THE REPUBLIC OF TURKEY
BAHÇEŞEHİR UNIVERSITY

SMART GRID DATA COLLECTION WITH VEHICULAR AD-HOC NETWORKS USING PUBLIC TRANSPORTATION BUSES

Ph.D. Thesis

BİLAL ERMAN BİLGİN

İSTANBUL, 2019

THE REPUBLIC OF TURKEY
BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

SMART GRID DATA COLLECTION WITH VEHICULAR AD-HOC NETWORKS USING PUBLIC TRANSPORTATION BUSES

Ph.D. Thesis

BİLAL ERMAN BİLGİN

Supervisor: ASSIST. PROF. DR. SELÇUK BAKTIR

İSTANBUL, 2019

THE REPUBLIC OF TURKEY
BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
COMPUTER ENGINEERING

Title of the Ph.D. Thesis	:	Smart Grid Data Collection With Vehicular Ad-Hoc Networks Using Public Transportation Buses
Name/Last Name of the Student	:	Bilal Erman BİLGİN
Date of Thesis Defense	:	01 August, 2019

The thesis has been approved by Graduate School of Natural and Applied Sciences.

Assist. Prof. Dr. Yücel Batu SALMAN
Graduate School Director

I certify that this thesis meets all the requirements as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Assist. Prof. Dr. Tarkan AYDIN
Program Coordinator

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Doctor of Philosophy in Computer Engineering.

Examining Commitee Members	Signature
Thesis Supervisor Assist. Prof. Dr. Selçuk BAKTIR	.....
Member Assist. Prof. Dr. Tarkan AYDIN	.....
Member Assist. Prof. Dr. Ahmet Onur DURAHİM	.....
Member Assist. Prof. Dr. Pınar SARISARAY BÖLÜK	.....
Member Assist. Prof. Dr. Mustafa Zahid GÜRBÜZ	.....

ACKNOWLEDGEMENTS

First of all I would like to thank Assist. Prof. Dr. Selçuk BAKTIR, who has given me the opportunity to work on this thesis. I am very grateful for his continuous support to my Ph.D study, insight, and invaluable help during the preparation for this thesis.

Moreover, I would like to thank my thesis defense committee, Assist. Prof. Dr. Tarkan AYDIN, Assist. Prof. Dr. Ahmet Onur DURAHİM, Assist. Prof. Dr. Pınar SARISARAY BÖLÜK and Assist. Prof. Dr. Mustafa Zahid GÜRBÜZ for their feedbacks and constructive comments to increase the quality of this study.

I also would like to thank my dear teachers who encouraged me in my Ph. D program.

I would like to thank my company, BELBIM, and my colleagues.

I cannot forget friends who went through hard times together, cheered me on, and celebrated each accomplishment. Thank you very much to all my friend.

Last but not least I wish to express my love and gratitude to all my parents, Semra and Aydın and my brother, Emir. I would particularly like to thank my parents and my brother for their unlimited support in every stage of my life. I would like to thank my precious wife Büşra for her endless love, patience, sacrifices, and understandings. I also would like to thank my son B. Eymen who became a member of our family at the last year of my Ph.D study. My family is my chance.

İstanbul, 2019 Bilal Erman BİLGİN

ABSTRACT

SMART GRID DATA COLLECTION WITH VEHICULAR AD-HOC NETWORKS USING PUBLIC TRANSPORTATION BUSES

Bilal Erman BİLGİN

Computer Engineering
Supervisor: Assist. Prof. Dr. Selçuk BAKTIR

August 2019, 89 Pages

Recent improvements in wireless communication technology, the popularity of Wireless Sensor Networks has increased. Agriculture, air pollution monitoring, animal tracking, chemical leakage detection in rivers, earthquake early detection, environmental monitoring, forest fire detection, gas monitoring, healthcare applications, roadside and transportation applications, smart parking, smart roads, and surveillance are possible applications of Wireless Sensor Networks. Moreover, smart grids and vehicular networks are two important application environments for wireless sensor networks with several potential applications in these environments.

Firstly, this thesis focuses on a novel solution for collecting smart meter data by merging vehicular ad-hoc networks and smart grid communication technologies. We apply vehicular ad-hoc networks to collect data from smart meters to eliminate the need for manpower. In this thesis, the use of IEEE 802.11p protocol has been proposed for the first time for use in smart grid applications. In our scheme, data flows first from smart meters to a bus through infrastructure-to-vehicle communication and then from the bus to a bus stop through vehicle-to-infrastructure (V2I) communication. Secondly, a secure routing protocol is proposed to detect and eliminate blackhole nodes in the network. Besides, the proposed solution secures the transmitted data. Finally, a data collection mechanism, with added security features, is proposed for collecting data from smart meters using public transportation buses.

The performance of proposed mechanisms has been investigated in detail in the matter of average end-to-end delay and delivery ratio. According to the performance evaluations, the proposed mechanisms perform desired delivery ratios without increasing extra communication delay.

Keywords: Wireless Sensor Networks, Smart Grid, Vehicular Ad-Hoc Networks, Routing Protocols, Blackhole Node Attack

ÖZET

ARAÇLAR ARASI AĞLARLA TOPLU TAŞIMA ARAÇLARINI KULLANARAK AKILLI ŞEBEKE VERİLERİNİ TOPLAMA

Bilal Erman BİLGİN

Bilgisayar Mühendisliği
Tez Danışmanı: Dr. Öğr. Üyesi Selçuk BAKTIR

Ağustos 2019, 89 Sayfa

Kablosuz iletişimde son ilerlemeler kablosuz algılayıcı ağların popülaritesi artmıştır. Tarım, hava kirliliği izleme, hayvan takibi, nehirlerdeki kimyasal sızıntı tespiti, erken deprem tespiti, çevresel izleme, orman yangını algılama, gaz izleme, sağlık uygulamaları, yol kenarı ve ulaşım uygulamaları, akıllı otopark, akıllı yollar ve gözetim uygulamaları kablosuz algılayıcı ağların olası uygulamalarıdır. Dahası, akıllı şebekeler ve araçsal ağlar birkaç potansiyel uygulamayla kablosuz algılayıcı ağlar ıçın iki önemli uygulama ortamıdır.

İlk olarak, bu tez araçsal arası ağlar ile akıllı şebekeler iletişim teknolojisini birleştirerek akıllı sayaç bilgilerini toplamak için yeni bir çözüme odaklanır. Akıllı sayaç bilgilerini toplamada insan gücünü saf dışı bırakmak için araçsal arası ağları kullandık. Bu çalışmada, akıllı şebeke uygulamalarında ilk kez IEEE 802.11p protokolü kullanılması önerilmiştir. Şemada, veri ilk olarak altyapıdan araca vasıtasıyla akıllı sayaçlardan otobüslere ve sonra araçtan altyapıya vasıtasıyla otobüsten otobüs durağına ulaşır. İkinci olarak, ağdaki zararlı düğümleri yakalamak ve elemek için bir güvenilir rota protokolü önerilmiştir. Ayrıca, önerilen çözüm iletilen veriyi de güvenceye alır. Son olarak, akıllı sayaçlardan bilgileri toplamak için toplu taşıma otobüsleri kullanarak güvenlik özellikleri eklenmiş bir veri toplama mekanizması önerilmiştir.

Önerilen mekanizmaların performansları ortalama uçtan uca gecikme ve aktarılma oranı açısından incelenmiştir. Performans değerlendirmelerine göre, önerilen mekanizmalar istenilen aktarılma oranlarına iletişim gecikmesini arttırmadan elde etmiştir.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Akıllı Şebekeler, Araçsal Arası Ağlar, Rota Protokolleri, Karadelik Düğüm Saldırıları

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

AODV	:	Ad-hoc On-Demand Distance Vector
AES	:	Advanced Encryption Standard
AMR	:	Automatic Meter Reading
BN	:	Base Node
BSN	:	Body Sensor Networks
CA	:	Certificate Authority
CRL	:	Certificate Revocation List
CBR	:	Constant Bit Rate
DAU	:	Data Aggregator Unit
DSRC	:	Dedicated Short Range Communication
DOS	:	Denial-of-Service
DSR	:	Dynamic Source Routing
GSM	:	Global System for Mobile Communications
I2I	:	Infrastructure-to-Infrastructure
I2V	:	Infrastructure-to-Vehicle
ITS	:	Intelligent Transportation Systems
IDS	:	Intrusion Detection System
MDMS	:	Meter Data Management System
MEMS	:	Micro Electro Mechanical Systems
MANET	:	Mobile Ad-Hoc Networks
NAN	:	Neighborhood Area Network
NS-2	:	Network Simulator-2
PLC	:	Power Line Communication
RF	:	Radio Frequency
RSU	:	Road Side Unit
RREP	:	Route Reply
RREQ	:	Route Request

SAODV	:	Secure AODV
VSC	:	Vehicle Safety Communications
V2I	:	Vehicle-to-Infrastructure
V2V	:	Vehicle-to-Vehicle
VANET	:	Vehicular Ad-Hoc Networks
WAVE	:	Wireless Access in Vehicular Environments
WAMR	:	Wireless Automatic Meter Reading
WBAN	:	Wireless Body Area Networks
WSNs	:	Wireless Sensor Networks

SYMBOLS

Amount of randomness	:	r
Horizontal distances between the fixed reference points for consecutive nodes	:	h
Noise power	:	P
Path loss exponent	:	η
Signal to noise ratio	:	$\gamma(d)_{dB}$
Standard deviation	:	σ
Transmit power	:	P_t
Vertical distances between the fixed reference points for consecutive nodes	:	v
Zero-mean Gaussian random variable	:	X_σ

1. INTRODUCTION

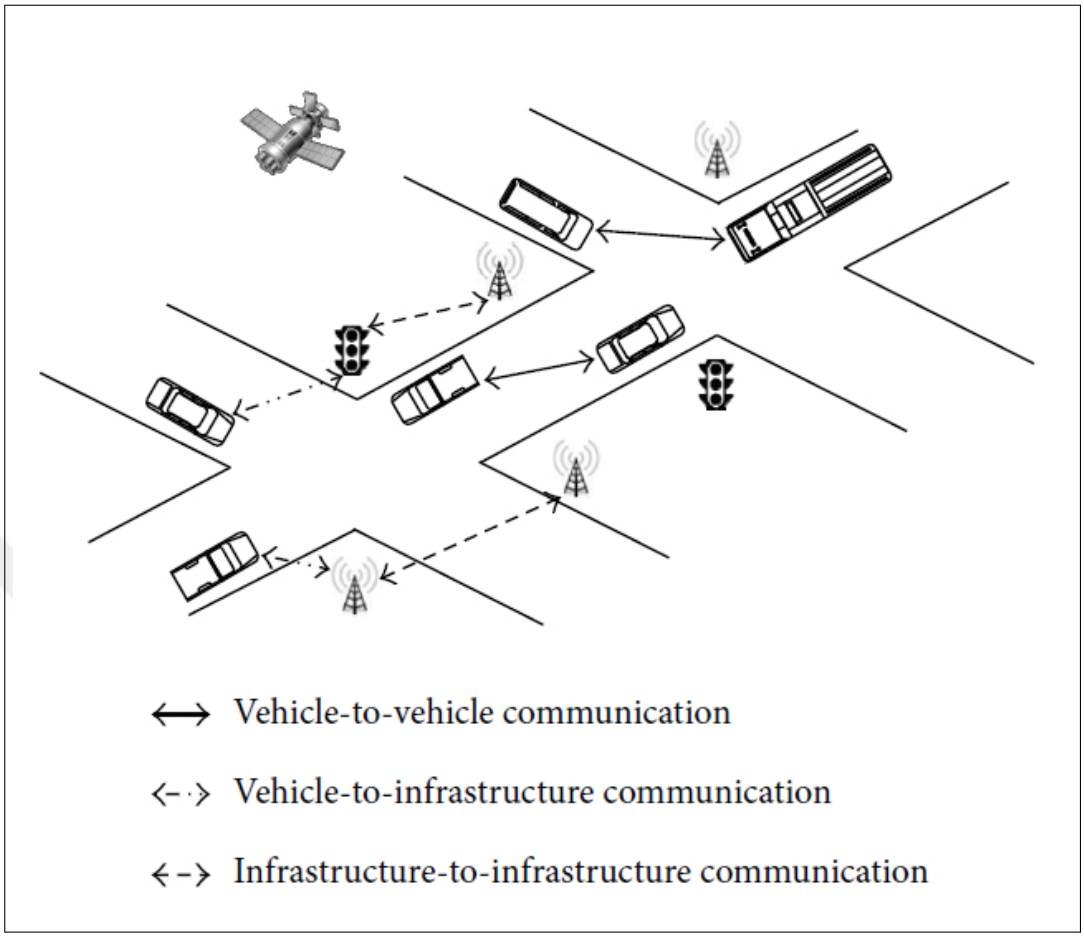
With the improvements in wireless communication and Micro-Electro-Mechanical Systems (MEMS), the usage of Wireless Sensor Networks (WSNs) have started in many areas. In a WSN, there are lots of sensor nodes. These sensors are cheap, small and have limited resources.Furthermore, studying in wireless sensors has been started an hot topic in academy collaborative and low-cost nature of WSNs. The main and possible applications of WSNs are agriculture, air pollution monitoring, animal tracking, chemical leakage detection in rivers, earthquake early detection, environmental monitoring, forest fire detection, gas monitoring, healthcare applications, roadside and transportation applications, smart grids, smart parking, smart roads, surveillance and vehicular ad-hoc networks (VANETs).

1.1 VEHICULAR AD-HOC NETWORKS

Vehicle-to-Vehicle (V2V) communication has recently become a hot topic in both academy and automotive industries (Gerla & Kleinrock 2011, Molisch et al. 2009, Santa et al. 2008). The communication between vehicles helps to improve road safety. In these networks, vehicles act like sensors and transmit the warning messages to other vehicles in communication range or receive the messages from other vehicles. Drivers can easily detect any abnormal or potentially dangerous situations, such as traffic accidents and traffic jam, by receiving telematics information, including location and speed information (Bilgin & Gungor 2013).

The illustration of V2V communication is shown in Figure 1.1. Generally, V2V has three types of communications (Zeadally et al. 2010). The first one is communication between vehicles (V2V), in which vehicles can give some meaningful information about road including, accident or collision information, and so forth. The second one is communication between vehicles and infrastructures (V2I), in which, road side units (RSU) can

Figure 1.1: Illustration of vehicular communications



transmit commercial advertisements, vehicles can pay toll or parking payments, and so forth. The third one is communication between infrastructures (I2I), in which the RSUs can exchange important information with each other that is come from the vehicles.

The existing applications of VANET are weather-related information alerts, blind spot warning, do-not-pass warning at intersections, emergency vehicle warning, forward collision/accident warning, road safety applications and lane change warning (Bilgin & Gungor 2013, Pereira et al. 2012, Hartenstein & Laberteaux 2008).

The communication protocols that are used in vehicular communication are dedicated short range communication (DSRC) and IEEE 1609 (Gerla & Kleinrock 2011, Härri et al. 2006, Zeadally et al. 2010). DSRC is used for short range communication in V2V and V2R applications. The main characteristic of DSRC are high data transfers and low com-

Table 1.1: Regional differences in DSRC

Features	Japan	Europe	USA
Radio band	80MHz	20MHz	75MHz
Data rate	1–4Mbps	250 Kbps	3–27Mbps
Communication range	30m	15–20m	1000m (max)
Radio frequency	5.8GHz	5.8GHz	5.9GHz

munication delay. DSRC has 7 channels, and they have been allocated in this order: first channel is used for safety communications, second channel is used for critical safety communications, third channel is used for high power public safety communications, and the rest of the channels are for either safety or non-safety communications. The standards of DSRC are different in Japan, Europe, and USA. In each of the three regions DSRC has different features. For example, the communication range is 30 meters in Japan, 15–20 meters in Europe, and 1000 meters (max) in USA. The data rate is 1–4 Mbps in Japan, 250 Kbps in Europe, and 3–27 Mbps in USA. The comparison of regional differences in DSRC has been summarized in Table 1.1.

In V2V, IEEE 802.11b protocol may be used for communication. However, there are some challenges, including high mobility, traffic patterns, and vehicle speed. These challenges affect the communication, that is, establishing communication between vehicles that approach from opposite direction. To address these challenges, IEEE 1609 standards for Wireless Access in Vehicular Environments (WAVE) have introduced. The main features of IEEE 1609 is multichannel operation protocols, resource manager protocols, security services protocols, networking protocols. By applying some modification on data link and physical layers on IEEE 802.11b, IEEE 802.11p has been introduced. By using IEEE 802.11p communication between high speed vehicles is enabled. WAVE protocol works on the rest of the OSI layers. The physical layer values of the IEEE 802.11b and IEEE 802.11p have been summarized in Table 1.2 (Bilgin & Gungor 2013).

Table 1.2: PHY layer values of IEEE 802.11b and IEEE 802.11p

Channel bandwidth	20MHz	10MHz
Data rates	1 to 11Mbps	3 to 27Mbps
Slot time	20 μs	16 μs
SIFS time	10 μs	32 μs
Preamble length	96 μs (short), 192 μs (long)	32 μs
Air propagation time	$<$2 μs	$<$4 μs
CWmin	31	15
CWmax	1023	1023

1.2 SMART GRID

Today's electric infrastructure was planned more than 50 years ago (Wang et al. 2011, Bilgin & Gungor 2012a).The reliability and efficiency of energy needs to be improved to increase the performance of existing electric power systems (Bilgin & Gungor 2012b). According to U.S. Department of Energy report the usage and demand for electricity is continuously increasing by 2.5 percent annually (Bilgin & Gungor 2011). Power outage, voltage problems, decreasing in the power quality and reliability are some of the problems which are caused by increasing in energy consumption. Besides, there is no automation, monitoring and pervasive and effective communications in the existing power grid systems (Bilgin & Gungor 2012a). Smart grid which is the new concept of existing power grids is introduced to address these problems (Bose 2010, Farhangi 2010, Gungor et al. 2010, Heile 2010, Javadi & Javadi 2010, Lightner & Widergren 2010, Gungor & Hancke 2009, U.S. Department of Energy 2008, Len et al. 2007, Gungor & Lambert 2006, Amin & Wollenberg 2005, U.S. Department of Energy 2002). The smart grid tries to improve efficiency, reliability, safety of the power grid by adding communication, control and monitoring capabilities to the existing power grid systems (Bilgin & Gungor 2011, Bumiller et al. 2010, Molderink et al. 2010).

The main smart electric power grid applications are automatic metering systems, demand response, distribution automation, electricity fraud detection, fault diagnostics, load control, outage detection, remote monitoring and underground cable system monitoring, (Bil-

gin & Gungor 2012b, Bilgin & Gungor 2011, Lightner & Widergren 2010, Gungor & Hancke 2009, Ipakchi & Albuyeh 2009, Len et al. 2007, Amin & Wollenberg 2005).

Using Advanced Metering Infrastructure (AMI) systems in Automatic Metering System (AMR) for smart grid, between customers and utility companies a two-way communication will be established. The use of AMI systems decreases the operational costs of utilities by allowing them to automatically read meters and get electricity consumption data remotely. Furthermore, it allows customers to be informed about how much power they are using by giving real-time consumption information (Gungor et al. 2013, Yan et al. 2013).

1.3 PROBLEM STATEMENT

The main problem of the existing traditional electric meters is there is no two-way communication between utility companies and customers. With the smart grid, there are many studies on AMR systems. With wireless technology, some wireless AMR (WAMR) projects have been offered. With two way communication capability in WAMR systems, utility companies can get timely electricity consumption data from their customers. This helps detect and prevent illegal electricity usage. Besides, meter reading expenses of utility companies reduces.

However, all the proposed studies made important amendments on existing AMR systems or proposed alternative mechanisms for collecting data from meters, they have some drawbacks. Many of them require subscription to GSM or telephone line service, and some require installations and cable costs. Furthermore, the existing solutions based on IEEE 802.15.4 protocol will not be a solution for long ranges.

In addition to this problem, security and attacks are another problems for WSNs. There are different types of attacks that can be applied at each protocol stack layer in WSNs. The attacks at network layer are very common. These attacks cause decrease in packet

delivery ratio, data integrity problems, data loss or obtaining sensitive information. There are different solutions for these network attacks in the literature. But most of them have some disadvantages such as single point of failure, vulnerability to hacking, high end-to-end delay.

This thesis proposes to investigate several options to address these problems. In this thesis, a new data collection mechanism from smart meter based on vehicular networks is proposed. The proposed data collecting mechanism uses public transportation buses, which has never been used for this purpose before. The data collected by a bus is transmitted to a bus stop. Thus, in our scheme, we combine the vehicular communication technology and the smart grid technology together. Also, this thesis proposes a light-weight solution for network layer attacks, especially for blackhole attacks. We propose improvements on the Ad-Hoc On-Demand Distance Vector (AODV) routing protocol to overcome some security problems and blackhole attacks. Besides, the importance of having reliable and secure end-to-end communication is emphasized for utility companies to prevent billing frauds and other attacks. Therefore, we apply the blackhole attack solution to our data collection mechanism to overcome some security problems and make the communication more reliable and secure.

1.4 MOTIVATION

The first motivation of this thesis is proposing a novel data collection mechanism. This proposed data collection mechanism is introduced at Chapter 3 and 4. In the proposed scheme, smart grid and VANET technologies are combined using public transportation buses. The second motivation of this thesis is proposing a solution to network attacks, especially for blackhole attacks in WSNs. The proposed solution is light-weight. Therefore, it increases the packet delivery ratio without causing extra communication delay. This proposed solution is introduced at Chapter 5. The third motivation of this thesis is proposing a secure data collection mechanism from smart meters by applying the study in Chapter 5 to the study in Chapter 4. The proposed mechanism achieves desirable packet

delivery ratio without increasing end-to-end delay significantly. This proposed solution is introduced at Chapter 6.

1.5 CONTRIBUTIONS

This thesis focuses on a new data collection mechanism from smart meter based on vehicular networks. Also having a reliable and secure end-to-end communication between customers and utility companies is another important issue.

The main contributions of this thesis is listed as below:

i This is the first study to the best of our knowledge that uses public transportation buses to collect smart meter data in the literature.

ii The proposed mechanism only needs smart meters with IEEE 802.11p communication capability. This communication protocol may extend the communication range of smart meters up to 1000. This communication protocol will also be used for the first time in the literature.

iii In the proposed mechanism, both V2I and I2V communication is utilised.

iv Since there are two way communication between customers and utility companies, the proposed mechanism not only get smart meter data from customers but also will transmit an alert message to its customers such as a message containing a reconfiguration file.

v By signing the routing packets in the AODV, routing information in sent packets are protected. This facilitates establishing secure routes between nodes.

vi The use of signatures in the routing packets facilitates identification of blackhole nodes in the network. Furthermore, it helps to discard the fraudulent messages coming from malicious nodes.

vii The proposed security mechanism is light-weight and does not cause significant communication delay.

1.6 THESIS OUTLINE

The remainder of this thesis as follows. Related works are given in Chapter 2. The first version of proposed data collection mechanism from smart meter is introduced in Chapter 3. Also, the experimental results are shown in the chapter. Chapter 4 introduces the second version of proposed data collection mechanism. Furthermore, the chapter shows the experimental results. In Chapter 5, the proposed Secure AODV (SAODV) is presented. Besides, the experimental results are shown in the chapter. In Chapter 6, the prosed SAODV is applied to the proposed data collection mechanism from smart meter. Also, the experimental results are shown in the chapter. Finally, this thesis is concluded in Chapter 7 by discussing future works.

2. BACKGROUND

The existing traditional electric meters suffer from lack of two way communication. Due to this problem, utility companies have to hire employees to read meters data manually. In this model, there are limited hours to read meters and if there is no one in a building, employees cannot read meters since employees cannot enter the building. Furthermore, utilities cannot learn actual demand on peak and non-peak hours.

Another issue that focused on this thesis is network attacks in WSNs. Security is one of the most vital problems of WSNs. Hence, there must be some improvements and modifications for reliable and secure communication to achieve protection against security attacks and to provide privacy and reliability for WSNs and their applications.

The organization of this chapter is as follows: Chapter 2.1 presents an overview of AMR systems. The existing AMR systems has been introduced. Chapter 2.2 presents an overview of existing security problems and solutions in WSN. Some security issues with the smart meter data communication and vehicular communication technologies are introduced in Chapter 2.3.

2.1 OVERVIEW OF EXISTING AMR SYSTEMS

The number of studies on AMR systems has been increased with recent advances in wireless technology. With WAMR systems, two way communication capability is enabled and this allows utilities to get timely electricity consumption data which helps detect and prevent illegal electricity usage. Moreover, the employee expenses of utilities are reduced since they do not need to hire employees to read meters.

The existing AMR systems are given as follows (Tuna et al. 2011):

i Drive by AMR systems

ii Fixed network AMR systems

iii Touch based AMR systems

iv Walk by AMR systems

A utility company personnel drives by all the streets where it has customers in drive by AMR systems. This means extra cost for utility companies since they need vehicle, gas and etc. In fixed network AMR systems, there is an initial setup cost for setting up a permanent network. In touch based AMR systems, if there is no one at the building at the time of scheduled measurement, the utility company cannot get in the building and get information from the meters in that building. In walk by AMR systems, a utility personnel has to go inside each building to read meters and this takes too much time. Except fixed network AMR systems, all others systems require an employee to read meters. This causes increased expenses for utilities. In addition, these three AMR systems cannot give timely information to utilities. In drive by AMR and walk by AMR systems, utilities may get timely information by increasing number of personnel or number of vehicles but these solutions increase cost significantly. Our proposed data collection mechanism does not need any utility personnel for reading meters which helps utilities reduce their operating costs. In addition, our solution helps utilities get timely information from meters. Thus, utilities can predict users' future electricity consumption more realistically. A comparison of existing AMR systems is shown in Table 2.1.

