen as the cluster heads (CH). The Threshold cryptography is deployed along with proactive sharing scheme that permits the cluster members to refresh all shares by generating a new set of shares for a same secret key from the old shares without reconstructing the secret key. During data transmission, when any node requests a certificate from CH, the cryptographic approach offers the certificate to the requested node. The certificate of a node is renewed or rejected by CH, based on its trust counter value. Apart from the authentication technique, an acknowledgement scheme is also used to detect and isolate the misbehaving nodes by checking the number of forwarded packets. By simulation results, we show that the proposed approach reduces the overhead.

REFERENCES

1. Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine, “An Ontological Approach to Secure MANET Management”, In Proceedings of the 2008 Third *International Conference on Availability, Reliability and Security*, pp 787-794 , 2008.

2. Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain, “Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol”, *European Journal of Scientific Research*, Vol. 32, No. 4, 2009, pp. 444-454.

3. M. Uma and G. Padmavathi, “A comparative Study and Performance Evaluation of Reactive Quality of Service Routing Protocols in Mobile Ad Hoc Networks”, *Journal of Theoretical and Applied Information Technology*, Vol. 6, No. 2, 2009, pp. 223-229.

4. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, *Wireless/Mobile Network Security,* Y. Xiao, X. Shen, and D.-Z. Du (Eds.), Springer, 2006.

5. Yu Huang, Beihong Jin, Jiannong Cao, Guangzhong Sun and Yulin Feng, “A Selective Push Algorithm for Cooperative Cache Consistency Maintenance over MANETs”, *EUC*, 2007, pp. 650-660.

6. Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, “Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes”, *World Academy of Science, Engineering and Technology* ,2008.

7. Aishwarya Sagar Anand Ukey, Meenu Chawla, “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”, *International Journal of Computer Science Issues*, Vol. 7, No 1, 2010, pp. 12-17.

8. Sheng-Ti Li, Xiong Wang, “Enhanced Security Design for Threshold Cryptography in Ad Hoc Network”, International conference on *Next Generation Tele-Traffic And Wired/Wireless Advanced Networking* (NEW2AN), 2004.

9. Hitoshi Asaeda, Musfiq Rahman, and Yoshihiro Toyama, “Structuring Proactive Secret Sharing in Mobile Ad-hoc Networks", Proc. *IEEE ISWPC*, January 2006.

10. GSR Emil Selvan, Dr. M. Suganthi, P Jeni, KA Krishna Priya, “Detection of Compromised Nodes in Mobile Ad-Hoc Networks”, *Journal of Computational Information Systems*, pp 1823-1829, 2011.

11. S.M. Sarwarul Islam Rizvi, Zinat Sultana, Bo Sun, Md. Washiqul Islam, “Security of Mobile Agent in Ad hoc Network using Threshold Cryptography”, *World Academy of Science, Engineering and Technology*, 2010.

12. Sanjay Raghani, Durga Toshniwal, R. C. Joshi, “Distributed Certification Authority for Mobile Ad Hoc Networks – A Dynamic Approach”, *Journal of Convergence Information Technology*, Volume 2, Number 2, June 2007.

13. Keun-Ho Lee, Sang-Bum Han, Heyi-Sook Suh, “Authentication Protocol Using Threshold Certification in Hierarchical-cluster-based Ad Hoc Networks”, *Journal of information science and engineering*, pp 539-567, 2007.

14. R. Murugan, A. Shanmugam, “A Cluster Based Authentication Technique for Mitigation of Internal Attacks in MANET", *European Journal of Scientific Research*, Volume 51, Issue 3.

15. R. Murugan, A. Shanmugam, “A Timer Based Acknowledgement Scheme for Misbehavior Detection and Isolation in MANET”, *International Journal of Network Security* [accepted for publication]

16. Network Simulator, http://www.isi.edu/nsnam/ns

INSTRUCTIONS TO CONTRIBUTORS

The *International Journal of Computer Science and Security (IJCSS)* is a refereed online journal which is a forum for publication of current research in computer science and computer security technologies. It considers any material dealing primarily with the technological aspects of computer science and computer security. The journal is targeted to be read by academics, scholars, advanced students, practitioners, and those seeking an update on current experience and future prospects in relation to all aspects computer science in general but specific to computer security themes. Subjects covered include: access control, computer security, cryptography, communications and data security, databases, electronic commerce, multimedia, bioinformatics, signal processing and image processing etc.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCSS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 6, 2012, IJCSS appears in more focused issues. Besides normal publications, IJCSS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCSS LIST OF TOPICS

The realm of International Journal of Computer Science and Security (IJCSS) extends, but not limited, to the following:

- Authentication and authorization models
- Computer Engineering
- Computer Networks
- Cryptography
- Databases
- Image processing
- Operating systems
- Programming languages
- Signal processing
- Theory
- Communications and data security
- Bioinformatics
- Computer graphics
- Computer security
- Data mining
- Electronic commerce
- Object Orientation
- Parallel and distributed processing
- Robotics
- Software engineering

CALL FOR PAPERS

Volume: 6 - **Issue:** 5 – October 2012

i. Paper Submission: July 31, 2012 **ii. Author Notification:** September 15, 2012

iii. Issue Publication: October 2012

CONTACT INFORMATION

Computer Science Journals Sdn BhD
B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2012
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org