Table 2.1: Comparison of AMR Systems

	Drive by AMR	Fixed network AMR	Touch based AMR	Walk by AMR	Our Solution
Less Cost	×	×	×	×	✓
Less Personnel	×	✓	×	×	✓
Initial Setup Cost	✓	✓	✓	✓	✓
Timely Measurements	✓	✓	×	✓	✓
Precise Measurements	✓	✓	×	✓	✓

The existing technologies that are used for data communication in AMR systems are

Power Line Communication (PLC), messaging over a GSM, phone line and short range Radio Frequency (RF) (Khalifa et al. 2011). In PLC, voltage transmission lines are used to transmit data. The meters transmit their data to PLC modems via the wireless or wired channels and these modems transmit data to the utility company using electric transmission lines (Choi et al. 2008, Kerk 2005, Soh & Kerk 2005, Park et al. 2002). In messaging over a GSM network, a GSM modem is installed on the meter and all data is transmitted via SMS to the utility company (Abdollahi et al. 2007, Tan et al. 2007, Zerfos et al. 2006). In telephone lines, it is assumed that each meter is equipped with a telephone line and data is transmitted via the telephone network in both directions (Kim 2006, Shi-Wei Lee et al. 1996). In RF, existing electricity meters are equipped with Bluetooth, Wi-Fi or ZigBee, and they transmit their data to a base station in a hop-by-hop fashion. All data collected on the base station is transmitted to the utility company using a dial-up connection or it is collected by an employee (Spencer 2008, Wesnarat & Tipsuwan 2006, Koay et al. 2003).

In (Niyato & Wang 2012), the authors introduced the applications for collecting data of smart meters in a smart grid. They also offered a solution to make better the transmission rate of a Data Aggregator Unit (DAU). The data in smart meters are transmitted to a DAU through a Neighborhood Area Network (NAN) via Wi-Fi and the DAU transmits the collected data to a Meter Data Management System (MDMS) through a WAN via WiMAX.

In (Ashna & George 2013), the authors designed a wireless GSM enabled energy meter. They also built a web site to manage the collected data and billing system. In their proposed mechanism, meters have GSM connection and thus utilities can monitor them regularly. The data collected at smart meters are periodically transmitted to the utility company and at the utility side a GSM receiver gets the data and writes it to a central database to update the consumption. In the proposed system, the data is processed in three steps as follows: 1) A digital GSM enabled power meter reads electricity consumption data, 2) The electricity consumption data is transmitted via SMS to the utility company, 3) The electricity consumption data is received and processed by the billing server

of the utility company.

In (Luan et al. 2015), the authors offered a hybrid cooperation mechanism for smart meters. In the proposed method, smart meters transmit their data to a base station using a short-distance communication technology such as Wi-Fi, ZigBee, Bluetooth, etc. And then, the base station uses the LTE technology to transmit the data to the utility company.

In (Tuna et al. 2011), the authors proposed a cost effective novel approach for AMR systems in rural areas. Instead of hiring people for meter reading, they offered using unmanned vehicles with GPS capability. They used the IEEE 802.15.4 communication protocol for their AMR system. They also made some simulations for the lifetime of battery used in WSN nodes. According to their performance evaluations, their proposed method is well suited for wide areas with few customers.

In (Miao et al. 2009), the authors designed and implemented a WAMR system. They added wireless modules to existing meters by using the ZigBee (Zigbee 2009) communication protocol. Since they used ZigBee communication, their proposed hardware has short-range and low-power wireless technology. In their proposed study, wireless modules are connected to meters through RS-485 buses. These wireless data collecting modules transmit their data to a sink node individually or through multi-hop communication in a hop-by-hop fashion. And then, on the sink node, the received data is wirelessly transmitted to a server node via an RS-232 bus.

In (Sheikh & Sharma 2011), the authors offered using GSM as the communication medium for WAMR Systems. In the suggested mechanism, meters transmit their information, including electricity usage, power quality and outage alarm, to the company, and at the end of each month, the utility suggested method would facilitate the generation of bills which will be sent to customers via SMS or e-mail.

Although all the mentioned studies in literature have made important amendments on existing AMR systems or proposed different data collection mechanisms for smart meters, they have some drawbacks. Many of them require subscription to GSM or telephone line

service, and some require installations and cable costs. Furthermore, the existing IEEE 802.15.4 protocol based solutions will not work in long ranges. In addition, since it has low data rate compared to IEEE 802.11p, when the size of transmitted data from smart meters increases or when the utility wants to transmit big data to its customers, the communication delay will increase significantly. The comparison of the technologies that are currently used in existing AMR systems and in our proposed scheme are shown in Table 2.2.

Table 2.2: Communication technologies for AMR systems

	Long Communication Range	No Subscription Requirement
ZigBee	×	✓
Bluetooth	×	✓
GSM	✓	×
Telephone Line	✓	×
Cable	×	×
IEEE 802.11p	✓	✓

2.2 OVERVIEW OF EXISTING SECURITY PROBLEMS AND SOLUTIONS IN WSN

Although WSNs are popular in both civilian and military sectors, they have their limitations, such as battery life, computation power and memory, when it comes to implementing traditional security mechanisms on WSN nodes (Patil & Chen 2017, 2013). In (Patil & Chen 2013), the authors give the WSN protocol stack and existing attacks on WSNs. They also give information about the basic security requirements including authentication, light-weight private key infrastructure and symmetric key algorithms. They also mention about secure routing in WSNs.

In (Finogeev & Finogeev 2017), the existing attacks on WSNs for SCADA systems are presented and classified. Key management methods are summarized for achieving secure data transmission. In (Kompara & Hölbl 2018), the security issues in Body Sensor Networks (BSN) are discussed. A key agreement protocol is proposed for BSNs and its

performance analysis is given in the matter of memory, communication and computation cost and energy consumption. It is concluded that, due to the limitations of BSNs such as small storage area and restricted computation power, symmetric key encryption is more preferable than asymmetric key encryption for providing security to BSNs.

In (Islam et al. 2012), the authors made research about automation and control of industrial systems. They introduced problems of WSNs in reliability and security for industrial systems. They claim that, after the energy consumption problem, security is the most important problem for WSNs in industrial applications. They mention cryptographic methods used in WSNs and suggest that traditional public key encryption algorithms are complex and not suitable for WSNs. They suggest that relatively less costly symmetric key algorithms such as AES, DES and RC4 are used in WSNs and the secret key is kept in a secure area on the sensor node.

In (He et al. 2017), an anonymous authentication method is proposed for Wireless Body Area Networks (WBAN). Since the client and server communicate wirelessly in WBANs, there should be an authentication scheme used for authenticating this communication. Instead of using traditional authentication schemes, they suggest storing the verification data on the network manager, unlike other approaches where the verification data is stored by the application provider. Although the proposed method provides security, since it uses a bilinear pairing scheme, it is not suitable for a distributed services environment and a multi-server architecture should be used to guarantee secure communications.

In (Li et al. 2015), the authors made research about the privacy and security issues for underwater sensor networks. They summarize some attacks on underwater sensor networks and countermeasures to overcome them. Furthermore, they propose mechanisms to achieve security and preserve node privacy in such networks.

In (Tomić & McCann 2017), the authors investigated attacks on WSNs. They review the protocol stack of WSNs, summarize possible attacks at different protocol stacks and give the consequences of the attacks on network performance. They implement some of these

attacks using Cooja, the Contiki's network simulator/emulator, to show their efficacy.

In (Deshmukh et al. 2016), the authors proposed a mechanism to detect blackhole nodes in the network. They add a validity value in reply packets to detect blackhole nodes. Although the simulation results are good, an intelligent blackhole attack may fail the proposed mechanism by resetting the validity value in the same way it is initially added.

In (Jain & Khuteta 2015), the authors proposed deploying the base node (BN) in the network to detect malicious nodes. According to the proposed scheme, the BN broadcasts dummy route request packets periodically and waits for replies. As the non-malicious nodes do not send a reply packet, the BN can list all the nodes sending a reply packet as malicious nodes. Finally, the BN shares its list of malicious nodes with the normal nodes, so that normal nodes can block the malicious nodes. This mechanism can prevent the blackhole attack and increase the delivery ratio. However, the BN is the single point of failure here and, in case of the failure of the BN, the proposed blackhole attack prevention mechanism will not work.

In (Patidar & Dubey 2014), the authors proposed a mechanism to protect the network against blackhole and wormhole attacks. They also try to improve network stability. They use a counter for checking the correct AODV routing behaviour. In order to monitor the system, they count the transmitted reply messages. Although, the delivery ratio increases for proposed system, there is also increasing in the end-to-end delay.

In (Elmahdi et al. 2018), the authors proposed a reliable and secure data transmission mechanism to mitigate blackhole attacks in Metropolitan Area Networks (MANETs). MANETs use the AOMDV routing protocol which is a modifed version of the AODV protocol. The main aim of the proposed system is splitting transmitted messages into many parts. All small messages are encrypted using an enhanced homomorphic encryption scheme. On the receiver side, all received message parts are decrypted. Although the delivery ratio increases in the proposed mechanism, since one message transforms into many small pieces, the total end-to-end delay increases. Moreover, the energy usage may

increase because of the increased total size of the transmitted messages.

In (Kaurav & Kumar 2017), the authors propose to install an Intrusion Detection System (IDS) to every node in the network. An unique ID has been assigned to all nodes in the network and the IDS monitors the traffic in the network. When the system detects a malicious node, it's information is transmitted to the base station. In this mechanism, the base station is the single point of failure and, if the base station breaks down, the system will fail in detecting malicious nodes. Furthermore, having an IDS run every WSN node adds a significant computational burden.

In (Kumar & Kumar 2015), the authors make improvements on the AODV routing protocol to detect blackhole attacks. They propose adding all incoming route reply packets in a table in the source node. The information from the received Route Reply (RREP) packets is stored in this table. Also, a threshold value is defined to compare the destination sequence number. When a RREP is received by a node, it compares the sequence number of the RREP with the threshold value and decides whether the node that sent the RREP is malicious or not. The proposed method increases the delivery ratio and throughput. However, it does not propose a solution for the RREQ packets and may not work if there is single adjacent node to the source.

All the studies mentioned above show that security is one of the most vital problems facing WSNs. Hence, there is an urgent need for investigating effective security mechanisms to increase the security and thus reliability of WSNs.

Although several of the studies mentioned above have made important and valuable contributions for blackhole attack prevention in WSNs, there is a single point of failure in most of these proposed solutions. Furthermore, many of the proposed existing solutions do not take advantage of an encryption algorithm. Finally, existing studies focus on only the reply packets in the AODV protocol. With this study, a solution is proposed which mitigates blackhole attacks by focusing on both the request and reply packets in the AODV protocol. The proposed solution uses encryption and it does not have a single point of

failure.

2.3 SECURITY ISSUES OF SMART METER DATA COMMUNICATION AND VEHICULAR COMMUNICATION TECHNOLOGIES

The existing traditional data collection mechanism from electric meters suffers from the lack of two-way communication and therefore information is collected from smart meters manually. With the integration of wireless communication technology and electric meters, smart meters have found a wider range of applications. Both utility companies and customers benefit from using Automatic Meter Reading (AMR) systems based on smart meters. By monitoring electricity consumption in real-time, utilities can effectively balance electricity consumption and production, and increase their efficiency, ultimately resulting in reduced electricity prices which would benefit customers. By using the smart metering technology having the capability to collect meter data remotely, utilities reduce their personnel costs.

Since VANET is updated version of Mobile Ad Hoc Network (MANET), it inherits the security issues related MANETs. In (Lin et al. 2008) the Vehicle Safety Communications (VSC) protocol is introduced. In VSC, the use of disposable anonymous certificates, signed by a certificate authority (CA), is offered to achieve privacy. However, if a Certificate Revocation List (CRL) is used, it is required to revoke compromised and expired certificates. A growing CRL and the overhead of the distribution of certificates are the main drawbacks of this system.

In (Isaac et al. 2010), some security problems and fragilities of VANETs are presented. In VANETs, malicious nodes can easily alter messages. By sending false messages, a node can mislead other nodes. By spoofing their identity, nodes can also cause Denial-of-Service (DOS) attacks. Finally, the identity of a vehicle can be obtained by brute force attack. In (Qu et al. 2015), threats and challenges related to VANETs are overviewed. These include the bogus information attack, the impersonation attack, eavesdropping, message

suspension and the hardware tampering attack. A summary of some basic ideas are also presented to mitigate these attacks. The use of symmetric and asymmetric cryptography is proposed to authenticate communicated messages. In (Mokhtar & Azab 2015), a classification of attacks on VANETs that exploit different network layers are presented. Furthermore, open research areas are presented for securing VANETs against the mentioned attacks, and the importance of data verification is emphasized for highly dynamic VANETs.

In (McDaniel & McLaughlin 2009), security and privacy challenges of smart grids are presented. The threat of smart meter data being manipulated by hackers is emphasized. It is mentioned that the hacking of smart meters can represent a billion dollar bug. Furthermore, privacy issues are pointed out related to customer data collected from smart meters. It is mentioned that household activities of home customers or trade secrets of business customers can be detected by sniffing networks and detecting the electricity usage patterns of customers. In (Hansen et al. 2017), the security aspects of the AMI system is analyzed and attacks on smart meters are summarized. Some of these attacks are categorized as theft of data and power, localized and widespread denial of power and disruption of grid. In addition, the direct and indirect impacts of these attacks are explained. In (Gungor et al. 2011), critical issues on smart grid technologies and standards are mentioned. A thorough review for existing communication systems in the smart grids are introduced and their pros and cons are summarized. The importance of having reliable and secure end-to-end communication is emphasized for utility companies to prevent billing frauds and other attacks. In (Deshmukh et al. 2016), the authors proposed a mechanism to detect blackhole node in the network. They added a validity value to reply packets to detect the blackhole node. Although the simulation results are good, an intelligent blackhole attack may fail the proposed mechanism by resetting the validity in the same way that the authors do.

As pointed out with the studies referred to in this section, the need for reliable and secure communication, in order to achieve protection against security attacks and provide privacy

for customers, is clear for both vehicular and smart grid communications. Our previous studies contributed to drive-by AMR systems by proposing the use of the IEEE 802.11p protocol by smart meters and public transportation buses collectively for facilitating smart grid data communication between household smart meters and utility companies (Bilgin et al. 2016b,a). In the same context, with this study, we address some security issues with the smart meter data communication and vehicular communication technologies.

3. DATA COLLECTION MECHANISM FROM SMART METER USING PUBLIC TRANSPORTATION BUSES

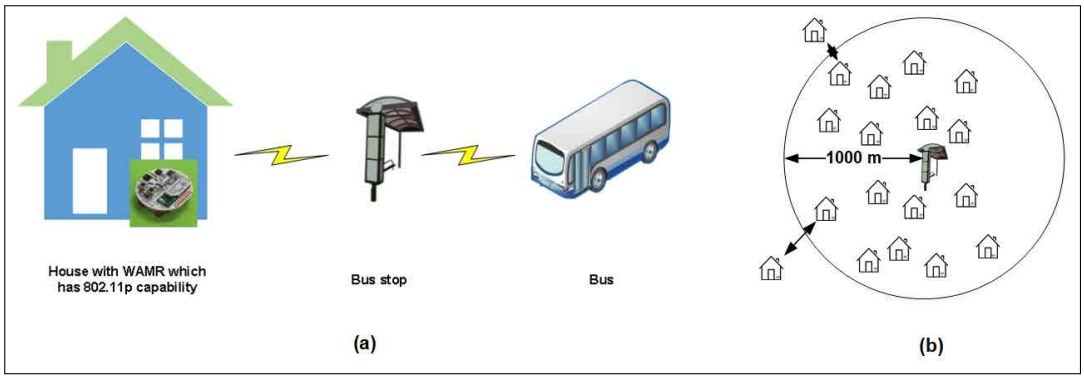
In this study, we explore the existing mechanisms for collecting data from smart meters and offer a new mechanism based on vehicular networks. Our solution enables collecting smart meter data using public transportation buses by extending the communication capability of smart meters to IEEE 802.11p. Since IEEE 802.11p allows communication in ranges up to 1000 m, smart meters within 1000 m of a public bus stop can transmit their data to the bus stop, and buses passing by the bus stop can receive the data and then transmit it to a central database via Road Side Units (RSUs).

3.1 PROPOSED SCHEME

In our proposed scheme, shown in Figure 3.1, data flows from houses, which have WAMR with 802.11p capability, to a bus stop, and then collected data on the bus stop is transmitted to a bus which drives by on its scheduled time. Upon receiving the collected data, the bus transmits it to the utility company using its on-board wide-band communication capability. Although we focus on the flow of smart meter data from smart meters to buses in this study, the proposed scheme would allow reverse data flow as well. For instance, if the utility control center wants to transmit an alert message to its customers, e.g. a new electricity unit price or a new campaign, or if it wants to send a message containing a reconfiguration file, a bus can download this message to the nearby bus stop within minutes, and finally the bus stop can transmit the message to the corresponding house. In the same way, regular updates to smart meters could be realized during specific times of the day.

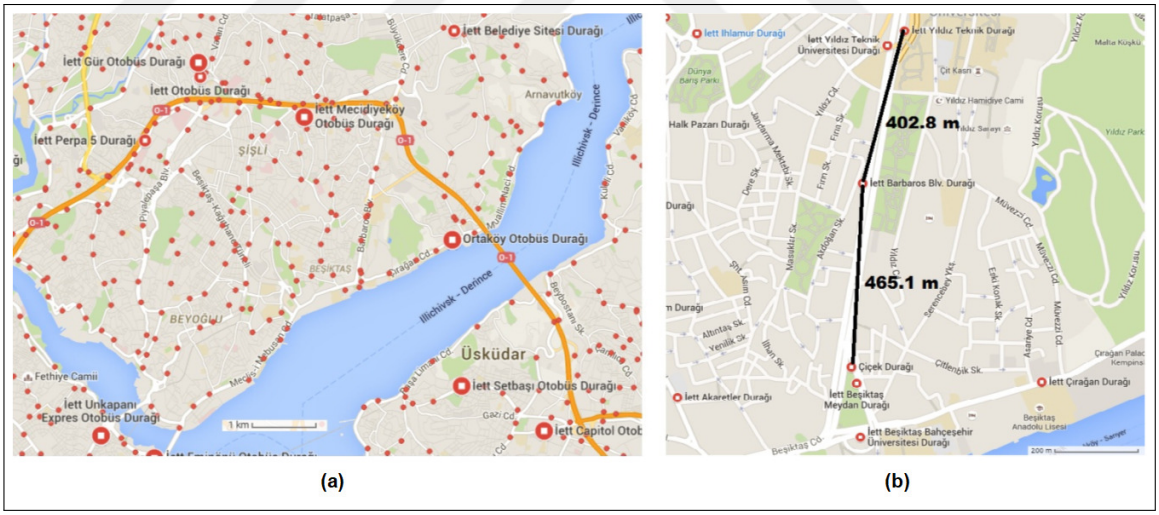
Figure 3.2 shows that Istanbul has a wide and dense network of bus stops and the distance between two bus stops in a typical urban neighbourhood is around 500 m. As seen in Figure 3.2 (b) the three neighbouring bus stops in the central Besiktas neighbourhood, located only 465.1 m and 402.8 m apart. Hence, in urban neighbourhoods of Istanbul,

Figure 3.1: (a) Proposed data collecting scheme (b) extended scheme allowing hop-by-hop communication



smart meters having a WAMR system with 802.11p capability can easily communicate with a nearby bus stop. With our proposed scheme, houses outside the direct communication range of a bus stop, i.e. farther than 1000 m from a bus stop, e.g. in rural areas far from city centre, can still communicate with a bus stop through an intermediary house, or through multiple intermediary houses, in a hop-by-hop fashion, as seen in Figure 3.1 (b).

Figure 3.2: (a) Map of Istanbul bus stops (b) distance between neighbouring bus stops



Source: Google Maps

3.2 PERFORMANCE EVALUATIONS

The performance of the proposed data collecting mechanism is investigated in this part. We conducted our performance evaluations using the ns-2 (NS-2 2011) simulator with

different numbers of sensor nodes.The log-normal channel parameters used for the simulations was experimentally determined by (Kunisch & Pamp 2008).

Wireless channel suffers from multi-channel effects, fluctuations in received signal strengths (fading), environmental characteristics such as outdoor, indoor, etc., and environmental effects such as noise (Nabar et al. 2004, Rappaport 2002). Also, there may be diffraction, scattering or reflection on the propagated signal wave. All these factors lead to decreased signal strength at the receiver since distance between the source and destination increases (Bilgin & Gungor 2012a, Zamalloa & Krishnamachari 2007). The following features of radio channels cause the fading phenomenon (Cerpa et al. 2003, Zhao & Govindan 2003, Ganesan et al. 2002):

i Asymmetrical links: Connectivity between nodes may be different,

ii Non-isotropic connectivity: Connectivity may not be same in all directions,

iii Non-monotic distance decay: Nodes far away from the source may get better connectivity compared to nodes that are geographically closer.

Therefore, a more general wireless channel model, based on empirical measurements, is required for more realistic performance evaluations.

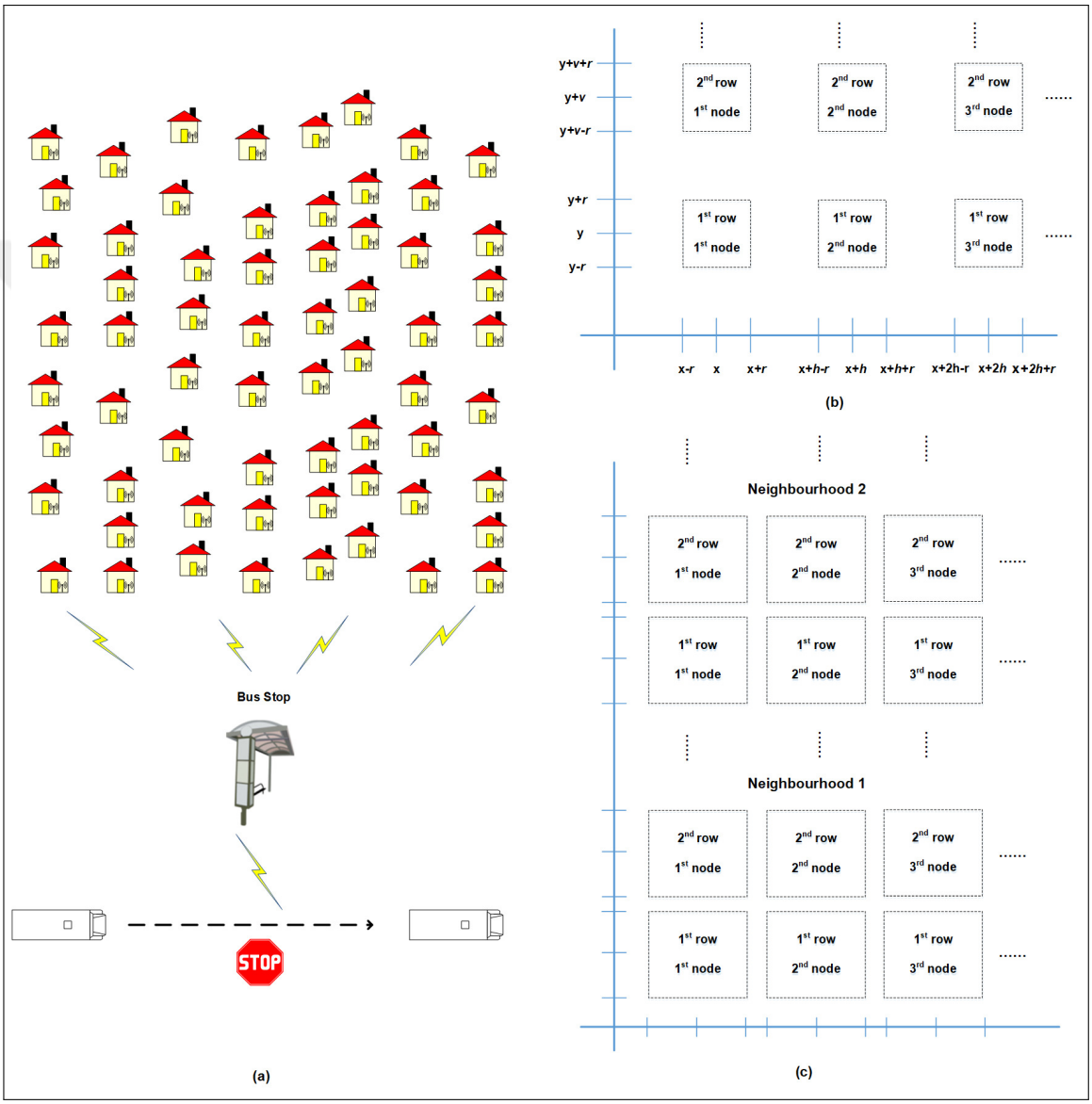
For the channel model log-normal shadowing is applied in our simulations, because this model is known to give more accurate results compared to other models, including Rayleigh or Nakagami for wireless environments (Rappaport 2002). The signal to noise ratio γ(d) at a distance d in the log normal shadowing model is:

$$\gamma(d)_{dB} = P_t - PL(d_0) - 10\eta \log_{10} \frac{d}{d_0} - X_\sigma - P_\eta \tag{3.1}$$

In equation 3.1, P_t shows the transmit power in dBm, PL(d_0) means the path loss at a reference distance d_0, $_\eta$ denotes the path loss exponent, X_σ indicates a zero-mean Gaussian random variable with standard deviation σ and P_η means the noise power in dBm.

The log-normal channel parameters have been acquired from field tests at 5.9 GHz, on highway, rural and urban environments. In our simulations, we used 1.61 as the path loss parameter and 3.4 as the shadowing deviation.

Figure 3.3: (a) An 8x8 cluster of nodes (b) node placement scenario (c) node placement scenario for hop-by-hop communication in a low population density neighbourhood



In our simulations, we have modelled a cluster of houses in a neighbourhood. For each simulation, we specified the number of rows and columns, which represent the number of horizontal and vertical lines along which houses are randomly aligned. Here, the num-

ber of rows multiplied with the number of columns in the cluster gives the number of nodes/houses (see the exemplary clusters in figure 3.3). Although we consider a grid structure, i.e. rows and columns of houses, the houses in the cluster are placed randomly to emulate houses in a neighbourhood. In our simulations, the starting point of the first node is fixed and the rest of the houses are randomly placed on the grid. We developed a C++ program to create the nodes (houses) in the ns-2 format and place them randomly on a grid. Our C++ program takes as input some simulation parameters such as the numbers of rows and columns in the grid and the initial starting position [x, y] of the node in the 1st row of the 1st column. Further simulation parameters are v and h, which denote the vertical and horizontal distances, respectively, between the starting points of consecutive nodes, and r which specifies up to how far away a node can be randomly placed from its starting position both in the horizontal and vertical axes. Then, nodes are randomly placed according to the following rule. Using the initial starting position [x, y], our program places the 1st node (the node at the 1st row and 1st column) randomly within the square area [x-r to x+r, y-r to y+r]. The starting points for the 1st node in the 2nd row is placed randomly around [x, y+v], within the square area [x-r to x+r, y+v-r to y+v+r]. Similarly, the 1st node in the 3rd row is placed randomly around [x, y+2.v], within the square area [x-r to x+r, y+2v-r to y+2v+r], etc. Likewise, the starting points for consecutive nodes on the same row are at a distance of h from each other. For instance, if the 1st node on a row is placed randomly within the square area [x-r to x+r, y-r to y+r], the 2nd one is placed randomly within the square area [x+h-r to x+h+r, y-r to y+r], the 3rd one placed randomly within the square area [x+2h-r to x+2h+r, y-r to y+r], etc. For each grid size, we used 100 different random seed values for the random placement of the nodes on the grid and ran our simulations with these seed values. An exemplary 8x8 cluster, a bus passing by and the bus stop are shown in figure 3.3 (a). In our performance results, we give the average of all the 100 measured values. At each simulation, we used 1 bus stop and 7 buses passing by which visit the bus stop according to the schedule given in Table 3.1. In order to make our simulations more realistic, we used the actual bus arrival times obtained from the Public Bus Transportation Authority of Istanbul (IETT) for the Besiktas Bahcesehir University bus stop, as listed in Table 3.1.

Table 3.1: Bus arrival times for the Besiktas Bahcesehir University bus stop (IETT 2014)

Bus Number	Arriving Time
29D	10:04:00 AM
43R	10:16:00 AM
25T	10:24:00 AM
58N	10:36:00 AM
63	10:44:00 AM
29C	10:55:00 AM
27E	11:05:00 AM

In our simulations, the electricity consumption data is transmitted from the houses to the bus stop every 10 minutes, and when a bus arrives at the bus stop, it receives from the bus stop the collected electricity consumption data of all the houses in the cluster for the last 10 minute time period. We utilized constant bit rate (CBR) traffic in our simulations. As the routing protocol, we tried the DSR and AODV routing protocols, since they are the most commonly used routing protocols for VANET studies. In our simulations the buses move in the same direction at a random speed of 45 to 55 km/h. All the parameters applied in the simulations are listed in Table 3.2.

Table 3.2: Simulation parameters

Paramater Name	Value
Network simulator	NS-2
Channel model	Log-Normal shadowing
Number of columns	2-20
Number of rows	2-20
Number of houses	4-400
Number of bus stops	1
Number of buses	7
Avg. max. bus speed	45-55
Packet size	100 bytes
Simulation time	3900 seconds
Traffic type	CBR
Queue type	Drop tail
Routing protocol	DSR, AODV
Vehicle movements	Same direction with different speed

The performance of the proposed mechanism is investigated for the transmission of data

packets from smart meters at houses, through the bus stop, to buses, all with IEEE 802.11p capability, using the following performance metrics:

i **End-to-End Delay:** Required time to transfer all data packets from source to destination side,

ii **Delivery Ratio:** Ratio of successfully received packets at destination to the all generated packets by source.

Successful transmission of consumer electricity consumption data from all houses to the bus stop is crucial in our mechanism. If data from some houses is lost during transmission, using the collected data the utility company may not produce a realistic data consumption report, which would decrease the efficiency of load balancing operations. Therefore, achieving a high delivery ratio is important. Similarly, the utility company needs to obtain the electricity consumption data in a timely manner to react to changes in load more quickly, which necessitates the data flow from the houses, through the bus stop, to the buses to be as fast as possible. Therefore, achieving a minimal end-to-end delay is desired.

For the proposed system, the performance of AODV and DSR protocols is investigated with regards to the delivery ratio and end-to-end delay performance metrics. Both AODV and DSR start discovering routes when a demand is initiated by the source node. Both of them broadcast RREQ packets to find a path between source and destination. The main difference between AODV and DSR is that in DSR multiple route cache entries are maintained for each destination, whereas in AODV one route entry is maintained per destination. Furthermore, in DSR source routing is used whereas in AODV a table-driven routing framework and sequence numbers are used to prevent loops (Rehan Rasheed et al. 2010, S Kaushik & R Deshmukh 2009, Yadav & Yadav 2009).

For testing the performance of the proposed scheme for varying node population densities, we performed simulations with varying numbers of nodes, representing neighbourhoods with different population densities. We achieved this by changing the simulation parameters v, h and r. We conducted simulations for neighbourhoods with up to 400 blocks of

houses, with the population densities of 676, 1326 and 169 houses/km^2, for normal, high and low population density neighbourhoods, respectively. The proposed data collecting mechanism is ideally offered for urban neighbourhoods where consecutive bus stops are less than 2 km apart and houses are less than 1 km away from the nearest bus stop. This will potentially yield a 100 percent coverage using the IEEE 802.11p protocol. We used a simulation space of size 800 m x 800 m in the maximum to ensure all nodes in the simulation are within 1 km from the bus stop. As noted in Figure 3.2, the average distance between consecutive bus stops in Istanbul is around 500 m in urban neighbourhoods, and hence an 800 m x 800 m simulation space is reasonable. For low, normal and high population density neighbourhoods, we set the distances between consecutive nodes to be around 40 m to 80 m by setting the simulation parameters v, h and r accordingly. Hence, along a distance of 800 m, there can be up to 800 m / 40 m = 20 houses. We considered row and column sizes of up to 20 in our simulations, resulting in a total number of up to 400 houses.

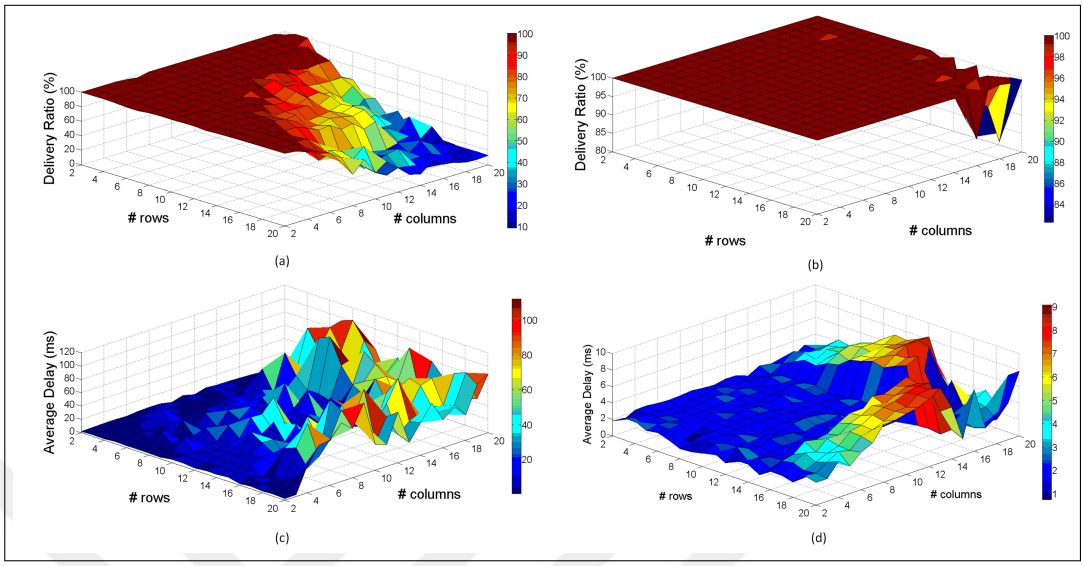
For the scenario when some houses are farther than 1000 m from the nearest bus stop, we also investigated through simulations the performance of a hop-by-hop data communication scheme. In this case, the smart meter data for the distant house is sent to the bus stop through an intermediary house in a hop-by-hop fashion.

3.2.1 Performance Results for Neighbourhoods With Normal Population Density

For normal population density neighbourhoods, we used the simulation parameters v = 40 m, h = 40 m, r = 10 m in our node placement scenario, which results in a population density of 676 houses/km^2. In this case, the starting points for consecutive nodes are placed 40 m apart on both the horizontal and vertical axes. In Figure 3.4, we give the simulation results for delivery ratio and end-to-end delay with the AODV and DSR routing protocols.

With AODV, for lower numbers of nodes the delivery ratios are higher, and all delivery

Figure 3.4: Simulation results in a normal population density neighbourhood for (a) delivery ratio with AODV, (b) delivery ratio with DSR, (c) end-to-end delay with AODV, (d) end-to-end delay with DSR



ratios are between 98.00 percent and 100 percent. As the numbers of rows and columns increase, delivery ratio decreases. Especially, when both the number of rows and the number of columns are higher than 15, the delivery ratio goes under 40 percent. The minimum and average delivery ratios with AODV are 9.39 percent (for the grid 20x18) and 75.74 percent, respectively. With DSR, for most cases the delivery ratio is between 96.00 percent and 100 percent. It starts decreasing when the number of rows and columns are both higher than 18, however it stays between 82.28 percent and 96.00 percent. The minimum delivery ratio of 82.28 percent occurs for the 17x19 grid and the average delivery ratio for all the simulated grid sizes is 99.61 percent. We can see that for larger grid sizes, i.e. higher numbers of nodes, the delivery ratios are dramatically low with AODV, and in general, the delivery ratios are much better with DSR.

As seen in Figure 3.4, with both routing protocols, the end-to-end delay increases with the number of nodes. The delay values are higher with AODV, compared to DSR. This may be due to the fact that the delay increases when the routing table entries in AODV expire. Note that if a routing table entry has not been active recently, it expires. All in all, DSR gives better results with the maximum delay of only 0.56 ms, compared to AODV with

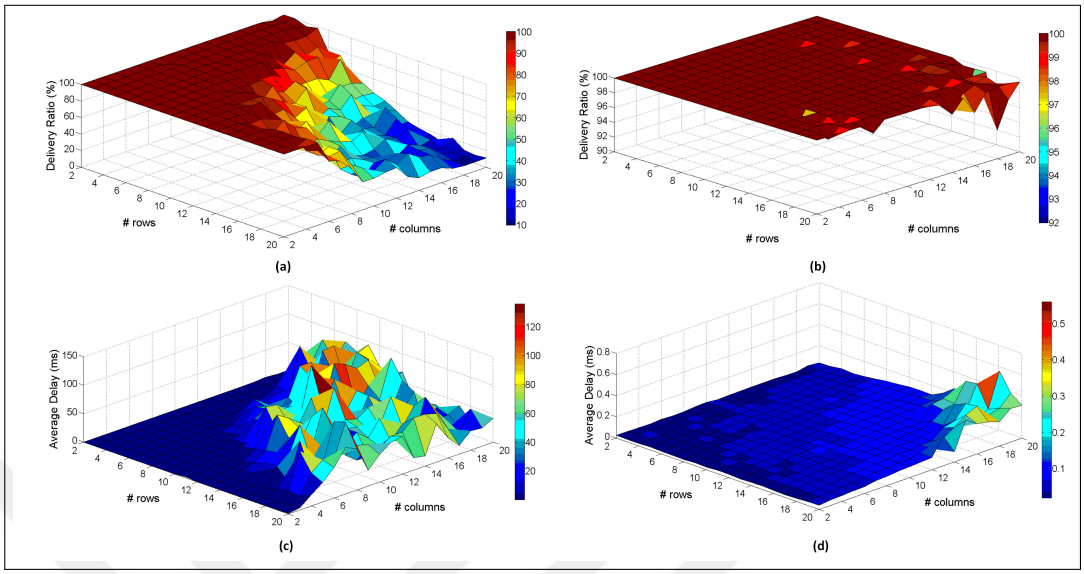
the significantly larger maximum delay of 135.31 ms. The average delay values are 31.68 ms and 0.08 ms with AODV and DSR, respectively. Note that in our proposed method most of the nodes are static and the only mobile nodes are the buses. Since the number of mobile nodes in our network is small, DSR gives better results. Furthermore, since AODV uses route expiry, packet drops may occur in this protocol when a new route is discovered, resulting in increased packet transmission times.

3.2.2 Performance Results for Neighbourhoods With High Population Density

We used the simulation parameters v = 40 m, h = 20 m, r = 10 m in our node placement scenario for a high population density neighbourhood, which results in a population density of 1326 houses/km^2. In this case, the starting points for consecutive nodes are placed 20 m apart on the horizontal axis for nodes on the same row and 40 m apart on the vertical axis for nodes on the same column. Note here that we allowed the spacing between consecutive rows to be larger than the spacing between consecutive columns to allow for interior parallel roads between rows of houses.

We give the simulation results for delivery ratio and end-to-end delay, with both the AODV and DSR routing protocols, in Figure 3.5. The mean of delivery ratio for all the number of nodes is 73.47 percent for AODV and 99.88 percent for DSR. With AODV, when both the numbers of rows and columns are higher than 16, the delivery ratio drops under 35 percent and the minimum delivery ratio is 9.95 percent (for the 20x19 grid). With DSR, the minimum delivery ratio of 91.99 percent occurs for the 18x20 grid. The maximum observed delay values are 111.94 ms and 9.07 ms, and the average the observed delay values are 30.01 ms and 3.60 ms, with AODV and DSR, respectively. In terms of delivery ratio and delay, while AODV is suitable for only smaller grids with lower number of nodes, DSR can be used for all grid sizes.

Figure 3.5: Simulation results in a high population density neighbourhood for (a) delivery ratio with AODV, (b) delivery ratio with DSR, (c) end-to-end delay with AODV, (d) end-to-end delay with DSR



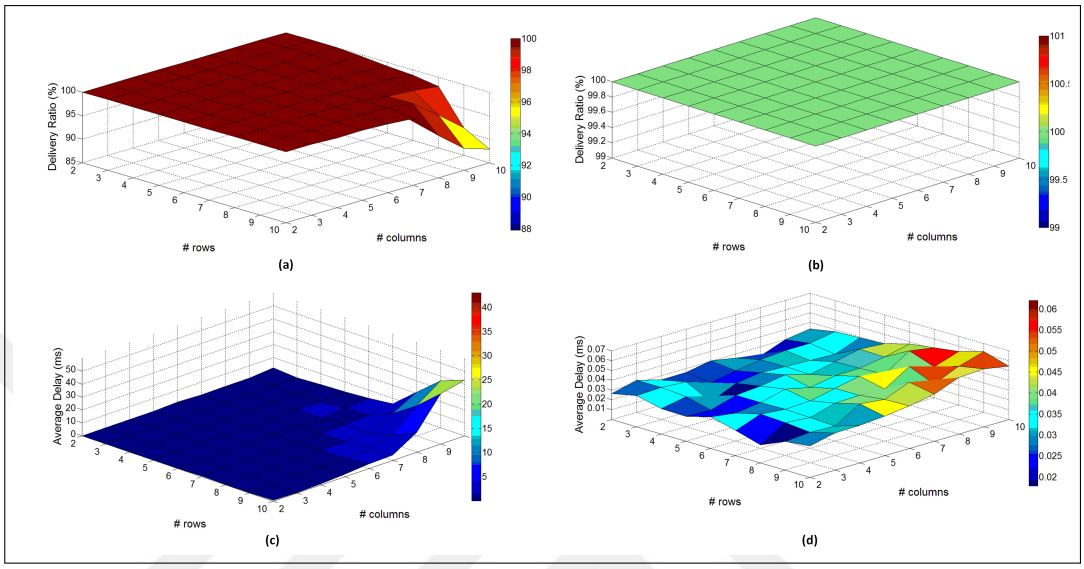
3.2.3 Performance Results for Neighbourhoods With Low Population Density

For low population density neighbourhoods, we used the simulation parameters v = 80 m, h = 80 m, r = 40 m in our node placement scenario, which results in a population density of 169 houses/km^2. In this case, the starting points for consecutive nodes are placed 80 m apart both on the horizontal and vertical axes for nodes placed on the same row and column, respectively.

The simulation results for delivery ratio, with both the AODV and DSR routing protocols, are given in Figure 3.6. As seen in the Figure 3.6, with AODV, for lower number of nodes, the delivery ratio is 100 percent, and for the number of nodes between 50 and 80, the delivery ratio is between 98.00 percent and 100 percent. When the number of nodes exceeds 80, the delivery ratio sharply decreases. Particularly, for the numbers of nodes higher than 90, the delivery ratio decreases down to 90 percent. Although the minimum delivery ratio is 87.95 percent (for the grid 10x10), the average delivery ratio for all grid sizes is 99.34 percent. With DSR, for all numbers of rows and columns, the delivery ratio is 100 percent. In terms of delivery ratio, the proposed mechanism gives good results with

both AODV and DSR for small grid sizes, however DSR is more desirable for larger grid sizes.

Figure 3.6: Simulation results in a low population density neighbourhood for (a) delivery ratio with AODV, (b) delivery ratio with DSR, (c) end-to-end delay with AODV, (d) end-to-end delay with DSR



In figures 3.6 (c) and (d), the simulation results with both AODV and DSR are given for end-to-end delay. With both protocols, when the number of nodes increases, the delay also increases. For number of nodes higher than 80, the delay exceeds 20 ms and the maximum delay is 43.01 ms (for the 10x10 grid and with AODV). The maximum delay value with DSR is only 0.06 ms. The average delay values are 3.28 ms and 0.037 ms with AODV and DSR, respectively.

3.2.4 Performance Results for Hop-by-Hop Communication in Low Population Density in Rural Neighbourhoods

We investigated the performance of the proposed scheme also with hop-by-hop communication for low population density neighbourhoods. We did simulations with both the AODV and DSR routing protocols. We used two 10x10 grids representing two consecutive neighbourhoods, as shown in Figure 3.3 (c), with the simulation parameters v = 80

m, h = 80 m, r = 40 m. In this scenario, we tried to achieve coverage for houses which are more than 1000 m farther from the bus stop. These houses transmit their data to the bus stop through another house located at the neighbouring grid that is within the communication range of the bus stop. We conducted simulations for only two neighbouring grids, each covering an area of approximately 1 km^2, however this scenario could be extended to cover multiple neighbourhoods and longer distances where houses would transmit their data to the bus stop through multiple intermediary neighbourhoods in a hop-by-hop fashion. We repeated all the simulations for 100 times and took the averages for the delivery ratio and end-to-end delay values.

Figure 3.7: (a) Delivery Ratio results (b) average end-to-end delay results (for hop-by-hop communication with the AODV and DSR routing protocols in low population density neighbourhoods)

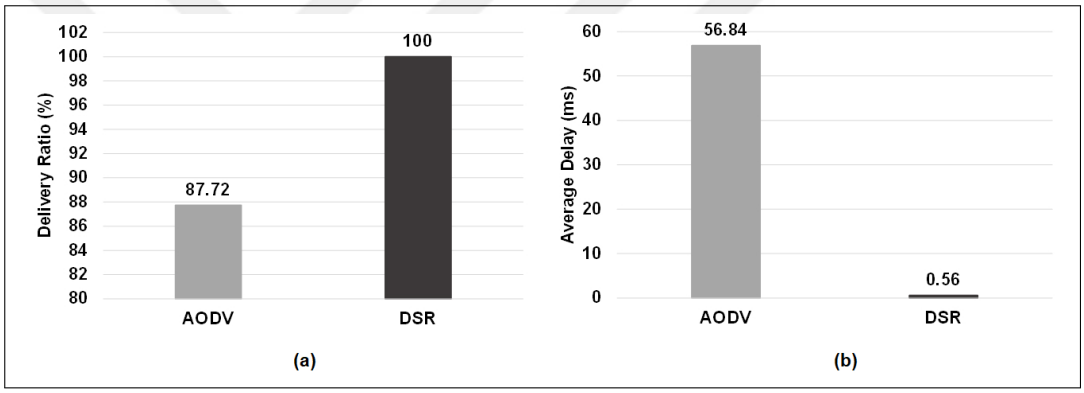


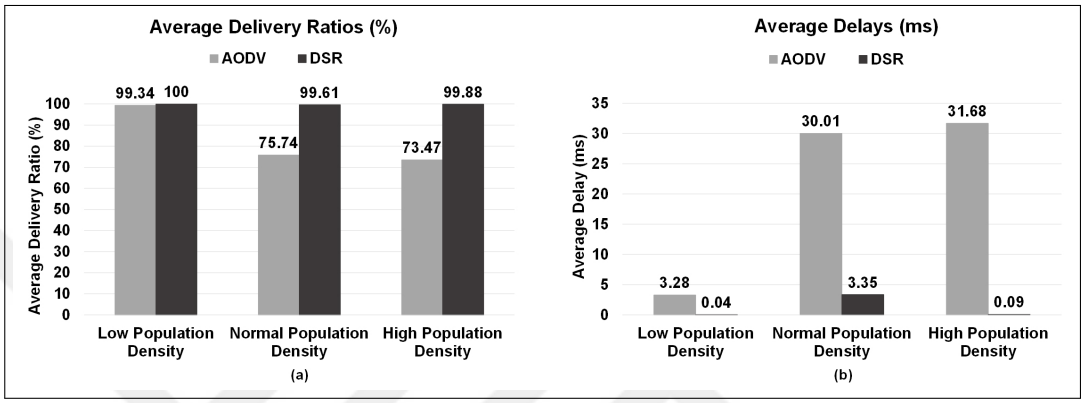
Figure 3.7 presents the simulation results for delivery ratio and end-to-end delay with both AODV and DSR. Obviously, both the delivery ratio and delay values are much better with DSR. While a 87.72 percent delivery ratio is achieved in 56.84 ms with AODV, a 100 percent delivery ratio is achieved in only 0.56 ms with DSR.

3.2.5 Overall Performance Analysis

In Figure 3.8, we summarize and compare our simulation results for the proposed smart grid data collecting scheme with both the AODV and DSR routing protocols, and for low, normal and high population density neighbourhoods. As seen in the Figure 3.8, DSR

results in a higher average delivery ratio than AODV for all population densities. Note that the average delivery ratio with DSR is equal to or only slightly less than 100 percent for all population densities. Similarly, DSR results in significantly lower average end-to-end delay compared to AODV. Note that in high population density neighbourhoods, the average end-to-end delay with DSR is orders of magnitude lower than that with AODV.

Figure 3.8: Simulation results for (a) delivery ratio (b) end-to-end delay



3.3 DISCUSSION

In this study, we merge WSNs with VANETs in a new mechanism for solving the data communication problem in smart grids. We have offered a new data collecting mechanism for smart meters by extending their communication capability to IEEE 802.11p. Changing their communication model, we propose collecting smart grid data from smart meters by using public transportation buses with wireless communication capability. In our proposed scheme, data of smart meters is transmitted to a bus stop, and then the bus stop transmits the data to a passing-by bus, which in turn transmits it to a central server of the utility company.

The performance of the proposed scheme is evaluated and simulations are made with two different routing protocols, namely AODV and DSR, to obtain end-to-end delay and delivery ratio values. The channel parameters used in our simulations were obtained from a set of field tests at 5.9 GHz in different environments. The performance measurements

show that the proposed data collecting scheme gets significantly better delivery ratio and lower delay when DSR is used.

4. NOVEL DATA COLLECTION MECHANISM USING PUBLIC TRANSPORTATION BUSES FOR SMART GRIDS

In smart grid systems the AMI technology plays a critical role(Yan et al. 2013, Bouhafs et al. 2012, Rua et al. 2010). Using the AMI technology the two-way communications between utility companies and consumers is enabled. Besides, AMI technology helps utilities to collect timely data on energy consumption, power quality and load profiles of their customers.

Vehicular communication is the vital technology in Intelligent Transportation Systems (ITS) to increase road safety and comfort (Härri et al. 2009). Recently, it has been reported as one of the most important technologies used in vehicles (Wang et al. 2012). The vehicular communication technology is also known as Vehicular Ad Hoc Networks (VANETs) which is an upgraded version of Mobile Ad Hoc Networks (MANETs) to vehicles. VANETs have special features compared to MANETs, including high and predictable mobility, large scale usage, partitioned networks and variable topology (Pereira et al. 2012).

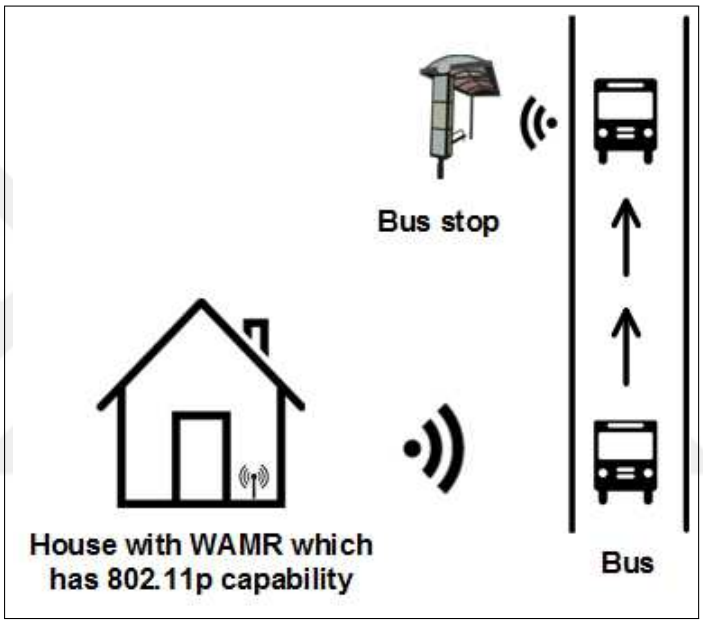
In this part, a new data collection mechanism is proposed. The proposed mechanism is a novel solution for data collection from smart meters and includes public transportation buses.

4.1 PROPOSED SCHEME

Almost all bus stops in Istanbul are smart bus stops that have embedded computers which are connected to the Internet through Wi-Fi and other wireless communication modules. In the long avenues of Istanbul, or in any similar city with a large network of smart bus stops, instead of hiring people to collect data from meters, meters with wireless capability may transmit their data to public transportation buses which pass regularly through their neighborhoods. The buses may then transmit their collected data wirelessly to the next bus

stop. And the bus stop, with its network connection, transmits the collected smart meter data to the utility company. This proposed scheme would be cost effective and provide a novel solution for transmitting consumer data to the utility company in a timely manner. It may be used for transmitting data related to billing, load-balancing or any other smart meter functionality. Since bus stops in Istanbul have Internet and Wi-Fi connection, the proposed system only needs smart meters with IEEE 802.11p communication capability. Likewise, all buses should be equipped with the IEEE 802.11p communication capability.

Figure 4.1: Proposed data collection scheme



The proposed data collecting mechanism uses public transportation buses, which has never been used for this purpose before. The data collected by a bus is transmitted to a bus stop. Thus, in our scheme, we combine the vehicular communication technology and the smart grid technology together. As shown in Figure 4.1, using the IEEE 802.11p communication protocol, our scheme extends the existing WAMR Devices' communication range to up to 1000 m. Smart meters within 1000 m of a public bus can transmit their data to the bus, and the data collected by the bus is transmitted to the bus stop when the bus arrives at the bus stop. In the proposed mechanism, bus stops are considered as Road Side Units (RSU) with an embedded processor and network connection to transmit their received smart meter data to the utility company.

With this study, the use of the IEEE 802.11p protocol is proposed for the first time in literature for use in smart grid applications. Unlike existing vehicular communication schemes in literature, our study uses both I2V and V2I communication. In our scheme, data flows first from smart meters to a bus through I2V communication and then from the bus to a bus stop through V2I communication.

The advantages of our proposed scheme can be summarized as follows. Since smart meters transmit their data to buses via the wireless channel, utility companies do not need to hire personnel to read this data manually. In addition, since buses operate regularly throughout most of the day, utility companies get electricity consumption data from customers in a timely manner. Moreover, utility companies can also send data, e. g. reconfiguration/update information, to their customers using this scheme.

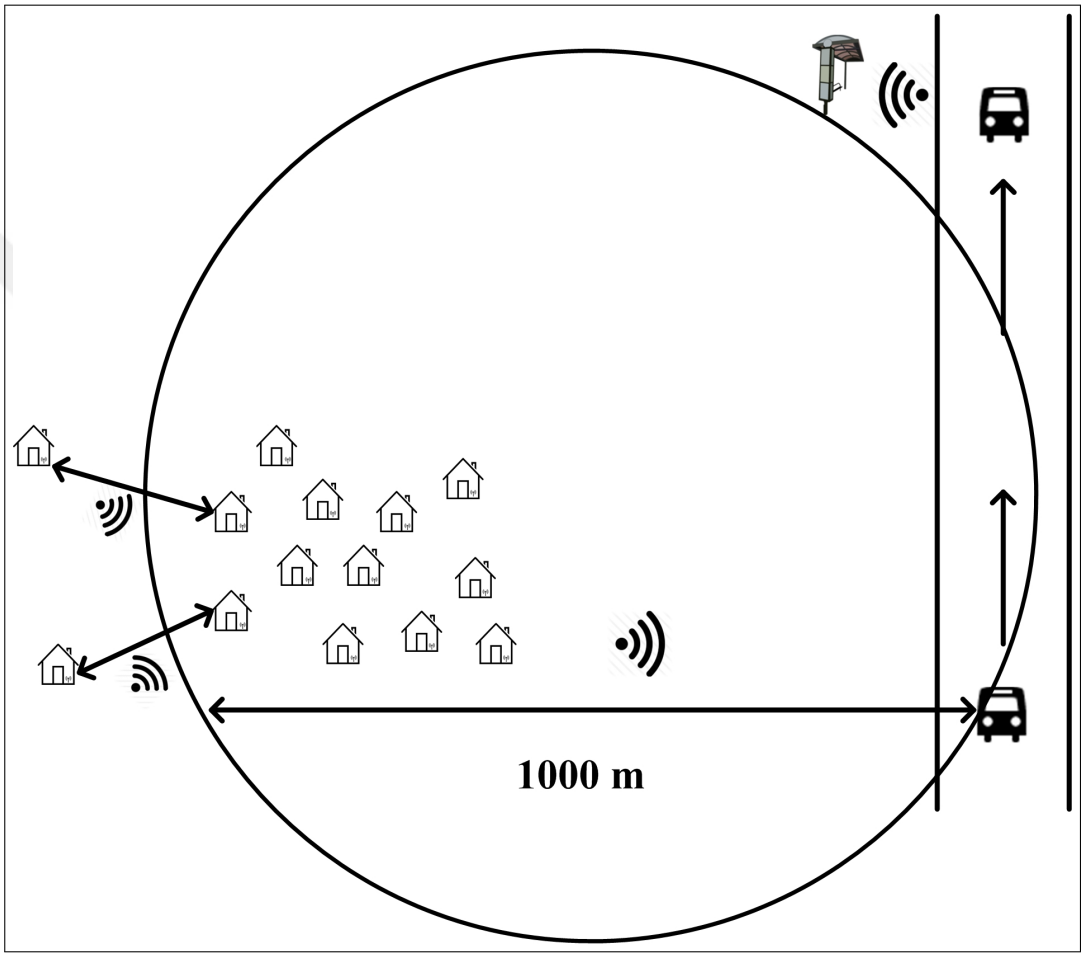
4.2 SYSTEM MODEL

In this part, we explain our proposed scheme in more detail. In the proposed scheme, houses with smart meters transmit their data, such as electricity consumption information, to buses which pass regularly through their neighborhoods. After that, the buses transmit the collected data wirelessly to the next bus stop. Finally, the bus stop transmits the collected smart meter data to the utility company. Although, the main concept of the proposed scheme is data collection from smart meters, it also supports two-way communication. For instance, when the utility company wants to transmit information to its customers, such as automatic reconfiguration data, the nearby bus stop can upload this information, which is received from the utility company, to a bus and the bus can transmit this information to the corresponding houses. In the proposed scheme, buses and bus stops are equipped with embedded computers and the buffer size for data transmission is the disc capacity of these embedded computers.

The mechanism mentioned above is most suitable for urban areas. The communication protocol used in our system has a communication range of up to 1000 m. In urban areas,

houses are typically covered by streets with running public transportation buses. Houses in rural areas, or houses in urban areas which are more than 1000 m away from a bus line, can also transmit their smart meter data to the bus through intermediary houses with hop-by-hop communication. In this scenario, the last house in the hop-by-hop communication should be within 1000 m far away from the bus road, as shown in Figure 4.2.

Figure 4.2: Extended proposed scheme allowing hop-by-hop communication



The total number of bus stops in Istanbul is 12396 and 774 of these are smart bus stops. Most of these smart bus stops are placed at central locations. However, the number of smart bus stops are increasing day by day. Therefore, we can assume that the percentage of smart bus stops in Istanbul will increase in the near future to cover significantly larger populations.

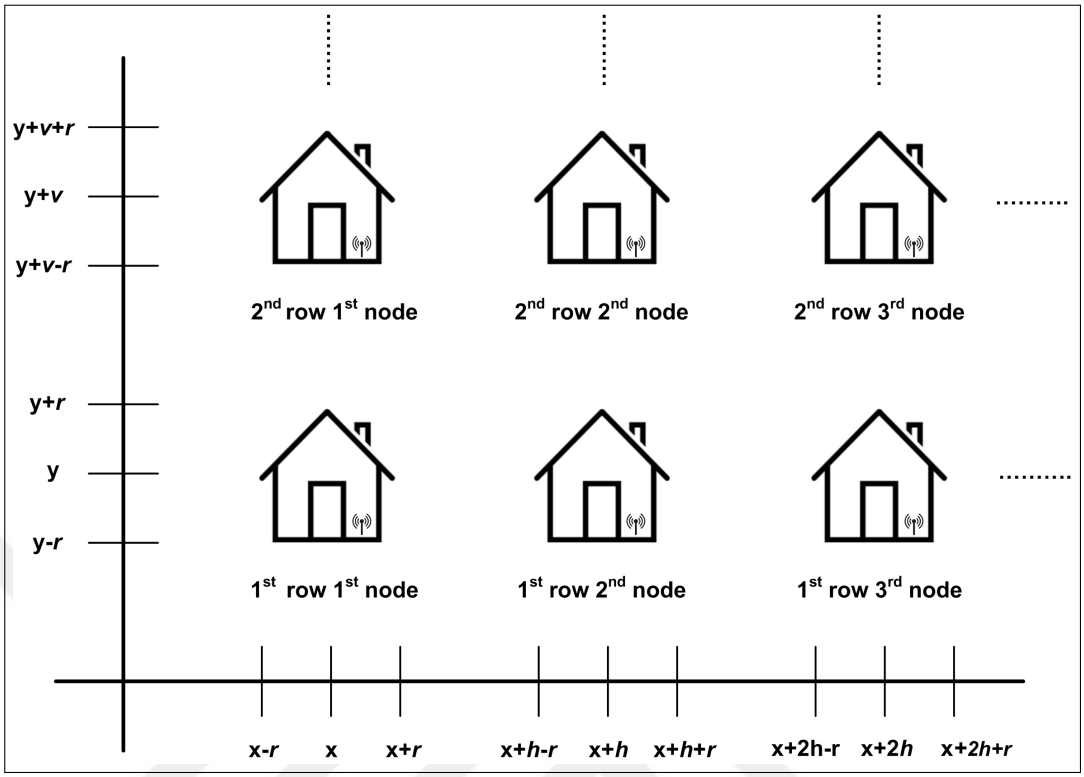
In our simulations, we have modeled a cluster of houses in a neighborhood. We used sev-

eral different numbers of rows and columns in the cluster. The number of rows multiplied by the number of columns gives the number of nodes (houses) in the grid (neighborhood). We developed a C++ program which puts the nodes (houses) randomly on the grid and creates them in the ns-2 simulation format. We also used three extra parameters for the node placement scenario in the proposed scheme. These parameters are *v, h* and *r* which represent vertical and horizontal distances between the fixed reference points for consecutive nodes and the amount of randomness used in the placement of nodes. Here, *v* and *h* specify how much away the fixed reference points for consecutive nodes are placed from each other along the vertical and horizontal axes, respectively, and the parameter *r* specifies the maximum distance up to which nodes are randomly placed from their fixed reference points on the grid in both the vertical and horizontal axes (see Figure 4.3). Nodes are placed by our program as illustrated with Figure 4.3. Here, using the initial starting position [x, y], our program places the 1st node, which is the node at the 1st row and1st column, randomly within the square area [x-*r* to x+*r*, y-*r* to y+*r*]. The second node on the same row is placed randomly within the square area [x+*h*-*r* to x+*h*+*r*, y-*r* to y+*r*] and the 3rd node is placed randomly within the square area [x+2*h*-*r* to x+2*h*+*r*, y-*r* to y+*r*], etc. Likewise, the reference points for consecutive nodes on the same column are placed *v* meters apart on the vertical axis starting from the position [x, y]. For instance, the 1st node in the 2nd row is placed randomly around its reference point [x, y+*v*], within the square area [x-*r* to x+*r*, y+*v*-*r* to y+*v*+*r*]. Similarly, the 1st node in the 3rd row is placed randomly around its reference point [x, y+2*v*], within the square area [x-*r* to x+*r*, y+2*v*-*r* to y+2*v*+*r*], etc.

4.3 PERFORMANCE EVALUATIONS

We conducted the performance evaluations of our proposed scheme using ns-2 (NS-2 2011) with different number of nodes. The channel parameters that are used in our simulations are given in Table 4.1. These parameters have been experimentally obtained with a set of field tests at 5.9 GHz for different vehicular communication environments, in-

Figure 4.3: Node placement scenario



cluding highway, rural and urban, based on (Kunisch & Pamp 2008). Here, the authors considered cars moving in the same and opposite directions in urban areas. In addition, they also included the scenario when two communicating cars are stationary while all the other cars are moving.

Table 4.1: Log-normal shadowing parameters

Variable Name	Value
Path Loss	1.61 AM
Shadowing deviation	3.4

There are some well-known problems for wireless channels, given as follows (Nabar et al. 2004, Rappaport 2002):

i Environmental characteristics such as outdoor, indoor, etc.

ii Environmental effects including noise, interference, etc.,

iii Fluctuations in received signal strengths which is also known as fading,

iv Multi-channel effects.

In addition to these problems, the propagated signal wave may be diffracted, reflected or scattered. All these problems cause a decrease on the received signal strength when the distance increases between transceivers (Zamalloa & Krishnamachari 2007, Bilgin & Gungor 2012a). The following features of radio channels are well-known and have to be considered carefully (Cerpa et al. 2003, Zhao & Govindan 2003, Ganesan et al. 2002):

i **Asymmetrical links:** The connectivity from node A to node B may not be same compared to node B to node A,

ii **Non-isotropic connectivity:** The connectivity may be different for the same distance from source in all directions,

iii **Non-monotonic distance decay:** Nodes which are closer to source may have worse connectivity compared to nodes which are far away from the source.

In our simulations, based on the problems and features mentioned above, we have chosen the log-normal shadowing model to get more realistic performance evaluations. Compared to other channel models, the log-normal shadowing model gives more correct and realistic results (Rappaport 2002).

The signal to noise ratio γ(d) at a distance d in the log normal shadowing model is:

$$\gamma(d)_{dB} = P_t - PL(d_0) - 10\eta \log_{10} \frac{d}{d_0} - X_\sigma - P_\eta \tag{4.1}$$

For measuring the performance of our proposed system, we made simulations with varying numbers of nodes by changing the *v, h* and *r* values which are defined in section 4.2. Thus, we achieved different population densities. For each grid size, we used 100 different random seed values for the random placement of the nodes in the grid and ran our simulations 100 times with these seed values. In our performance results, we give

the average of the 100 measured values. In order to have more realistic simulations, we used the actual bus arrival times obtained from the Public Bus Transportation Authority of Istanbul (IETT) for the Beşiktaş Bahçeşehir University bus stop, as listed in Table 3.1. In our simulations, the smart meter data for electricity consumption, load profile of customers and the power quality are transmitted from the houses to the bus every 10 minutes, and when the bus arrives at the bus stop, it transmits all the data collected from the houses in the cluster, for the previous 10 minute time period, to the bus stop.

The simulation parameters which are used for performance evaluations are listed in Table 4.2. As shown in the table, CBR traffic is utilized. In addition, DSR and AODV are chosen as routing protocol. The speed of the buses are defined random between 45 to 50 km/h.

Table 4.2: Simulation parameters

Paramater Name	Value
Network simulator	NS-2
Channel model	Log-Normal shadowing
Number of columns	2-20
Number of rows	2-20
Number of houses	4-400
Number of bus stops	1
Number of buses	7
Avg. max. bus speed	45-50
Packet size	100 bytes
Simulation time	3900 seconds
Traffic type	CBR
Queue type	Drop tail
Routing protocol	DSR, AODV
Vehicle movements	Same direction with different speed

In our performance evaluations, we investigated the performance of our system, for data transmission from the smart meters to the buses and from buses to the bus stop, using the following performance metrics:

i **Total End-to-End Delay** is the total time to transmit all packets from source to destination side.

ii **Delivery Ratio** is the ratio of the successfully received packets on the destination side to all packets generated on source side.

In our mechanism, data generated by a smart meter firstly flows from the house to a bus, and then from the bus to the bus stop. To generate a more realistic report on electricity consumption in the neighborhood for the utility company, it is crucial that data is delivered from all the houses to the bus. Therefore, achieving a high delivery ratio, e.g. as close to 100 percent as possible, is very important. Similarly, in order to react to changes in the load more quickly and achieve load-balancing in a timely manner, electricity consumption data should be received as fast as possible. Therefore, the end-to-end delay should be as small as possible.

We simulated our proposed smart grid data collection scheme using AODV and DSR, which are two well-known reactive routing protocols, (Rendong Bai & Singhal 2006) and investigated its performance in detail in terms of total end-to-end delay and delivery ratio. Both AODV and DSR are on demand routing protocols that means they start discovering routes when a demand is initiated by the source node. They both start flooding RREQ to find a route between destination and source. The main difference between the two routing protocols is that in AODV only one route entry is maintained per destination. On the other hand, in DSR multiple route cache entries are maintained for each destination. However, in order to prevent loops, in AODV a table-driven routing framework and sequence numbers are used, whereas in DSR source routing is used (Rehan Rasheed et al. 2010, S Kaushik & R Deshmukh 2009, Yadav & Yadav 2009).

4.3.1 Performance Results for Normal Population Density

In order to investigate the performance of our proposed scheme in a normal population density neighbourhood, we selected the simulation parameters for our node placement scenario as v = 40 m, h = 40 m and r = 10 m. In this scenario, the distance between the reference points for consecutive nodes is 40 m along both the vertical and horizontal axes,

and there are a total number of up to 225 houses in the simulated grid.

Figure 4.4 shows the end-to-end delays from houses to a bus, with both the AODV and DSR routing protocols, for our normal population density scenario. As shown in the Figure 4.4, for both routing protocols, the end-to-end delay increases when the grid size, and hence the number of nodes (houses), increases. For smaller grid sizes, the end-to-end delay is lower in the AODV routing protocol compared to the DSR routing protocol. On the other hand, for larger grid sizes, DSR has lower end-to-end delay, and even when the numbers of rows and columns both take the maximum value of 15 (which means there are 225 nodes in the cluster), its end-to-end delay is less than 80 milliseconds.

Figure 4.4: End-to-end delays from the houses to the bus with the (a) AODV and (b) DSR routing protocols for normal population density

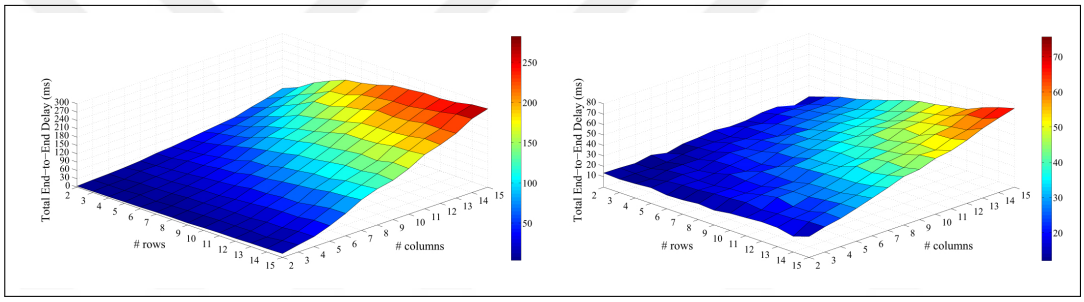


Figure 4.5 shows the end-to-end delays from the bus to the bus stop with both the AODV and DSR routing protocols for normal population density. As expected, the end-to-end delay increases when the number of nodes increases. An increase in the number of nodes means an increase in the amount of data collected by the bus. As shown in the Figure 4.5, the AODV routing protocol is more efficient for smaller grid sizes compared to the DSR routing protocol. On the other hand, for larger grid sizes the DSR routing protocol has better delivery ratio results and its end-to-end delay is less than 70 milliseconds in all cases.

To calculate the total end-to-end delay from the houses to the utility company, we assumed that all bus stops have 1 Mb/sec network connection speed and calculated the delay for transmitting data from a bus stop to the utility using this connection speed. Finally, we added the calculated delay to our end-to-end delay results from houses to the bus stop.

Figure 4.5: End-to-end delays from the bus to the bus stop with the (a) AODV and (b) DSR routing protocols for normal population density

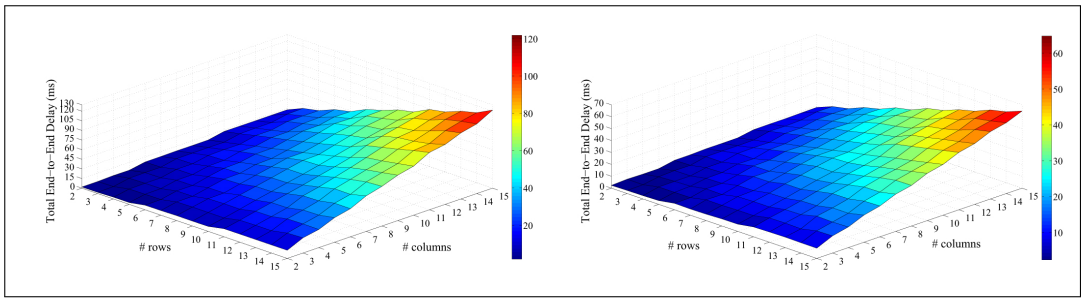


Figure 4.6 shows the total end-to-delays from houses to the utility company, with both the AODV and DSR routing protocols, for normal population density. Note that the results here are the summation of the delay values given in Figures 4.4 and 4.5, and the delay due to data transmission from the bus stop to the utility company.

Figure 4.6: Total end-to-end delays from houses to the utility center with the (a) AODV and (b) DSR routing protocols for a normal population density neighbourhood

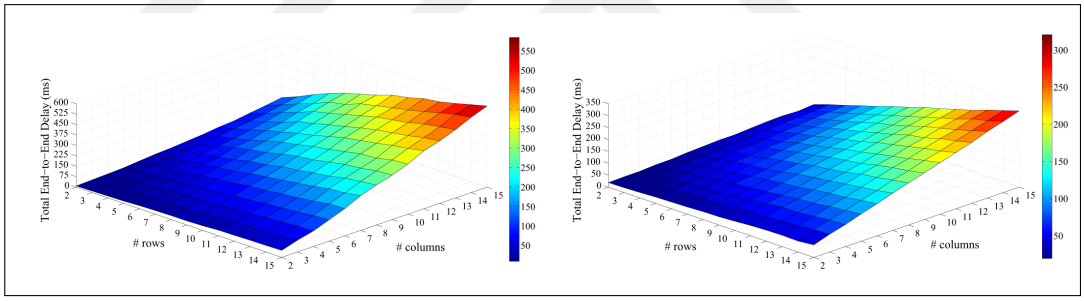
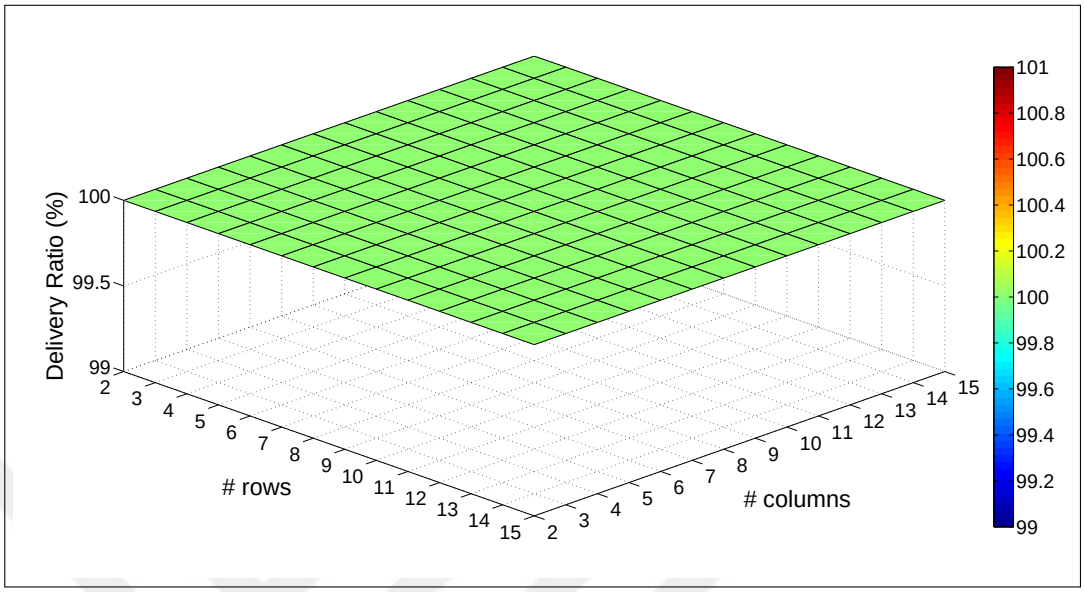


Figure 4.7 shows the delivery ratio results with the AODV and DSR routing protocols for smart meter data transmission from the houses, through a bus, to the bus stop in a normal population density neighbourhood. As shown in the Figure 4.7, the delivery ratio is 100 percent for all scenarios which means all smart meters successfully transmitted their data to the bus and all collected data on the buses is successfully transmitted to the bus stop.

Figure 4.7: Delivery ratios for smart meter data transmission from houses, through the bus, to the bus stop in a normal population density neighbourhood, using the AODV and DSR routing protocols



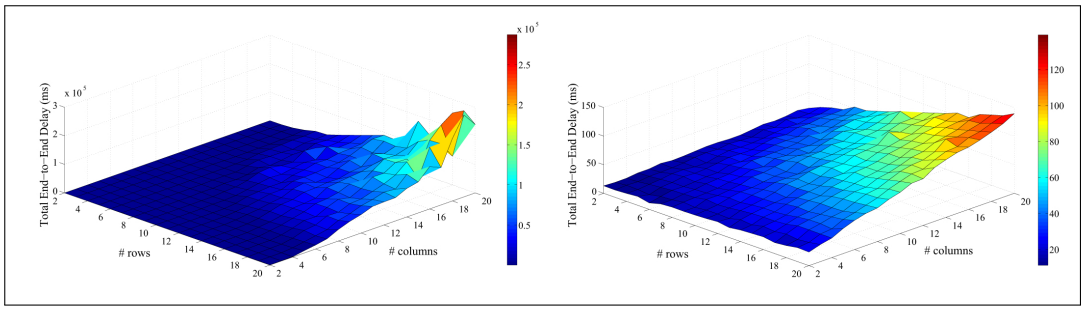
4.3.2 Performance Results for High Population Density

In order to investigate the performance of the proposed scheme in a high population density neighbourhood, we selected the simulation parameters for our node placement scenario as v = 20 m, h = 20 m and r = 10 m. In this scenario, the distance between the reference points for consecutive nodes is 20 m along both the vertical and horizontal axes, and there are a total number of up to 400 houses in the simulated grid.

Figure 4.8 shows the end-to-end delays for smart meter data transmissions from the houses to the bus using the AODV and DSR routing protocols in a high population density neighbourhood. As shown in the Figure 4.8, with both routing protocols, the end-to-end delay increases when the grid size (number of houses) increases. Compared to the DSR routing protocol, the AODV routing protocol results in lower end-to-end delays for smaller grid sizes. In contrast, using the DSR protocol leads to a lower end-to-end delay for larger grid sizes compared to the AODV protocol.

Figure 4.9 shows the end-to-end delays for smart meter data transmission from the bus

Figure 4.8: End-to-end delays from the houses to the bus with the (a) AODV and (b) DSR routing protocols for high population density



to the bus stop, using the AODV and DSR routing protocols, in high population density neighbourhoods. As shown in the Figure 4.9, when the number of nodes increases, the data transmission time increases. We can see that for all grid sizes the AODV routing protocol has better performance in end-to-end delay than the DSR routing protocol.

Figure 4.9: End-to-end delays from the bus to the bus stop with the (a) AODV and (b) DSR routing protocols for high population density

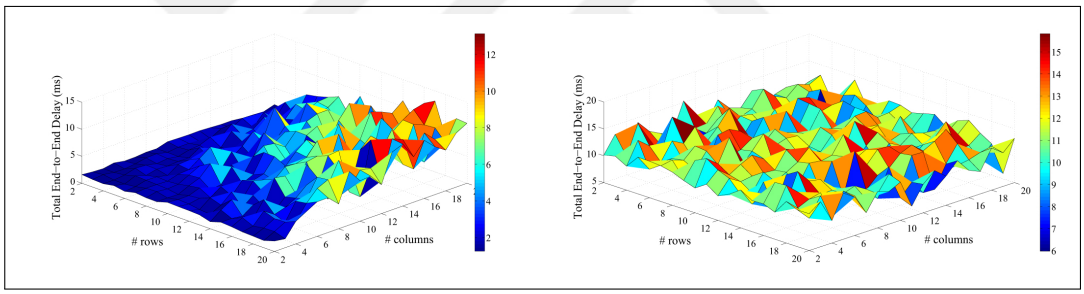


Figure 4.10 shows the total end-to-delays from houses to the utility center in high population density neighbourhoods, for both the AODV and DSR routing protocols. These delay values are the summation of the delay values given in Figures 8 and 9, and the delay due to data transmission from the bus stop to the utility company. Although, the AODV routing protocol results in lower end-to-end delays than the DSR routing protocol for smaller grid sizes, for larger grid sizes DSR results in lower end-to-end delay values than AODV. Even when the numbers of rows and columns take the maximum value of 20 (which means there are 400 houses in the grid), the total end-to-end delay is less than 500 milliseconds with DSR. Whereas, with AODV, in the same scenario with 400 houses in the grid, the total end-to-end delay has the dramatically higher value of more than 287

seconds.

Figure 4.10: Total end-to-end delays from the houses to utility with the (a) AODV and (b) DSR routing protocols for high population density

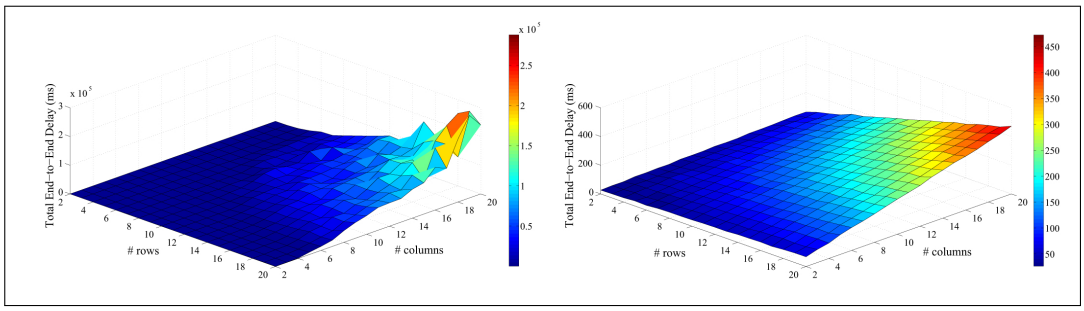


Figure 4.11: Delivery ratios for smart meter data transmission from houses to the bus in high population density neighbourhoods with (a) AODV and (b) DSR routing protocols

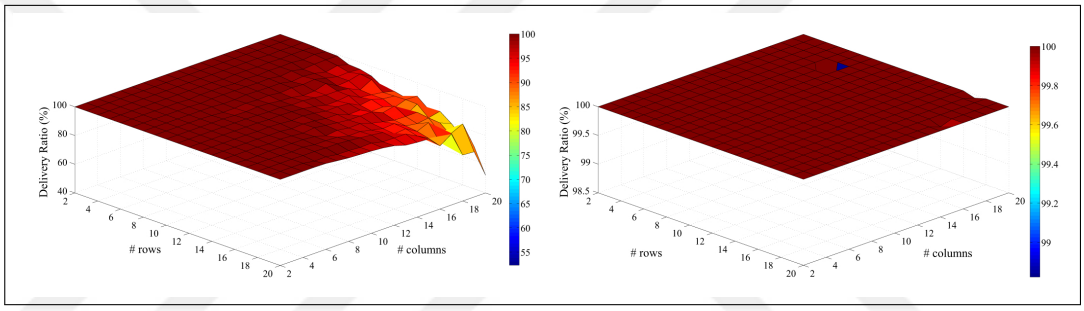
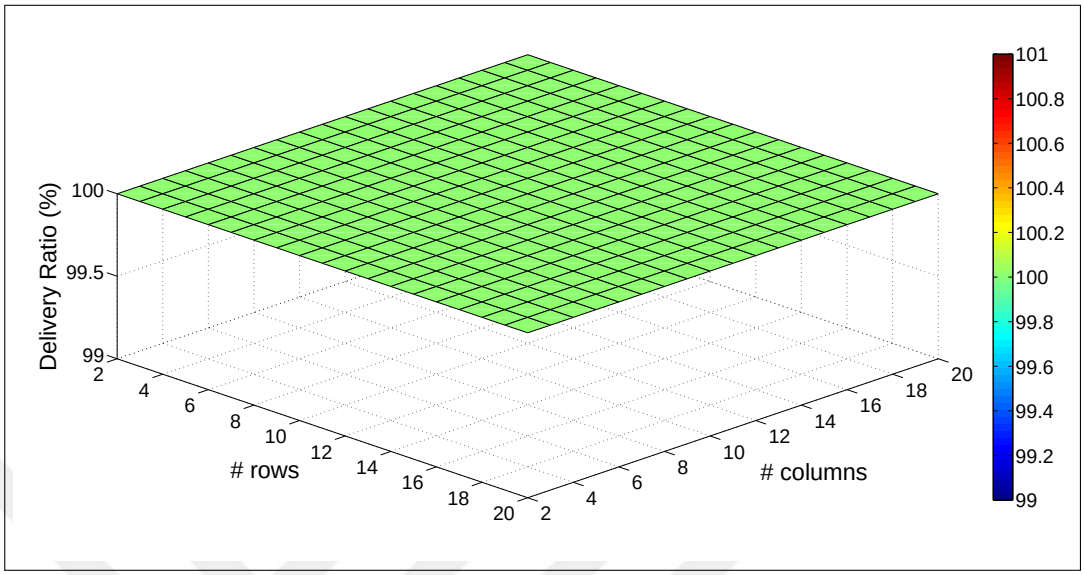


Figure 4.11 and 4.12 show the delivery ratios for smart meter data transmission from the houses to the bus and from the bus to the bus stop, respectively, in high population density neighbourhoods, using the AODV and DSR routing protocols. As shown in the Figure 4.11, with the AODV routing protocol, the delivery ratio for data transmission from houses to bus decreases when the number of nodes increases. The delivery ratio decreases down to 52 percent for AODV. For the same data transmission scenario, the DSR routing protocol achieves almost 100 percent delivery ratio, i.e. the delivery ratio is always higher than 98 percent. As shown in Figure 4.12, with both AODV and DSR, the delivery ratio is 100 percent for smart meter data transmissions from the bus to the bus stop.

Figure 4.12: Delivery ratios for smart meter data transmission from the bus to the bus stop in a high population density neighbourhood with (a) AODV and (b) DSR routing protocols



4.3.3 Performance Results for Hop-by-Hop Communication in a Low Population Density Neighbourhood

For neighbourhoods where some houses are located farther than 1000 m away from bus roads, we explored the applicability of our scheme using multi-hop communication between a houses and a bus. In urban areas, houses are typically covered by streets with running public transportation lines. However, houses in rural areas, or houses in urban areas which are more than 1000 m away from a bus line, can still transmit their smart meter data to the bus through intermediary houses using an extended version of our scheme which allows hop-by-hop communication. In this scenario, the last house in the hop-by-hop communication should be within 1000 m distance from the bus line. In this study, we conducted simulations for a 2-hop communication scenario where a house communicates its smart meter data to the bus through another intermediary house that is within 1000 m proximity from the bus road. In our node placement scenario, we have two consecutive neighbourhoods, each in the shape of a 13x13 grid (with 169 houses), where one of the neighbourhoods is placed completely within 1000 m from the bus line and the other one is located outside the coverage range of the bus line. Here, the houses in the distant

neighbourhood communicate with the bus through an intermediary house located in the consecutive neighbourhood that is within the coverage area of a bus line. The simulation parameters for our node placement scenario are defined as v = 80 m, h = 80 m, r = 40 m. In this situation, the distance between nodes are 80 m for both the vertical and horizontal axes.

Figure 4.13: Total end-to-end delays with the AODV and DSR routing protocols for the hop-by-hop communication scenario

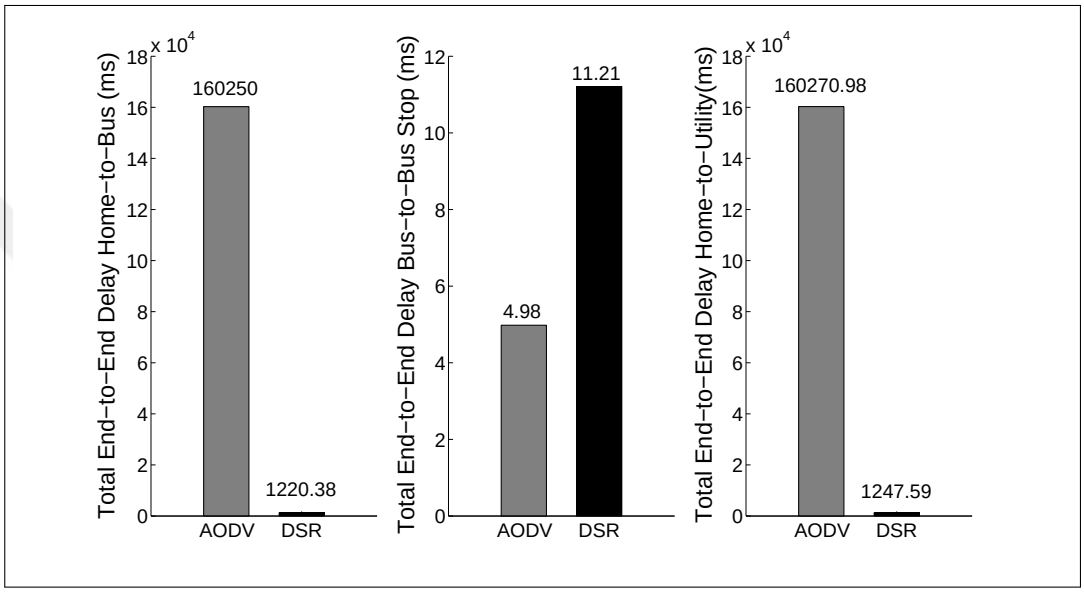
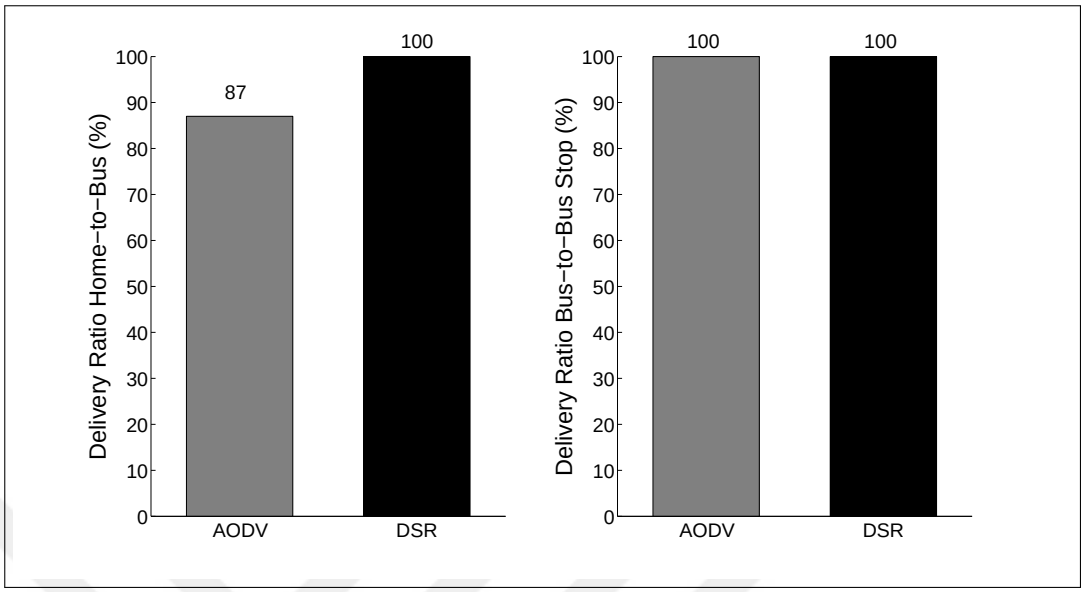


Figure 4.13 and 4.14 show the total end-to-end delays and the delivery ratios for AODV and DSR routing protocols, respectively, for 2-hop communication in a low population density neighbourhood. As shown in Figure 4.13, AODV has lower delay than DSR for smart meter data transmission from bus to bus stop. On the other hand, for data transmission from houses to the bus, DSR has lower delay than AODV. In terms of delivery ratio, as shown in the Figure 4.14, DSR performs better than AODV for smart meter data transmission from houses to buses. With both AODV and DSR, the delivery ratio is 100 percent for smart meter data transmission from the bus to the bus stop.

Figure 4.14: Delivery ratios with the AODV and DSR routing protocols for the hop-by-hop communication scenario



4.4 DISCUSSION

In this study, we proposed a solution to the data collection problem in smart grids using the wireless communication technology and by merging the smart grid AMI technology with vehicular Ad-Hoc networks. We proposed a data collection mechanism that extends the communication range of smart meters by up to 1000m by adapting the IEEE 802.11p communication protocol. With this new communication model, data generated by smart meters can be transmitted to the utility company via public transportation buses. In our proposed mechanism, data from smart meters is transmitted to a public transportation bus. After then, the bus transmits the data to the bus stop with a network connection. The bus stop then transmits the smart meter data to the utility company.

The performance of the proposed data collection scheme have evaluated in terms of end-to-end delay and delivery ratio with AODV and DSR protocols, for normal density, high density and hop-by-hop communication scenarios. Importantly, the channel parameters used in the simulations were obtained from a set of field tests at 5.9 GHz in different environments. Our performance evaluations show that the proposed data collection mecha-

nism gets better performance for delivery ratio and delay when the DSR routing protocol is used.

5. A LIGHT-WEIGHT SOLUTION FOR BLACKHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

WSNs have been started to used in many areas since they have collaborative and low-cost nature and the improvements in wireless communication technology is started to increase (Al-Karaki & Kamal 2004, Akyildiz et al. 2002). Possible applications of WSNs include the following (Dener 2017, Rashid & Rehmani 2016, Puccinelli & Haenggi 2005):

Agriculture, air pollution monitoring, animal tracking, chemical leakage detection in rivers, commercial asset tracking, earthquake early detection, environmental monitoring, forest fire detection, gas monitoring, gully pot monitoring, healthcare applications, precipitation monitoring, roadside and transportation applications, smart grid, smart lighting, smart parking, smart roads, snow level monitoring, solid waste monitoring, surveillance, traffic congestion and vehicular communication applications.

While the applications of WSNs are increasing, the number of potential attacks against them are also increasing. Certain applications of WSNs process and communicate critical/sensitive information that should not be eavesdropped and changed by illegitimate malicious nodes. With this study, a secure routing protocol has been proposed for WSNs to make communication between the source and destination nodes more reliable.

In this study, some modifications have been made on the AODV routing protocol, mostly preferred in WSNs, to make data communication more reliable. The proposed routing protocol is shown to be capable of detecting and eliminating malicious blackhole nodes. It also secures the transmitted data.

5.1 PROPOSED SECURE ROUTING PROTOCOL

In the WSN protocol stack, there are five layers and each layer has a different responsibility (Du & h. Chen 2008, Tomić & McCann 2017). The protocol stack and possible

attacks at each layer are given in Table 5.1 and summarized as follows:

i Data aggregation and interactions with the end user are performed at the **application layer**. The clone attack (Jaballah et al. 2018) is a possible attack applied at this layer.

ii Reliable data transfer is performed at the **transport layer**. The data integrity attack (Zhao et al. 2017), energy drain attack and flooding attack (Sicari et al. 2018) are possible attacks at this layer.

iii Routing for data communication is performed at the **network layer**. The blackhole attack (Panos et al. 2017, Deshmukh et al. 2016, Liu et al. 2016, Jain & Khuteta 2015, Patidar & Dubey 2014), replay attack (Hsueh et al. 2015), selective forwarding attack, grayhole attack (Pu & Lim 2018), wormhole attack (Li et al. 2018) and hello flood attack (Mahajan et al. 2016) are performed at this layer.

iv Medium access and error control for transmitted data are performed at the **data link layer**. The intelligent jamming attack (Mokdad et al. 2015) and collision attack (Razaque et al. 2017) are possible attacks at this layer.

v Modulation and frequency/channel selection are performed at the **physical layer**. The eavesdropping attack (Zhu et al. 2017) and node tampering attack (Rani & Jayakumar 2017) are possible attacks at this layer.

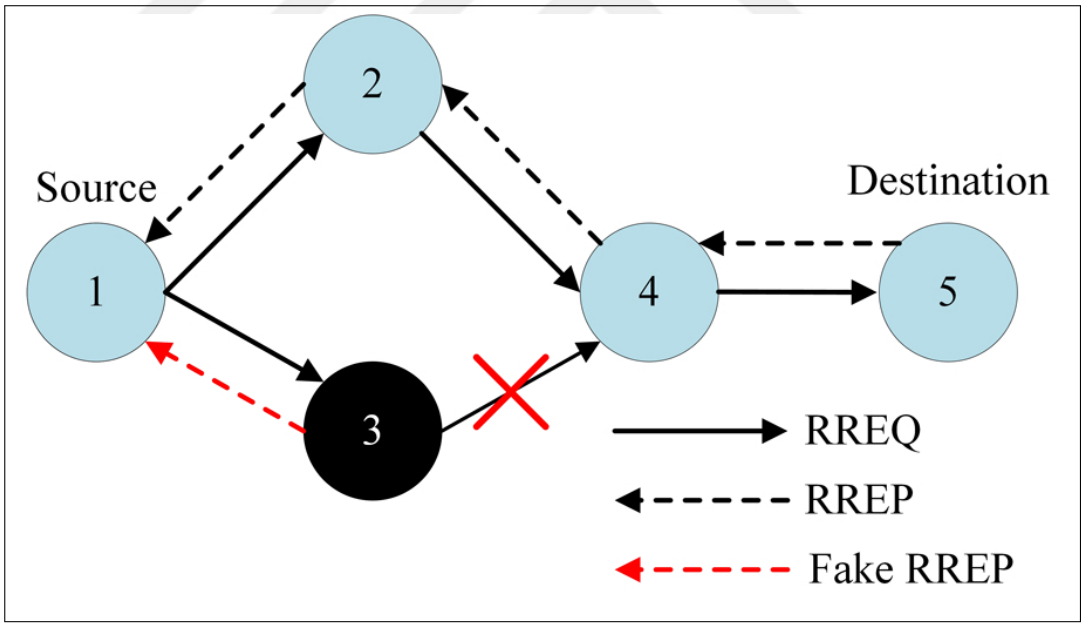
In this study, the blackhole node attack, which is a popular network layer attack, is focused on. The blackhole node attack aims at misleading source nodes. In this attack, a malicious node in the network, named as blackhole node, claims that it is the owner of the shortest path to the destination node. Thus, all data packets are directed to the malicious node to be forwarded by it to the destination node. However, when a data packet is received by the malicious node, it just drops the packets without transmitting it to the destination node (Elmahdi et al. 2018, Kaurav & Kumar 2017, Panos et al. 2017, Deshmukh et al. 2016, Liu et al. 2016, Jain & Khuteta 2015, Kumar & Kumar 2015, Patidar & Dubey 2014).

Table 5.1: Classification of attacks on WSNs according to the protocol stack layer

Layer name	Possible attacks
Application layer	Clone attack (Jaballah et al. 2018)
Transport layer	Data integrity (Zhao et al. 2017), energy drain, flooding (Sicari et al. 2018)
Network layer	Blackhole attack (Panos et al. 2017, Deshmukh et al. 2016, Liu et al. 2016, Jain & Khuteta 2015, Patidar & Dubey 2014), replay attack (Hsueh et al. 2015), selective forwarding attack, grayhole attack (Pu & Lim 2018), wormhole attack (Li et al. 2018) and hello flood attack (Mahajan et al. 2016)
Data link layer	Intelligent jamming attack (Mokdad et al. 2015) and collision attack (Razaque et al. 2017)
Physical layer	Eavesdropping attack (Zhu et al. 2017) and node tampering attack (Rani & Jayakumar 2017)

An illustration of the blackhole node attack against the AODV routing protocol, a popular one for WSNs, is shown in Figure 5.1.

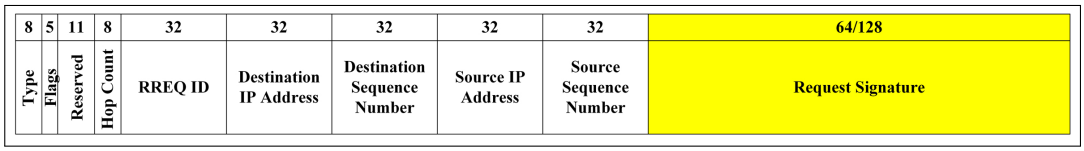
Figure 5.1: Blackhole node attack against the AODV routing protocol



In the existing AODV routing protocol, when the source node wants to transmit a packet to the destination side, firstly a RREQ packet is broadcasted to neighbors of source node to discover the route. Then the intermediate nodes (neighbor nodes) check their route tables to see whether they have a route to the destination. If one of the intermediate nodes has a

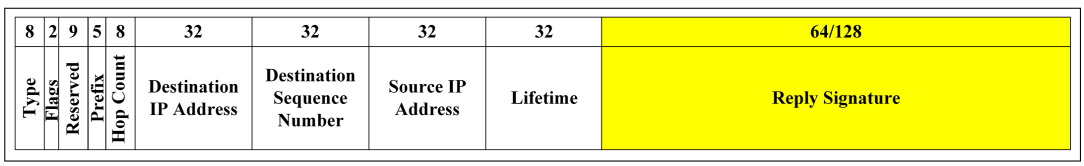
valid route, it immediately transmits a RREP packet. Otherwise, it forwards the received RREQ to its neighbors. This situation goes on until the RREQ packet is received by the destination node. When the RREQ packet is received by the destination node, a RREP packet is transmitted which is forwarded all the way back to the source node (Perkins & Royer 1999). This algorithm is the underlying mechanism of the AODV protocol.

Figure 5.2: Proposed AODV RREQ packet format



With this study, a new mechanism is proposed for the AODV routing protocol which increases the security of the original AODV protocol by including a signature to the RREQ and RREP packets. The proposed protocol, named as the Secure AODV (SAODV), mitigates the blackhole node attack. As shown in Figures 5.2 and 5.3, the additional 64-bit or 128-bit signature value fields "Request Signature" and "Reply Signature" are included to the original RREQ and RREP packets, respectively. The signature is generated by encrypting the 32-bit source IP address of the node using the Advanced Encryption Standard (AES) (with 128-bit message size) or SPECK64 (with 64-bit message size). Furthermore, in order to prevent replay attacks, the 32-bit destination sequence number is used as the nonce value and padded to the 32-bit source IP address before applying encryption. It is assumed that the shared secret key that is used for encryption. It is assumed that the shared secret key that is used for encryption/decryption is stored inside the secured tamper-resilient memory of each node during the chip manufacturing process.

Figure 5.3: Proposed AODV RREP packet format



In the proposed scheme, when the source node wants to transmit data to the destination node, it has to sign the RREQ packet before transmitting it. The 32-bit source IP address

of the node that transmits the RREQ packet, together with the 32-bit destination sequence number, is encrypted using a symmetric key cryptographic algorithm, namely the AES or the SPECK64 algorithm. The resulting 64-bit ciphertext for SPECK64, or the 128-bit ciphertext for AES, is added as the RequestSignature variable in the proposed RREQ packet format. When the RREQ packet is received by an intermediate node or the destination node, the received signature is first verified before the data is processed or relayed. If the signature is verified, either the RREQ packet is broadcasted or a RREP packet is sent back (if the verifying node is the destination node). Otherwise, the RREQ packet is discarded. Thus, authentication is achieved by controlling the signature on the RREQ packet.

On the reply side, when the destination node receives a RREQ packet, it replies back with a RREP packet. The RREP packet in SAODV includes the encrypted form of its 32-bit source IP address padded with the 32-bit destination sequence number as nonce. The nonce value is used here to prevent replay attacks. For encryption, the SPECK64 or the AES encryption algorithm is used. The resulting 64-bit ciphertext for SPECK64, or 128-bit ciphertext for AES, is added as the ReplySignature variable in the proposed RREP packet format. When an intermediate node or the source node receives the RREP packet, it first checks the received signature. If the signature is not verified, i.e. if the packet is not coming from a legitimate address, the RREP packet is discarded. Otherwise, the other operations are performed on the packet as usual. The signature control mechanism on the reply side provides the desired authentication mechanism. Figure 5.4 summarizes the proposed SAODV mechanism by showing how the RREQ and RREP packets are generated and processed.

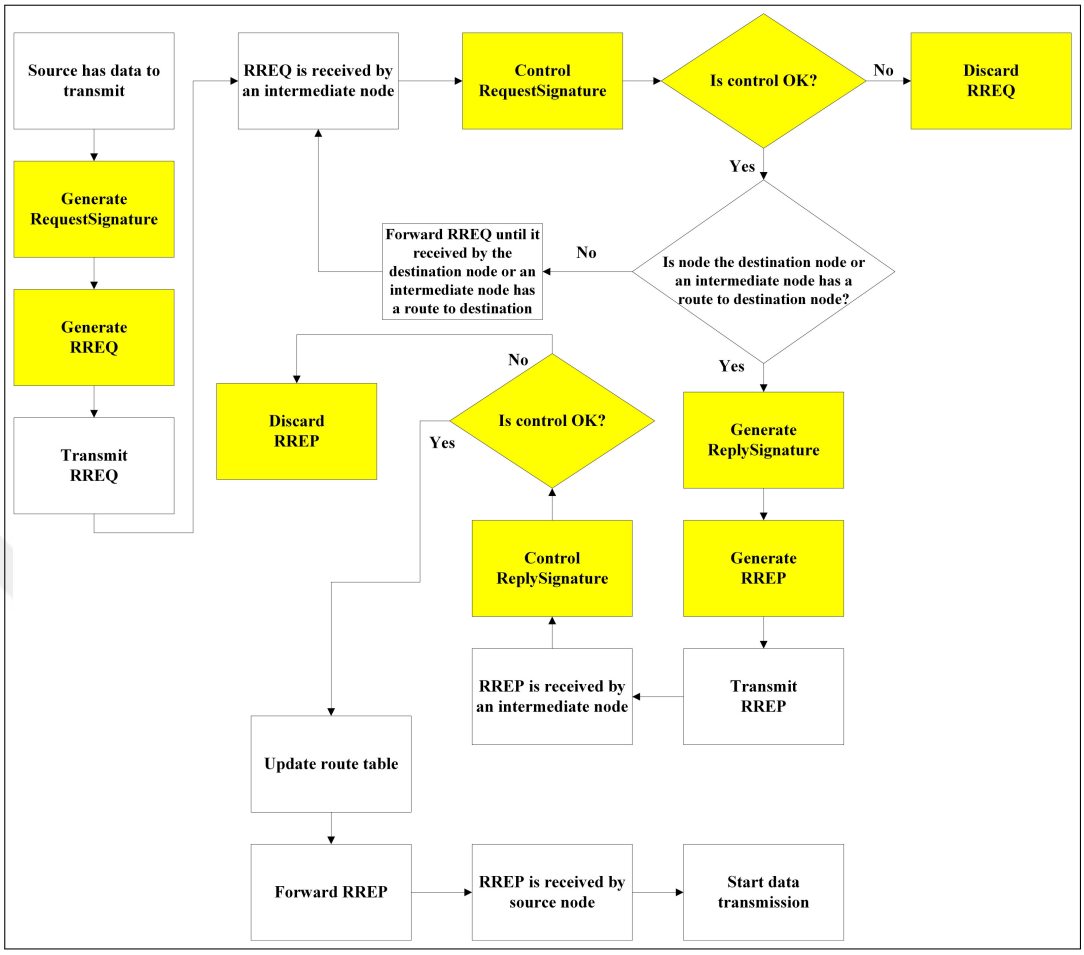
Table 5.2 summarizes the comparison of the proposed secure routing protocol with the existing solutions. In (Deshmukh et al. 2016), since the authors add only a single bit validity value in replay packets, there is no increase in the communication delay. In (Jain & Khuteta 2015), only malicious nodes send reply packets in response to dummy route requests. Therefore, this solution also does not cause extra communication delay. In (Patidar & Dubey 2014), the authors propose monitoring the system by counting the transmit-

Table 5.2: Comparison of the proposed blackhole attack prevention mechanism with the existing solutions

Solution	Delay	Usage of encryption	No single point of failure	Response and reply packets protection
SAODV	Normal	✓	✓	✓
(Deshmukh et al. 2016)	Normal	×	✓	×
(Jain & Khuteta 2015)	Normal	×	×	×
(Patidar & Dubey 2014)	High	×	✓	×
(Elmahdi et al. 2018)	High	✓	×	×
(Kaurav & Kumar 2017)	Normal	×	×	×
(Kumar & Kumar 2015)	Normal	×	✓	×

ted reply messages to start the communication between source node and destination node, which causes extra delay. In (Elmahdi et al. 2018), the authors propose sending packets to the destination by first splitting and then encrypting them. All received split message parts are first decrypted and then combined together on the destination side. The splitting and combining operation increases total end-to-end delay in the network. In (Kaurav & Kumar 2017), the base station broadcasts the list of malicious nodes to the network. This operation does not cause extra communication delay. In (Kumar & Kumar 2015), the authors propose comparing the destination sequence number with a threshold value on the route reply side. This comparison operation does not increase the communication delay. Unlike some of the existing solutions (Kaurav & Kumar 2017, Deshmukh et al. 2016, Jain & Khuteta 2015, Kumar & Kumar 2015, Patidar & Dubey 2014), the proposed solution uses an encryption mechanism to verify the validity of routing packets. Since a light-weight symmetric key encryption algorithm is used, the additional delay due to

Figure 5.4: The modified AODV mechanism



encryption/decryption operations is negligible as also pointed out in (Cazorla et al. 2015). Unlike in several of the existing solutions (Elmahdi et al. 2018, Kaurav & Kumar 2017, Jain & Khuteta 2015), there is no single point of failure in the proposed protocol. Furthermore, the proposed protocol protects both the response and reply packets in the routing protocol while existing other solutions protect only the reply packets.

5.2 NODE PLACEMENT SCENARIO

The Network Simulator-2 (ns-2) (NS-2 2011) is used to get the performance of the proposed secure AODV mechanism. In the simulations, different numbers of nodes that range between 10 and 100 and CBR traffic are used. The “setdest” function of ns-2 is

used, which is responsible to generate the positions of nodes, their moving speeds and their moving directions. The number of nodes, maximum sizes of the topology along the x and y axes (the topology boundary), simulation time, maximum speed of nodes and pause time are the parameters of this function. An example usage of the setdest function is shown as below:

setdest -v 1 -n 40 -p 1 -M 10 -t 200 -x 500 -y 500

According to this example, the topology boundary is defined as 500 $\times$ 500 with 40 nodes and the maximum speed of the nodes is 10 m/s. An illustration of the setdest function for the node placement scenario with these parameters is shown in Figure 5.5.

The "cbrgen.tcl" script is responsible for generating the traffic pattern. This script generates cbr or tcp traffic connections between nodes. The traffic connection type, number of nodes, maximum number of connections, seed value and interval rate between cbr packets are the parameters of this script. An example usage of the cbrgen.tcl script is shown as below:

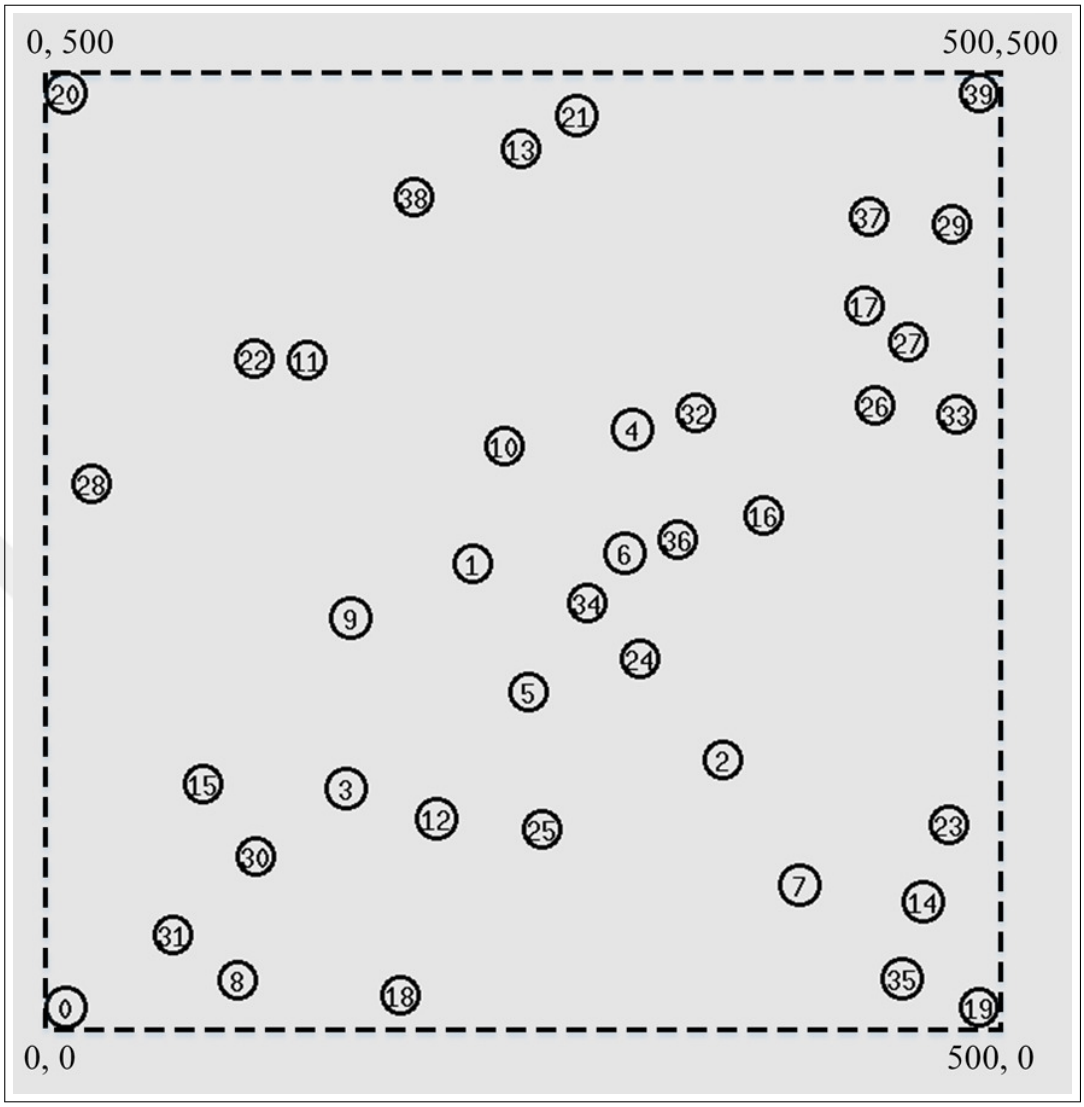
ns cbrgen.tcl -type cbr -nn 50 -seed 10 -mc 15 -rate 10.0

According to this example, a cbr type traffic is created for 50 nodes and there are 15 connections between these nodes with the seed value of 10 and the interval rate of 0.1 seconds.

5.3 PERFORMANCE RESULTS

The performance of the original AODV routing protocol is compared with the proposed secure AODV protocol in terms of average end-to-end delay and delivery ratio, for different numbers of nodes. Cbr traffic is utilized. The number of nodes in the network ranges

Figure 5.5: Node placement scenario with 40 nodes



between 10 and 100. The ratio of the number of blackhole nodes to the total number of nodes in the grid is 10 percent and 20 percent. To analyze the system statistically, seed values (time function of ctime library in c language) are choosen differently. For tis reason, 100 experiments are run with different seeds for each simulation and the average of the measured values is presented. In each experiment, different blackhole nodes are selected and different traffic connections between nodes are established. All the parameters used in the performance evaluations are listed in Table 5.3. The simulations are performed and the performance results for both the original AODV routing protocol and the proposed secure AODV routing protocol are obtained.

In the analyzed scenario for this study, only the intermediate nodes are the blackhole nodes. When the source or the destination node is a blackhole node, intermediate nodes drop the received packet since the received "Request Signature" or "Reply Signature" of the packet is not verified.

Table 5.3: Simulation parameters

Paramater Name	Value
Network simulator	Ns-2
Number of nodes	10-100
Packet size	100 bytes
Traffic type	CBR
Queue type	Drop tail
Routing protocols	AODV, SAODV
Blackhole ratio	10% and 20% of nodes in the grid
Encryption algorithms	AES, SPECK64
Encryption and decryption time in AES	1.30 ms 1.55 ms (Cazorla et al. 2015)
Encryption and decryption time in SPECK64	0.55 ms 0.42 ms (Cazorla et al. 2015)
Experiment number for each simulation	100
Seed value	Time function

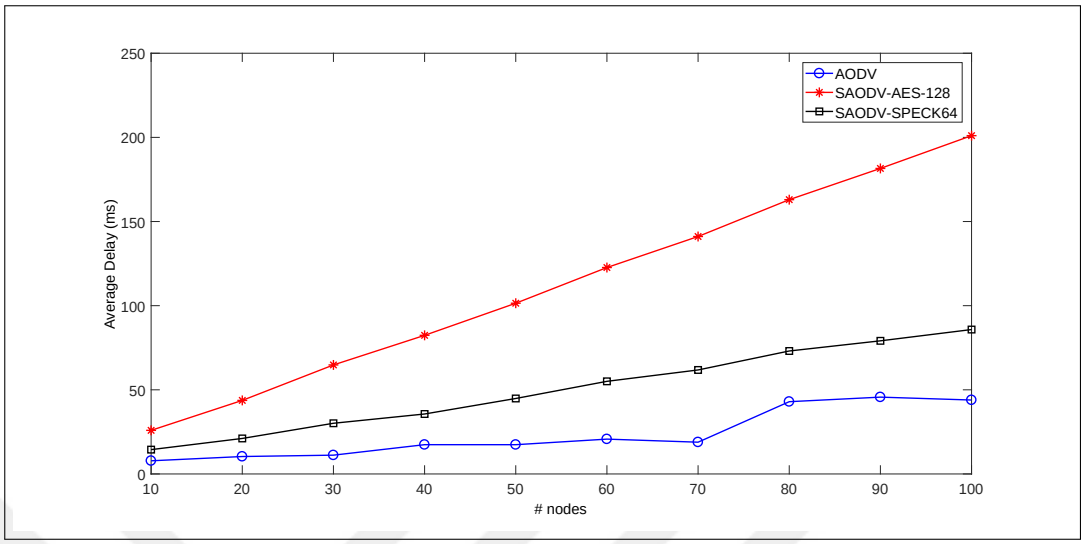
The performance metrics that are used in the performance evaluations are described as follows:

i **Average end-to-end delay** the average of the total time to transmit all packets from source to destination side.

ii **Delivery ratio** means the ratio of the successfully received packets on the destination side to all packets generated on source side.

Figure 5.6 shows the average end-to-end delays for the original AODV protocol and the proposed SAODV protocol with AES and SPECK64 when there are no blackhole nodes in the grid. As shown in Figure 5.6, the end-to-end delay increases for both AODV and SAODV routing protocols when the number of nodes increases. Since there are no blackhole nodes in the grid, the source nodes try to transmit their data to the destination nodes and it takes a longer time for all the data to be transmitted when the number of

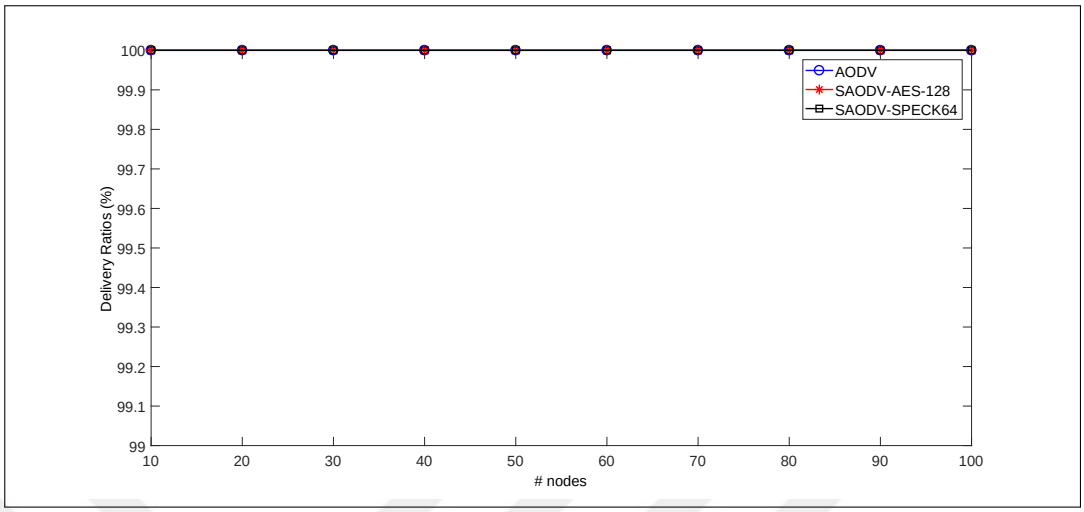
Figure 5.6: Average end-to-end delays when there are no blackhole nodes in the grid: (a) original AODV protocol, (b) SAODV protocol



nodes increases. The average end-to-end delay ranges between 7.82 ms and 43.93 ms with an average of 23.62 ms for the AODV routing protocol without blackhole nodes. For the proposed SAODV routing protocol, when there are no blackhole nodes in the grid, the average end-to-end delay (including the encryption and decryption timings) for all transmissions ranges between 25.91 ms and 201.03 ms, with an average of 112.76 ms, when AES is used. For the proposed SAODV routing protocol without blackhole nodes, the average end-to-end delay (including the encryption and decryption timings) for all transmissions changes between 14.46 ms and 85.81 ms, with an average of 50.1 ms, when SPECK64 is used. The proposed SAODV routing protocol, with SPECK64 or AES, results in slightly higher end-to-end delay values compared to the AODV routing protocol when there are no blackhole nodes in the grid. This is because of the additional processing time and increased transmission and propagation delays due to increased message size.

Figure 5.7 shows the delivery ratios for the original AODV routing protocol and the proposed SAODV routing protocol (with AES and SPECK64) when there are no blackhole nodes in the grid. As shown in Figure 5.7, for both AODV and SAODV (with AES or SPECK64), all transmitted data packets are successfully received by the destination nodes. The delivery ratio is 100 percent for both the AODV and the proposed SAODV

Figure 5.7: Delivery ratios when there are no blackhole nodes in the grid: (a) original AODV protocol, (b) SAODV protocol



routing protocols when there are no blackhole nodes in the grid.

Figure 5.8: Average end-to-end delays for the (a) Original AODV protocol, (b) SAODV protocol, in the existence of blackhole nodes in the grid

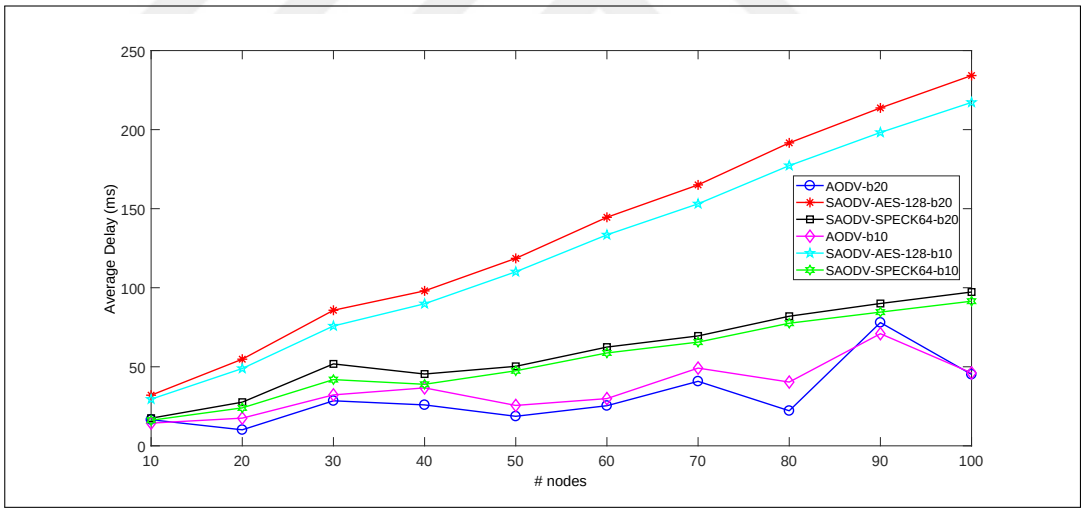
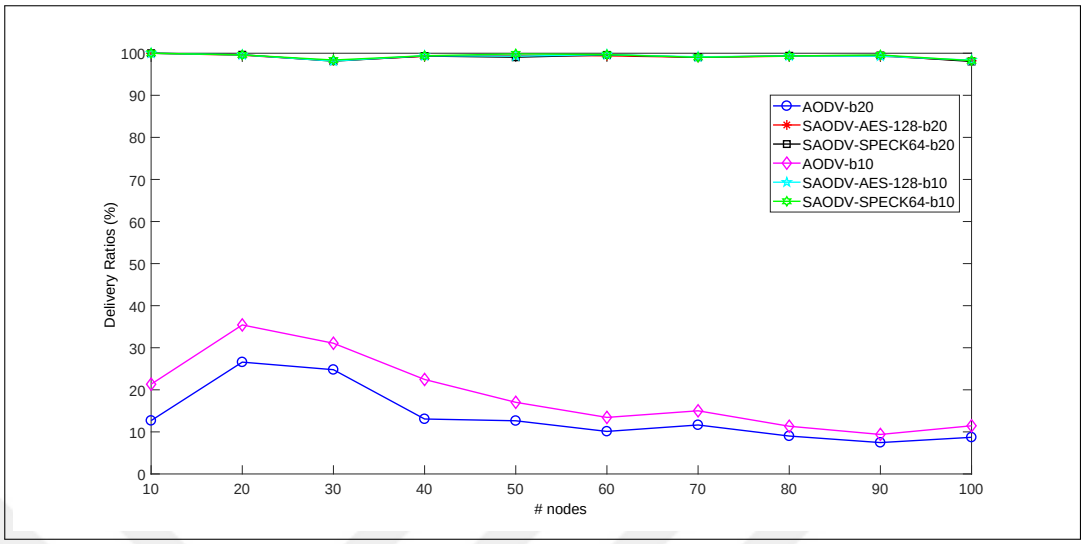


Figure 5.8 shows the average end-to-end delays for the original AODV protocol and the proposed SAODV protocol with AES and SPECK64 in the existence of blackhole nodes in the grid. As shown in the Figure 5.8, for both the AODV and SAODV routing protocols, the end-to-end delay increases when the number of nodes in the network increases. Since there exist blackhole nodes in the grid, the blackhole nodes try to mislead the source nodes to drop all transmitted packets by immediately sending them reply packets. In the

existence of blackhole nodes in the grid, the original AODV routing protocol has lower end-to-end delay than the proposed SAODV routing protocol. This is due to the fact that responses from blackhole nodes are transmitted to source nodes immediately (fake routes are established between source nodes and blackhole nodes) and there is no mechanism to check the validity of the received responses. The average end-to-end delay ranges between 14.36 ms and 70.92 ms, with an average of 36.27 ms, for the AODV routing protocol in the existence of blackhole nodes accounting for 10 percent of all the nodes in the grid. When the blackhole ratio is 20 percent, the average end-to-end delay ranges between 16.5 ms and 77.98 ms, with an average of 31.12 ms, for the AODV routing protocol. When the blackhole nodes ratio is 10 percent and AES is used, the average end-to-end delay plus encryption and decryption time for all transmissions ranges between 29.5 ms and 217.22 ms, with an average of 123.33 ms, for the proposed SAODV routing protocol in the existence of blackhole nodes. For the proposed SAODV routing protocol in the existence of blackhole nodes accounting for 20 percent of all the nodes in the grid, the average end-to-end delay plus encryption and decryption time for all transmissions ranges between 32.03 ms and 234.21 ms, with an average of 133.83 ms when AES is used. When the blackhole nodes ratio is 10 percent and the proposed SAODV routing protocol is used with SPECK64, the average end-to-end delay plus encryption and decryption time for all transmissions ranges between 16.16 ms and 91.48 ms, with an average of 54.64 ms. When the proposed SAODV routing protocol is used with SPECK64, and in the existence of blackhole nodes with 20 percent blackhole nodes ratio, the average end-to-end delay plus encryption and decryption time for all transmissions ranges between 17.48 ms and 97.28 ms, with an average of 59.39 ms. Since the proposed SAODV routing protocol tries to find new routing paths to eliminate the blackhole nodes and increase the delivery ratio, it has higher end-to-end delay compared to the original AODV routing protocol.

Figure 5.9 shows the delivery ratios for the original AODV protocol and the proposed SAODV protocol with AES and SPECK64 in the existence of blackhole nodes in the grid. As shown in Figure 5.9, the delivery ratio decreases down to 9.39 percent for the AODV routing protocol when there are 10 percent blackhole nodes in the grid. The delivery ratio

Figure 5.9: Delivery ratios for the (a) Original AODV protocol, (b) SAODV protocol, in the existence of blackhole nodes in the grid



ranges between 9.39 percent and 35.42 percent and the average delivery ratio is 18.79 percent for the AODV routing protocol when 10 percent of all nodes are blackhole nodes. When the blackhole nodes ratio is 20 percent, the delivery ratio decreases down to 7.46 percent for the AODV routing protocol. The delivery ratio ranges between 7.46 percent and 26.58 percent and the average delivery ratio is 13.67 percent for the AODV routing protocol. When the AODV protocol was tested, it was observed that the delivery ratio continued to increase until the number of nodes reached 20 and then started decreasing. The number of connection for each simulation is 60 percent of all nodes. When the number of node is 10, the number of connection between nodes is 6 and the number of connection is 12 for 20 nodes and etc. Since the number of connection is minimum when number of nodes is 10, the delivery ratio is lower compared to 20 nodes. Although the number of connections between the nodes increases with the number of nodes, when the number of nodes exceeds 20, the increase in the number of blackhole nodes causes the delivery ratio to decrease. For the proposed SAODV routing protocol with AES, when the blackhole nodes ratio is 10 percent, the delivery ratio ranges between 98.14 percent and 100.00 percent and the average delivery ratio is 99.22 percent. When the blackhole nodes ratio is increased to 20 percent, the delivery ratio ranges between 98.21 percent and 100.00 percent and the average delivery ratio is 98.21 percent. When the proposed SAODV

routing protocol with SPECK64 is used and the blackhole nodes ratio is 10 percent, the delivery ratio ranges between 98.24 percent and 100 percent and the average delivery ratio is 99.31 percent. When the blackhole nodes ratio is increased to 20 percent, the delivery ratio ranges between 98.04 percent and 100 percent and the average delivery ratio is 99.17 percent. The proposed SAODV routing protocol, with AES or SPECK64, has higher delivery ratio compared to the AODV routing protocol in the existence of blackhole nodes in the grid. This shows that the proposed mechanism eliminates the blackhole nodes and increases the delivery ratio by establishing new routing paths. The all results for all routing protocols are listed in Table 5.4.

Table 5.4: Results for all nodes and routing protocols

Routing Protocol	Number of nodes									
	10	20	30	40	50	60	70	80	90	100
AODV blackhole ratio 10	21.33	35.42	31.07	22.46	17.03	13.44	15.01	11.34	9.39	11.45
AODV blackhole ratio 20	12.68	26.58	24.78	13.06	12.64	10.11	11.64	9.01	7.46	8.71
SAODV-AES blackhole ratio 10	100	99.6	98.14	99.41	99.3	99.67	99.15	99.36	99.3	98.35
SAODV-AES blackhole ratio 20	100	99.52	98.22	99.26	99.51	99.38	99.03	99.29	99.31	98.21
SAODV-SPECK64 blackhole ratio 10	100	99.61	98.39	99.4	99.84	99.68	99.04	99.35	99.59	98.24
SAODV-SPECK64 blackhole ratio 20	100	99.64	98.12	99.33	99.05	99.6	99.05	99.4	99.47	98.04

5.4 DISCUSSION

In this study, the problem of blackhole node attacks on WSNs is addressed by proposing a secure routing protocol. The protocol is an improved version of the commonly used AODV routing protocol for WSNs. Added mechanism to the original AODV routing protocol helps detect and discard blackhole nodes in the network. The performance of the proposed secure routing protocol is evaluated and compared against the original AODV protocol in terms of average end-to-end delay and delivery ratio. The comparative performance evaluations prove that, by detecting and discarding the blackhole nodes in the network, the proposed mechanism increases the delivery ratio without causing too much extra delay.

6. A SECURE MECHANISM FOR DATA COLLECTION FROM SMART METERS VIA PUBLIC TRANSPORTATION

WSNs have started being used in many environments with the advances in MEMS. A WSN contains lots of sensor nodes which are cheap, small and have limited resources. The collaborative features of sensor nodes facilitate their use in a variety of application areas, including biomedical health monitoring, home applications, hazardous environment sensing, military and surveillance applications, smart grid applications and vehicular communications (Yick et al. 2008, Akyildiz et al. 2002).

In this study, we address the reliability issue for data collection mechanisms in smart meters and propose improvements in earlier studies (Bilgin et al. 2016b,a). We use an enhanced version of the AODV protocol which discards malicious blackhole nodes from the network. Although in earlier studies (Bilgin et al. 2016b,a), DSR routing protocol has better results in terms of average end-to-end delay, we prefer working on AODV routing protocol since it is preferable in the literature on blackhole attack studies compared to DSR.

6.1 ATTACKS IN WIRELESS SENSOR NETWORKS

There are different types of attacks in WSNs. Attacks against WSNs can be classified according to their exploited WSN protocol stack (Tomić & McCann 2017, Du & h. Chen 2008). The WSN protocol stack is summarized as follows and possible attacks for each layer are summarized in Table 5.1.

i **Application layer** is responsible for data aggregation and interacts with the end user.

ii **Transport layer** is responsible for reliable data transfer.

iii **Network layer** is responsible for providing routing paths for data communication.

iv **Data link layer** is responsible for medium access and deals with transmission errors.

v **Physical layer** is responsible for modulation and frequency/channel selection.

In the clone attack, a node in the network is caught by the intruder and thus the attacker acquires all the information, such as ID and cryptographic information, to fabricate clone nodes (Jaballah et al. 2018).

In the data integrity attack, the attacker attempts to listen to the channel to sniff messages transmitted between the sender and receiver. Then, the attacker tries to alter the messages to cause data loss or obtain sensitive information (AL-Mousawi & AL-Hassani 2017, Zhao et al. 2017).

In the energy drain and flooding attack, the attacker generates fake requests to exhaust the resources of the nodes in the network. This causes victim nodes to stay in active mode continuously and thus their energy is wasted (Abidoye & Obagbuwa 2018, Sicari et al. 2018).

In the replay attack, the malicious node eavesdrops messages transmitted in the network and fraudulently retransmits or repeats them (Hwang & Huang 2017, Hsueh et al. 2015).

In the selective forwarding and grayhole attack, the malicious nodes in the network drop some of the packets randomly. This damages data integrity in sensitive applications and decreases the delivery ratio. The main target of this attack is multi-hop WSNs (Pu & Lim 2018, Schweitzer et al. 2017, Ren et al. 2016).

In the wormhole attack, a special path called as the wormhole tunnel is created by at least two malicious nodes. The source node is deceived by one of these malicious nodes which would claim it has a shorter path to the destination. In this attack, malicious nodes transmit the data to the destination without modifying it but they listen to all the data traffic between the source and the destination (Li et al. 2018, Tiruvakadu & Pallapa 2018).

In the hello flood attack, the malicious node advertises hello messages with very high power to transmit them to a large distance. This causes energy loses and collisions in victim nodes (Mahajan et al. 2016, Haghighi et al. 2011).

In the intelligent jamming attack, the malicious node generates interferences. Since the nodes share the wireless medium, this prevents victim nodes from transmitting and receiving messages reliably (Zou et al. 2016, Mokdad et al. 2015).

In the collision attack, the attacker node prevents transmissions of its neighbors by not following the medium access control protocol. This causes packet drops in the network (Razaque et al. 2017, Reindl et al. 2010).

In the eavesdropping attack, the attacker sniffs the communication channel and obtains all the transmitted traffic which is possible due to the broadcast nature of radio propagation. The attacker in this scenario would be capable of reading the transmitted messages and also corrupting them (Zhu et al. 2017, Li et al. 2015).

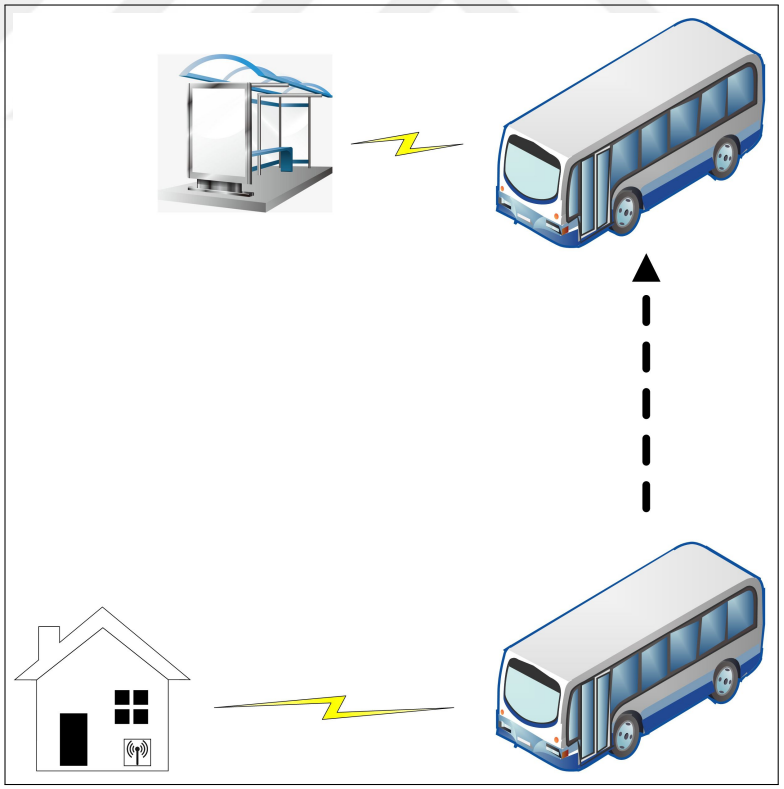
In the node tampering attack, a node in the network is captured and then it is reprogrammed or refabricated (Rani & Jayakumar 2017, Mishra & Turuk 2016).

In this study, network layer attacks are focused on, in particular blackhole node attack. The blackhole node attack targets the AODV routing protocol. In this attack, a malicious node in the network, known as blackhole node, claims that it has the shortest path to the destination node by manipulating the AODV parameters. Thus, the blackhole node attracts route request packets from other nodes and drops the received packets without transmitting them to its neighboring nodes or the destination node (Panos et al. 2017).

6.2 SECURE AODV FOR RELIABLE DATA COLLECTION IN SMART GRIDS USING PUBLIC TRANSPORTATION

A data collection mechanism for smart grids is proposed in (Bilgin et al. 2016b) where smart grid data is collected from houses through public transportation buses. In this scenario, Wireless Automatic Meter Reading (WAMR) devices, which are located in houses and enabled with the IEEE 802.11p communication protocol, transmit their data to public transportation buses passing by their neighborhood. The data collected by the public transportation bus is then forwarded to a bus stop which transmits it to the utility company or an intermediary central authority. The illustration of the proposed mechanism is shown in Figure 6.1. We propose a secure AODV mechanism for securely transmitting routing packets and eliminating blackhole nodes in the smart grid data collection with public transportation bus scenario.

Figure 6.1: Proposed data collection scheme



In this section, we propose an improved version of the AODV routing protocol, which we

call the Secure AODV (SAODV), to overcome some security problems of vehicular and smart grid networks. We apply the SAODV protocol to a data collection mechanism for smart grids that uses public transportation buses. Furthermore, we show the efficacy of the proposed protocol to detect and eliminate blackhole nodes in the network.

In the original AODV routing protocol, when data is transmitted by the source node, firstly a RREQ packet is broadcasted to its neighbors to find the route to the destination. Then, the neighbor nodes (intermediate nodes in the grid) check the received RREQ packet to see whether the packet received is sent for them. Then, the receiver control if it the destination or not. If it is not the destination, it checks its route table whether it contains a route to destination or not. If an intermediate node is the destination or if it has an active route to the destination, a RREP packet is immediately transmitted. Otherwise, the RREQ is forwarded. This loop goes on until the RREQ packet is received by the destination node. Finally, when the RREQ packet is received by the destination node, a RREP packet is transmitted to the source node (Perkins et al. 2002). In this study, we use a new mechanism that increases the security of the original AODV protocol by including a signature field to the RREQ and RREP packets. The signature is generated by encrypting the address of the node by using the SPECK64 cryptosystem (Beaulieu et al. 2015). We assume that the shared secret key that is used in the encryption algorithm is stored inside the tamper-resilient memory of every node in the network during manufacturing.

Figure 6.2: Existing AODV RREQ packet format

8	5	11	8	32	32	32	32	32
Type	Flags	Reserved	Hop Count	RREQ ID	Destination IP Address	Destination Sequence Number	Source IP Address	Source Sequence Number

Figure 6.3: Secure AODV RREQ packet format

8	5	11	8	32	32	32	32	32	64
Type	Flags	Reserved	Hop Count	RREQ ID	Destination IP Address	Destination Sequence Number	Source IP Address	Source Sequence Number	Request Signature

Figures 6.2 and 6.3 show the formats of the RREQ packet in the existing AODV protocol and the new one, respectively. As shown in Figure 6.2, the original RREQ packet has 24 bytes which consists of the 8-bit type, 5-bit flag, 11-bit reserved, 8-bit hop count, 32-bit RREQ ID, 32-bit destination IP address, 32-bit destination sequence number, 32-bit source IP address and 32-bit source sequence number fields. In the new mechanism, we add an additional 64-bit signature value field as shown in Figure 6.3. The extra bits added are generated by the SPECK64 cryptographic algorithm (Beaulieu et al. 2015) and they provide message integrity and authentication. Before starting transmission between source and destination, the RREQ packet has to be signed by including signature. We generate this 64-bit signature value by encrypting the 32-bit the source node's address, padded with the 32-bit destination sequence number which is used as the nonce value to prevent replay attacks. We call this 64-bit ciphertext that is added to the new AODV RREQ packet format as the RequestSignature variable. When an intermediate node or a destination node receives a RREQ packet, it first verifies the received signature before analyzing the packet. If the signature is not verified, i.e. if the packet is not coming from a legitimate address, it discards the RREQ packet. Thus, the signature controls on the RREQ broadcast side provide us with the desired authentication mechanism.

Figure 6.4: Existing AODV RREP packet format

8	2	9	5	8	32	32	32	32
Type	Flags	Reserved	Prefix	Hop Count	Destination IP Address	Destination Sequence Number	Source IP Address	Lifetime

Figure 6.5: Secure AODV RREP packet format

8	2	9	5	8	32	32	32	32	64
Type	Flags	Reserved	Prefix	Hop Count	Destination IP Address	Destination Sequence Number	Source IP Address	Lifetime	Reply Signature

Figures 6.4 and 6.5 show the existing and proposed AODV RREP packet formats, respec-

tively. As shown in Figure 6.4, a RREP packet is 20 bytes in size and consists of the 8-bit type, 2-bit flag, 9-bit reserved, 5-bit prefix, 8-bit hop-count, 32-bit destination IP address, 32-bit destination sequence number, 32-bit source IP address and 32-bit lifetime fields. In the new packet format, a 64-bit signature field is added to the RREP packet, where the ReplySignature variable is stored, as shown in Figure 6.5. The value of the ReplySignature variable is obtained by encrypting the 32-bit address of the node that generates the RREP packet padded with the 32-bit destination sequence number. Here, the 32-bit destination sequence number is used as the nonce value to prevent replay attacks. For the encryption operation, the SPECK64 cryptographic algorithm is used which has the block size of only 64-bit and does not create too much packet overhead. The included ReplySignature variable provides authentication on the reply side. When a RREQ packet is received by destination, it transmits a RREP packet that includes the signature value. When the RREP packet is received by an intermediate node or the source node, the received signature is checked. If the signature is verified, i.e. if the packet is coming from a legitimate address, the other operations are performed on the packet as usual. Otherwise, the packet is discarded. Algorithm 1 summarizes the proposed mechanism by showing how the RREQ and RREP packets are generated and processed.

Algorithm 1: Pseudocode of the proposed mechanism

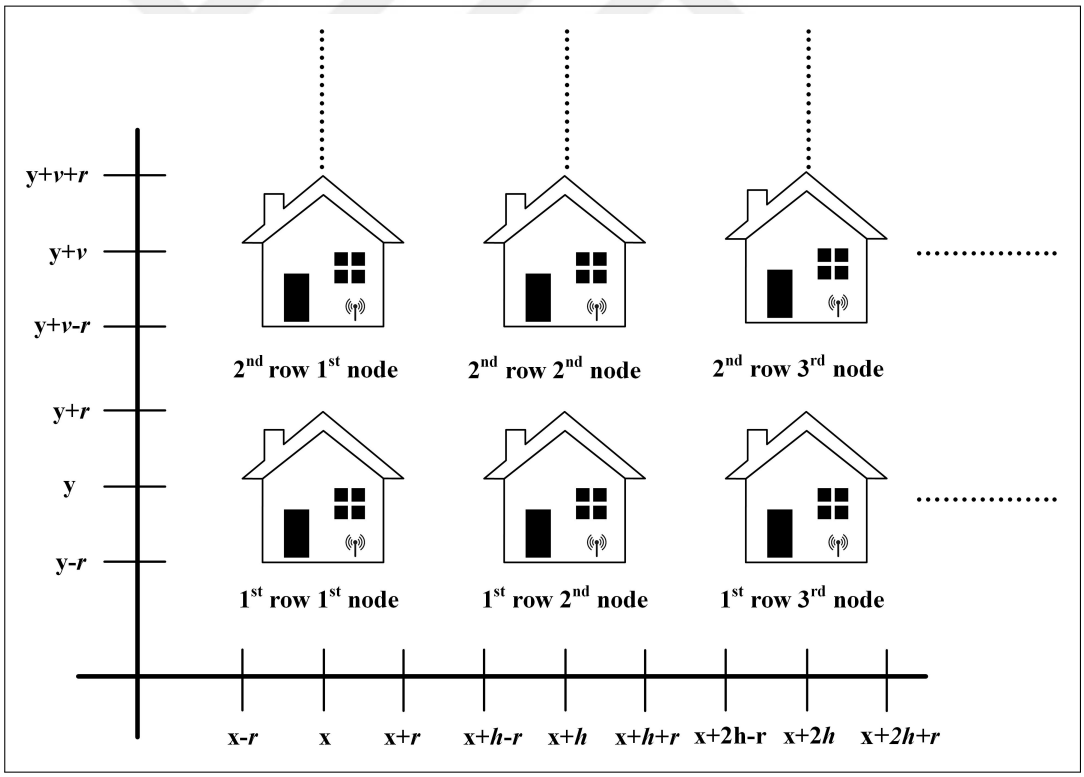
```
/* On the Request Side */
INITIALIZE RequestSignature using the SPECK64 algorithm with
 RequestPrivateKey when source node wants to transmit data
TRANSMIT RREQ packet until the packet is received by the destination node or an
 intermediate node that has a route to the destination
CONTROL RequestSignature when a RREQ packet is received
if RequestSignature is correct then
    if the node is destination or the intermediate node has route to destination then
        /* On the Reply Side */
        INITIALIZE ReplySignature using SPECK64 algorithm with
         ReplyPrivateKey TRANSMIT RREP packet to source node
        CONTROL ReplySignature
        if ReplySignature is correct then
            UPDATE Route table and Forward RREP until source node
            START data transmission
        else
            DISCARD RREP packet
        end
    else
        FORWARD RREQ packet
    end
else
    DISCARD RREQ packet
end
```

6.3 PERFORMANCE EVALUATIONS

We do our performance simulations for the SAODV mechanism in the smart grid network where smart meter data is collected by a public transportation bus passing by the neighborhood, which is the scenario given in Figure 6.1. In our simulations, we model

a neighborhood as a cluster of houses. We use different number of rows and columns in the cluster to simulate neighborhoods of varying sizes. The nodes (houses) are randomly placed in the cluster. For the placement of the nodes, we use the parameters v, h and r, where v and h represent the average vertical and horizontal distances between adjacent nodes, respectively, and r denotes the degree of randomness that is added to the placement of nodes. The unit for all these parameters is meter (m). As shown in Figure 6.6, nodes are placed according to the number of rows and columns in the cluster starting with the initial [x, y] coordinate. The first node is placed randomly within the square area [x - r to x + r, y - r to y + r] and the second node at the same row is randomly placed within [x + h - r to x + h + r, y - r to y + r]. The first node at the second row is randomly placed within [x - r to x + r, y + v - r to y + v + r]. The other nodes are placed similarly using the same procedure.

Figure 6.6: Node placement scenario



We perform our simulations using the Network Simulator (ns-2) (NS-2 2011) to evaluate the performance of the proposed secure AODV mechanism for different number of nodes

in urban environment. In our simulations, CBR traffic is utilized. The speed of the bus is randomly selected between 45-55 km/h. The ratio of the blackhole nodes in the grid is 20 percent. All the parameters applied in the performance evaluations are listed in Table 6.1. We perform our simulations for both the AODV routing protocol and the SAODV routing protocol, and compare their performances. To achieve more realistic results, we run 10 experiments for each simulation using different seed values and present the average of the results. Besides, 20 percent of all the nodes are randomly selected as blackhole nodes at each run of the simulation. The performance metrics that we have used in our performance evaluations are described as follows:

i **Average end-to-end delay** means the average of the total time to transmit all packets from source to destination side.

ii **Delivery ratio** means the ratio of the successfully received packets on the destination side to all packets generated on source side.

Table 6.1: Simulation parameters

Paramater Name	Value
Network simulator	Ns-2
Number of columns	2-20
Number of rows	2-20
Number of houses	4-400
Number of bus stops	1
Number of buses	1
Average maximum bus speed	45-55 km/h
Packet size	100 bytes
Traffic type	CBR
Queue type	Drop tail
Routing protocols	AODV, SAODV
Blackhole ratio	20% of nodes in the grid
Encryption algorithm	SPECK64
Encryption and decryption time in SPECK64	0.55 ms 0.42 ms (Cazorla et al. 2015)

6.3.1 PERFORMANCE RESULTS

For urban environment, we consider a neighborhood with a high population density. Therefore, we select the v, h and r parameters in our node placement scenario as 20, 20 and 10, respectively, which results in a population density of 2500 houses/km^2.

Figure 6.7: Average end-to-end delays with the (a) original AODV protocol, (b) SAODV protocol for the proposed smart grid network scenario when there are no blackhole nodes in the grid

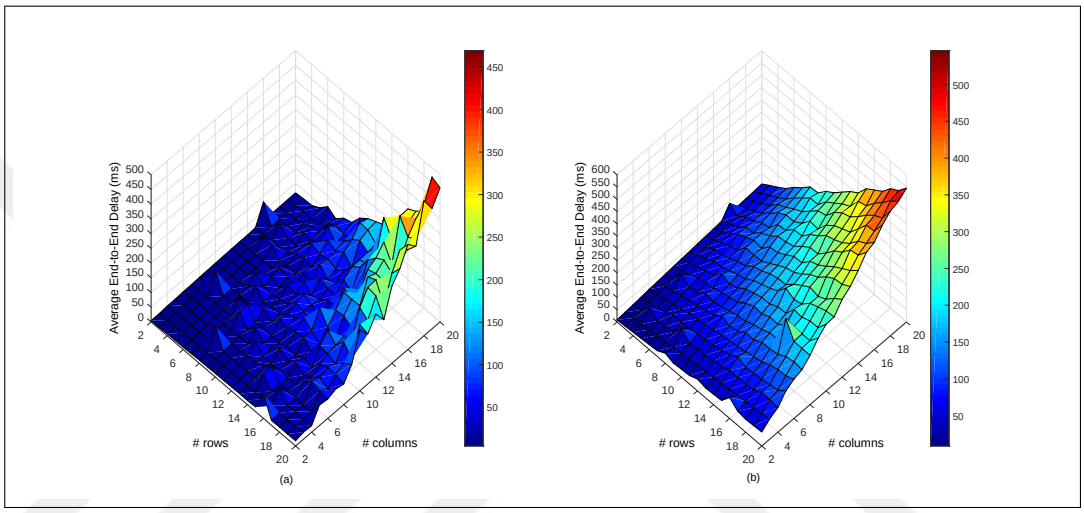


Figure 6.7 shows the average end-to-end delays from the houses to the bus in the urban environment scenario with the AODV protocol and the proposed SAODV protocol when there are no blackhole nodes in the grid.

As shown in Figure 6.7, the end-to-end delay increases with both the original AODV and the SAODV routing protocols when the number of nodes increases. In this scenario, there are no blackhole nodes in the grid, therefore, the source nodes try to transmit their data to the destination nodes and this causes longer time for all the data to be transmitted when the number of nodes increases. For the original AODV routing protocol, the average end-to-end delay varies between 4.48 ms and 469.1 ms for different number of nodes and the average is 74.96 ms. For the proposed SAODV routing protocol, the average end-to-end delay (including the encryption and decryption timings) varies between 8.73 ms and 545.83 ms with an average value of 159.11 ms. The proposed SAODV routing

protocol has a slightly higher end-to-end delay compared to the AODV protocol due to the encryption/decryption operations and increased message size.

Figure 6.8: Minimum (i), maximum (ii) and average (iii) of average end-to-end delays with the (a) original AODV protocol, (b) SAODV protocol for the proposed smart grid setting when there are no blackhole nodes in the grid

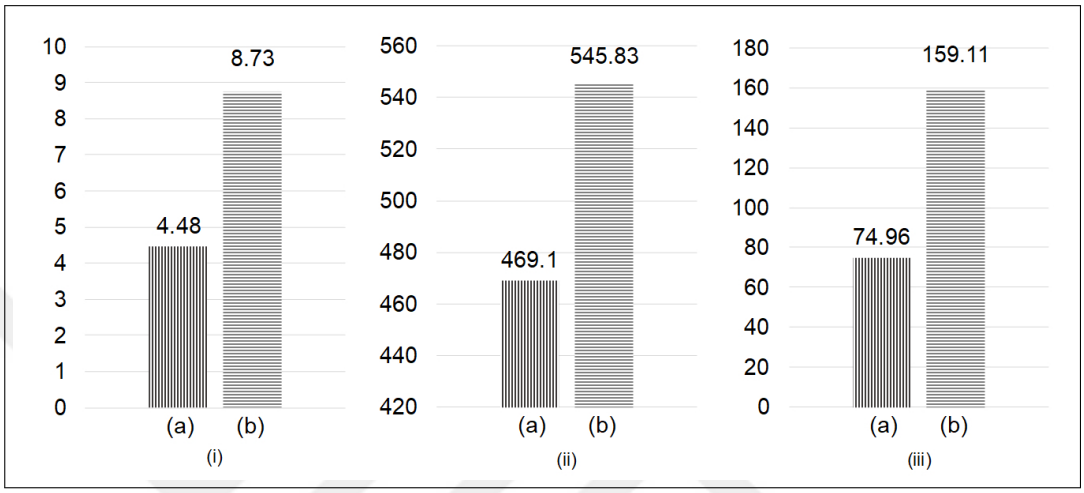
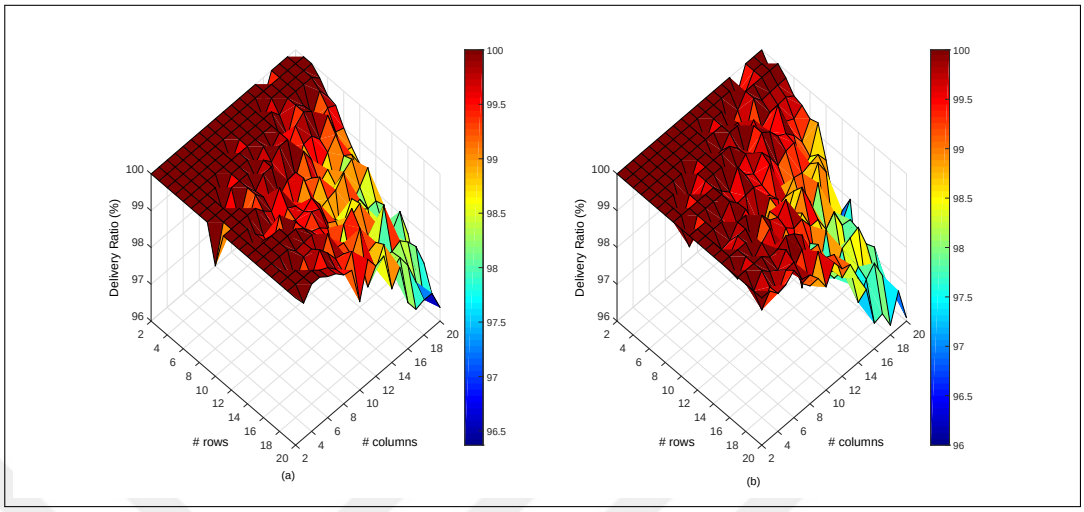


Figure 6.8 shows the minimum, maximum and average of average end-to-end delays with the AODV protocol and the proposed SAODV protocol. As shown with the simulation results, the proposed SAODV routing protocol has slightly higher average end-to-end delay than the original AODV protocol because of the additional processing time and increased transmission and propagation delays due to increased message size.

Figure 6.9 shows the delivery ratios from the houses to the bus with the original AODV protocol and the proposed SAODV protocol when there are no blackhole nodes in the grid.

As shown in the Figure 6.9, with the original AODV and the SAODV, the delivery ratio decreases when the number of nodes increases. Both the original AODV and the proposed SAODV result in almost the same average delivery ratio. The delivery ratio varies between 96.37 percent and 100 percent and the average delivery ratio for all scenarios is 99.39 percent for the AODV routing protocol. For the SAODV routing protocol, the delivery ratio varies between 96 percent and 100 percent and the average delivery ratio

Figure 6.9: Delivery ratios in the urban environment scenario with the (a) original AODV protocol, (b) SAODV protocol for the proposed smart grid setting when there are no blackhole nodes in the grid



for all scenarios is 99.28 percent. Note that when there are no blackhole nodes in the grid, in the proposed mechanism, the delivery ratio is almost the same compared to the original AODV mechanism.

Figure 6.10: Minimum (i), maximum (ii) and average (iii) delivery ratios with the (a) original AODV protocol, (b) SAODV protocol, in the proposed smart grid setting when there are no blackhole nodes in the grid

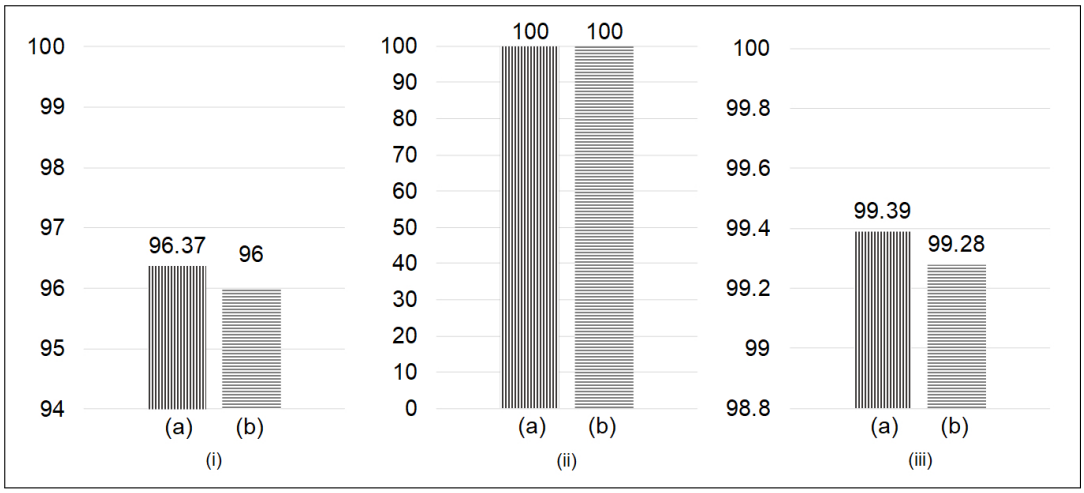


Figure 6.10 shows the minimum, maximum and average delivery ratios with the original data collection mechanism with AODV and the proposed mechanism with SAODV. As

shown in Figure 6.10, the delivery ratio is almost the same with the original AODV and the proposed mechanism with blackhole node protection.

Figure 6.11: Average end-to-end delays for the (a) original AODV protocol, (b) SAODV protocol with SPECK64 in urban environment in the existence of blackhole nodes in the grid

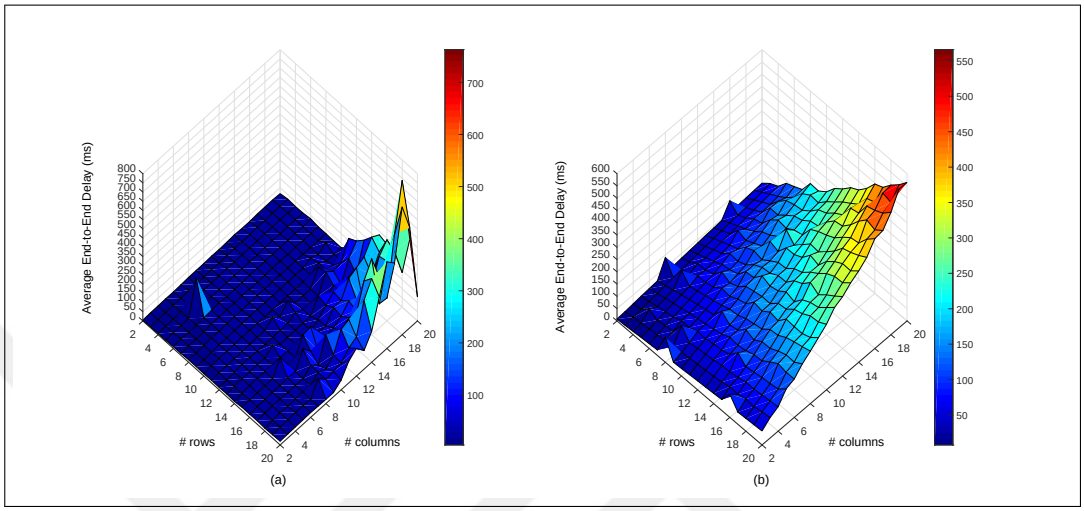


Figure 6.11 shows the average end-to-end delays from the houses to the bus with the original data collection mechanism with AODV and the proposed mechanism with SAODV in the existence of blackhole nodes in the grid.

As seen in the Figure 6.11, the end-to-end delay increases with both original AODV and SAODV routing protocols when the number of nodes increases. In this scenario, there exists blackhole nodes in the grid and the responses from blackhole nodes are transmitted to source nodes immediately. Therefore, the original AODV routing protocol has lower end-to-end delay compared to the proposed SAODV routing protocol. On the other hand, the proposed SAODV routing protocol tries to check the validity of the received responses and drops the fake requests and responses. Therefore, the proposed SAODV protocol has higher end-to-end delay than the original AODV protocol. For the original data collection mechanism with the AODV routing protocol, the average end-to-end delay varies between 4.08 ms and 762.75 ms for different number of nodes and the average is 63 ms. For the proposed data collection mechanism with the SAODV, the average end-to-end delay (including encryption and decryption timings) for all transmissions varies between 7.69 ms

and 565.78 ms and the average for all scenarios is 162.28 ms. The proposed mechanism has a slightly higher end-to-end delay compared to the original one since new routing paths are formed to eliminate the blackhole nodes.

Figure 6.12: Minimum (i), maximum (ii) and average (iii) of average end-to-end delays for the (a) original AODV protocol, (b) SAODV protocol with SPECK64 in urban environment in the existence of blackhole nodes in the grid

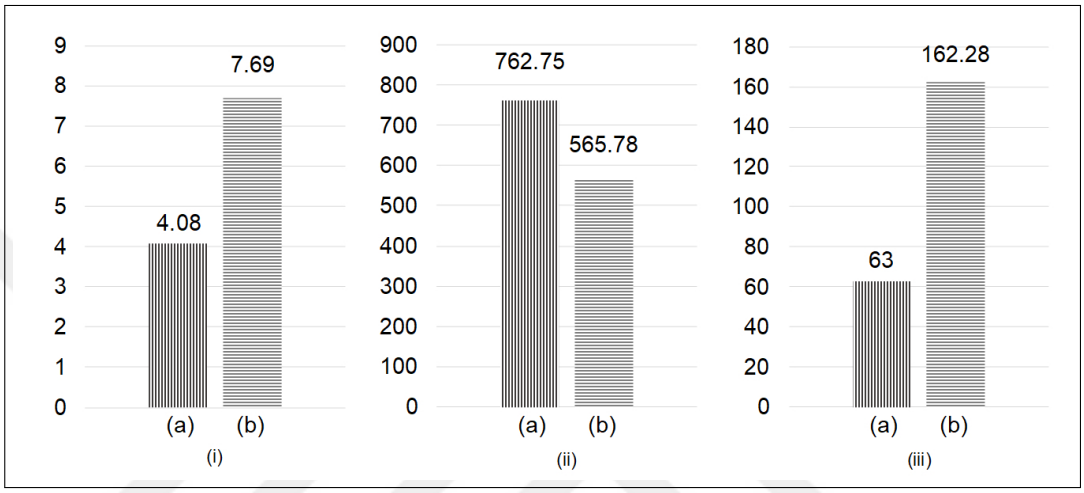
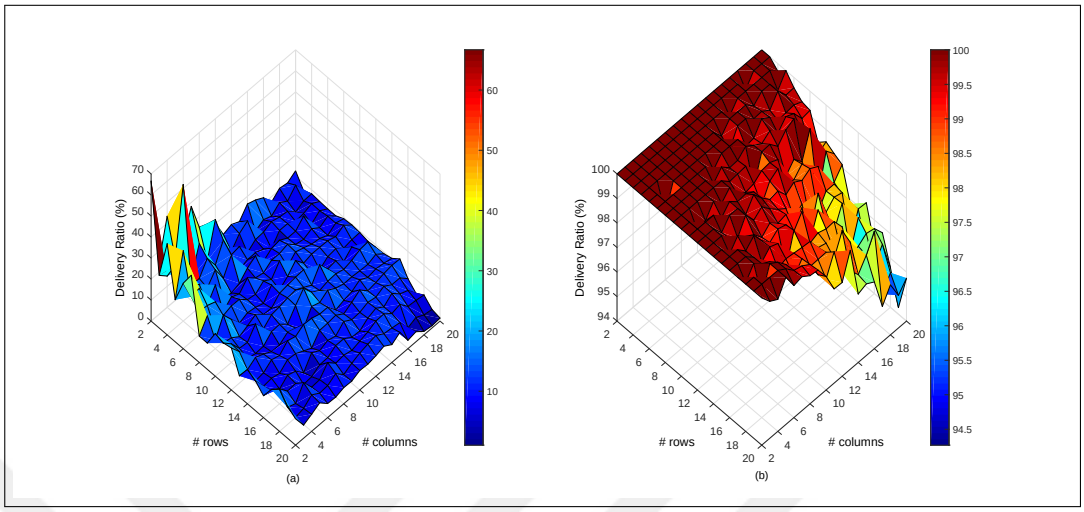


Figure 6.12 shows the minimum, maximum and average of average end-to-end delays with the original data collection mechanism with AODV and the proposed mechanism with the SAODV. As shown with our simulation results, the proposed mechanism has slightly higher average end-to-end delay than the original one because of the additional processing time and increased transmission and propagation delays since it tries to increase the delivery ratio by eliminating the blackhole nodes.

Figure 6.13 shows the delivery ratios from the houses to the bus with the original AODV protocol and the proposed mechanism with SAODV in the existence of blackhole nodes in the grid.

As shown in Figure 6.13, with both routing protocols, the delivery ratio decreases when the number of nodes increases. The delivery ratio decreases down to 1.05 percent with the AODV routing protocol. The delivery ratio varies between 1.05 percent and 66.67 percent and the average delivery ratio is 12.18 percent with the AODV routing protocol.

Figure 6.13: Delivery ratios in the urban environment scenario for the (a) original AODV protocol, (b) SAODV protocol with SPECK64 in urban environment in the existence of blackhole nodes in the grid



For the proposed data collection mechanism with the SAODV, the delivery ratio varies between 94.27 percent and 100 percent and the average delivery ratio for all scenarios is 99.18 percent. The proposed mechanism with SAODV results in higher delivery ratios compared to the original AODV when there are blackhole nodes in the grid. This shows that the proposed mechanism eliminates blackhole nodes and increases the delivery ratio by establishing new routing paths.

Figure 6.14: Minimum (i), maximum (ii) and average (iii) of delivery ratios with the (a) original AODV protocol, (b) SAODV protocol in the existence of blackhole nodes in the grid

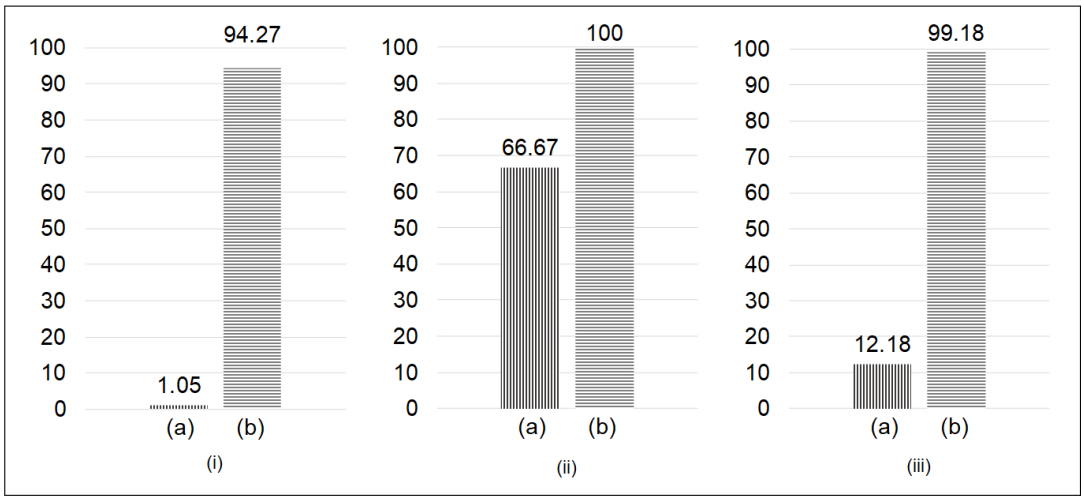


Figure 6.14 shows the minimum, maximum and average delivery ratios for the proposed reliable data collection mechanism with the original AODV and with the SAODV protocol. As shown in Figure 6.14, the delivery ratio is higher with the proposed mechanism with the SAODV, compared to the mechanism with the AODV.

6.4 DISCUSSION

With advances in wireless communications technologies, sensor networks have started being deployed widely in many applications, e.g. biomedical health monitoring, home applications, hazardous environment sensing, military and surveillance, smart grid applications and vehicular communications.

In this study, we proposed a secure and reliable solution for collecting smart grid data. Our solution combines the smart grid AMI technology with vehicular ad-hoc networks. In an earlier study, a mechanism was proposed for automatically collecting smart grid meter data and sending it to the utility company through a public transportation bus passing by and then through a bus stop. In this study, we improved upon that mechanism by using a security improved routing protocol that helps identify and eradicate blackhole nodes in the network.

We evaluated the performance of our secure routing mechanism with the original AODV protocol in terms of average end-to-end delay and delivery ratio. According to our performance evaluations, our proposed routing mechanism eliminates the malicious nodes in the network and achieves almost the same delivery ratio values as AODV routing protocol without causing extra delays and increasing request packet size only only 64-bit.

7. CONCLUSION

This thesis presents a novel solution for collecting smart meter data by merging VANET and smart grid communication technologies. Also some modifications have been made to the AODV protocol, mostly preferred in wireless sensor networks, to make data communications more reliable. Finally, these security features is added to the proposed data collecting solution to address security, privacy and reliability issues.

With this motivation, firstly, the existing AMR systems and their problems are introduced in Chapter 2.1. The communication technologies that used for these system is also presented. Then, an overview of existing security problems and solutions in WSNs is presented in Chapter 2.2. Finally, the existing security issues of smart grid and vehicular communication are presented in Chapter 2.3.

In Chapter 3, we offer a new data collecting mechanism by extending the communication capability of smart meters to IEEE 802.11p. With this protocol communication ranges up to 1000m. In this proposed mechanism, data of smart meters flows from houses to a bus stop, and then collected data on the bus stop is transmitted to a bus which drives by on its scheduled time. The proposed scheme is evaluated in terms of end-to-end delay and delivery ratio with two different routing protocols, namely the AODV and DSR protocols. According to the comparative performance evaluations, the proposed data collecting mechanism achieves significantly better delivery ratio and lower delay when DSR is used.

In Chapter 4, a new solution to collect data of smart meter is proposed by changing data flow of the study that proposed in Chapter 3. In this solution, data flows first from smart meters to a bus through infrastructure-to-vehicle (I2V) communication and then from the bus to a bus stop through vehicle to-infrastructure (V2I) communication. We have evaluated the performance of the proposed data collection mechanism in terms of end-to-end delay and delivery ratio with two different routing protocols, namely the AODV and DSR

protocols, for normal density, high density and hop-by-hop communication scenarios. Importantly, the channel parameters used in the simulations were obtained from a set of field tests at 5.9 GHz in different environments. Our performance evaluations show that the proposed data collection mechanism achieves high delivery ratio and low end-to-end delay when the DSR routing protocol is used.

In Chapter 5, a light-weight solution for blackhole attack which is very popular in WSN is proposed. The protocol is an improved version of the commonly used AODV routing protocol for WSNs. The added mechanism to the original AODV routing protocol helps detect and discard blackhole nodes in the network. The performance of the proposed secure routing protocol is evaluated and compared against the original AODV protocol in terms of average end-to-end delay and delivery ratio. The comparative performance evaluations prove that, by detecting and discarding the blackhole nodes in the network, the proposed mechanism increases the delivery ratio without causing too much extra delay.

In Chapter 6, VANET is combined with smart grids and proposed a data collection mechanism, with added security features, for collecting data from smart meters using public transportation buses. In the smart grid data collection through public transportation buses scenario which introduced in Chapter 4, the performance of the proposed secure routing mechanism is evaluated with the original AODV protocol in terms of average end-to-end delay and delivery ratio, under the existence of blackhole nodes in the network. We did our performance evaluations for urban neighborhood. According to the comparative performance evaluations, the proposed routing mechanism eliminates the malicious nodes in the network and achieves almost the same delivery ratio values as AODV routing protocol without causing extra delays and increasing request packet size only only 64-bit.

Possible future research directions are identified as follows:

i The transmitted data size from smart meter is 100 bytes for every 10 mins from houses to a bus stop. The influence of varying packet sizes and transmission periods on the efficiency of the proposed scheme may be studied.

ii The case when a bus would not arrive at the bus stop on its scheduled arrival time is not considered. The no show case for a bus may be studied and possible countermeasures could be investigated.

iii For houses located more than 1000 m away from the nearest bus stop, hop-by-hop communication is proposed and preliminary simulations is made. A more comprehensive study could be conducted on this scenario for a detailed analysis of hop-by-hop communication.

iv The security and privacy aspects of the proposed scheme may be studied. Efficient mechanisms may be investigated for communicating smart grid data in a secure and privacy preserving manner in the proposed scheme.

v In the proposed scheme, the IEEE 802.11p communication protocol, which supports a communication range of up to 1000 m, is used. Different wireless technologies may be investigated for the proposed system and their influence on the effective communication distance may be studied.

vi In the proposed scheme, one smart meter per building is assumed. For buildings with multiple smart meters, one smart meter (preferably on the top floor of the building) could be picked as the central smart meter which is responsible for collecting data from other smart meters in the building using a wired or a wireless communication technology, then using 802.11p the accumulated data could be sent by this central smart meter to buses. The alternative would be individual data transmissions from all smart meters in a building to buses. Such scenarios extending the capability of the proposed scheme could be explored, and their efficacy and performance could be investigated.

vii If buses are passing by an area with high-rise buildings, data transmission from buildings in the back streets may be hindered, which could be mitigated by using multi-hop communication. The influence of unusual or problematic scenarios on the effectiveness of the proposed scheme could be investigated and possible countermeasures could be studied.

viii Potential other uses of the proposed technology could be explored, e.g. remote patient monitoring for healthcare applications, where patient data, measured by sensors, is communicated to a physician periodically.

ix The scenario of using a sink node in the network, where sensor nodes connect with a data center, may be investigated and the proposed secure AODV mechanism can be studied for this scenario.

x Encryption algorithms other than AES and SPECK64 could be explored, and their efficacy and performance could be investigated for the proposed secure AODV protocol.

xi The use of hash-based message authentication codes, such as HMAC, could be investigated as a replacement for the currently used symmetric key encryption algorithms in the proposed mechanism. While using HMAC would have the added benefit of authenticating the integrity of transmitted packets, it would result in longer packets due to the hash output included in packets, e.g., if HMAC is used with SHA-256, the hash output will be 256 bits in length, which is significantly larger than the 64-bit signature used in the proposed mechanism. The use of different message authentication codes and hash functions could be explored and their efficacy and performance could be investigated.

xii The proposed SAODV protocol for data collecting mechanism may be tested for suburban or rural areas.

REFERENCES

Books

Patil, H. K. & Chen, T., 2013. *Computer and Information Security Handbook*, chap. Wireless sensor network security the internet of things. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 3 ed., pp. 317–337.

Patil, H. K. & Chen, T., 2017. *Computer and Information Security Handbook*, chap. Wireless sensor network security. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2 ed., pp. 301–322.

Rappaport, T., 2002. *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2 ed.

Periodicals

Abidoye, A. P. & Obagbuwa, I. C., 2018. Ddos attacks in wsns: detection and countermeasures. *IET Wireless Sensor Systems* **8(2)**, pp. 52–59.

Akyildiz, I., Su, W., Sankarasubramaniam, Y., & Cayirci, E., 2002. Wireless sensor networks: a survey. *Computer Networks* **38(4)**, pp. 393 – 422.

Al-Karaki, J. N. & Kamal, A. E., 2004. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications* **11(6)**, pp. 6–28.

AL-Mousawi, A. J. & AL-Hassani, H. K., 2017. A survey in wireless sensor network for explosives detection. *Computers & Electrical Engineering* .

Amin, S. M. & Wollenberg, B., 2005. Toward a smart grid. *IEEE Power & Energy Magazine* **3(5)**, pp. 34–41.

Bilgin, B. & Gungor, V. C., 2012a. Adaptive error control in wireless sensor networks under harsh smart grid environments. *Sensor Review* **32**, pp. 203–211.

Bilgin, B. & Gungor, V. C., 2012b. Performance evaluations of zigbee in different smart grid environments. *Computer Networks* **56(8)**, pp. 2196 – 2205.

Bilgin, B. & Gungor, V. C., 2013. Performance comparison of ieee 802.11p and ieee 802.11b for vehicle-to-vehicle communications in highway, rural, and urban areas. *International Journal of Vehicular Technology* **2013**.

Bilgin, B. E., Baktir, S., & Gungor, V. C., 2016a. Collecting smart meter data via public transportation buses. *IET Intelligent Transport Systems* **10(8)**, pp. 515–523.

Bilgin, B. E., Baktir, S., & Gungor, V. C., 2016b. A novel data collection mechanism for smart grids using public transportation buses. *Computer Standards & Interfaces* **48**, pp. 19 – 29.

Bose, A., 2010. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid* **1(1)**, pp. 11–19.

Bouhafs, F., Mackay, M., & Merabti, M., 2012. Links to the future: Communication requirements and challenges in the smart grid. *Power and Energy Magazine, IEEE* **10(1)**, pp. 24–32.

Bumiller, G., Lampe, L., & Hrasnica, H., 2010. Power line communication networks for large-scale control and automation systems. *IEEE Communications Magazine* **48(4)**, pp. 106–113.

Cazorla, M., Gourgeon, S., Marquet, K., & Minier, M., 2015. Survey and benchmark of lightweight block ciphers for msp430 16-bit microcontroller. *Security and Communication Networks* **8(18)**, pp. 3564–3579.

Dener, M., 2017. Wisen: A new sensor node for smart applications with wireless sensor networks. *Computers & Electrical Engineering* **64**, pp. 380 – 394.

Du, X. & h. Chen, H., 2008. Security in wireless sensor networks. *IEEE Wireless Communications* **15(4)**, pp. 60–66.

Farhangi, H., 2010. The path of the smart grid. *IEEE Power and Energy Magazine* **8(1)**, pp. 18–28.

Finogeev, A. G. & Finogeev, A. A., 2017. Information attacks and security in wireless sensor networks of industrial scada systems. *Journal of Industrial Information Integration* **5**, pp. 6 – 16.

Gerla, M. & Kleinrock, L., 2011. Vehicular networks and the future of the mobile internet. *Computer Networks* **55(2)**, pp. 457 – 469. Wireless for the Future Internet.

Gungor, V. & Lambert, F., 2006. A survey on communication networks for electric system automation. *Computer Networks* **50(7)**, pp. 877 – 897.

Gungor, V. C. & Hancke, G. P., 2009. Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics* **56(10)**, pp. 4258–4265.

Gungor, V. C., Lu, B., & Hancke, G. P., 2010. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics* **57(10)**, pp. 3557–3564.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P., 2011. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics* **7(4)**, pp. 529–539.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P., 2013. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics* **9(1)**, pp. 28–42.

Haghighi, M. S., Mohamedpour, K., Varadharajan, V., & Quinn, B. G., 2011. Stochastic modeling of hello flooding in slotted csma/ca wireless sensor networks. *IEEE Transactions on Information Forensics and Security* **6(4)**, pp. 1185–1199.

Hansen, A., Staggs, J., & Shenoi, S., 2017. Security analysis of an advanced metering infrastructure. *International Journal of Critical Infrastructure Protection* **18(C)**, pp. 3–19.

Hartenstein, H. & Laberteaux, K., 2008. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE* **46(6)**, pp. 164–171.

He, D., Zeadally, S., Kumar, N., & Lee, J., 2017. Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal* **11(4)**, pp. 2590–2601.

Heile, B., 2010. Smart grids for green communications [industry perspectives]. *IEEE Wireless Communications* **17(3)**, pp. 4–6.

Härri, J., Filali, F., & Bonnet, C., 2009. Mobility models for vehicular ad hoc networks: a survey and taxonomy. *Communications Surveys Tutorials, IEEE* **11(4)**, pp. 19–41.

Hsueh, C. T., Wen, C. Y., & Ouyang, Y. C., 2015. A secure scheme against power exhausting attacks in hierarchical wireless sensor networks. *IEEE Sensors Journal* **15(6)**, pp. 3590–3602.

Ipakchi, A. & Albuyeh, F., 2009. Grid of the future. *IEEE Power and Energy Magazine* **7(2)**, pp. 52–62.

Isaac, J. T., Zeadally, S., & Camara, J. S., 2010. Security attacks and solutions for vehicular ad hoc networks. *IET Communications* **4(7)**, pp. 894–903.

Jaballah, W. B., Conti, M., File, G., Mosbah, M., & Zemmari, A., 2018. Whac-a-mole: Smart node positioning in clone attack in wireless sensor networks. *Computer Communications* **119**, pp. 66 – 82.

Kaurav, A. & Kumar, K. A., 2017. Detection and prevention of blackhole attack in wireless sensor network using ns-2.35 simulator. *International Journal of Scientific Research in Computer Science* **2(3)**, pp. 717–722.

Khalifa, T., Naik, K., & Nayak, A., 2011. A survey of communication protocols for automatic meter reading applications. *IEEE Communications Surveys Tutorials* **13(2)**, pp. 168–182.

Kompara, M. & Hölbl, M., 2018. Survey on security in intra-body area network communication. *Ad Hoc Networks* **70**, pp. 23 – 43.

Kumar, V. & Kumar, R., 2015. An adaptive approach for detection of blackhole attack in mobile ad hoc network. *Procedia Computer Science* **48**, pp. 472 – 479. International Conference on Computer, Communication and Convergence (ICCC 2015).

Len, R. A., Vittal, V., & Manimaran, G., 2007. Application of sensor network for secure electric energy infrastructure. *IEEE Transactions on Power Delivery* **22(2)**, pp. 1021–1028.

Li, H., He, Y., Cheng, X., Zhu, H., & Sun, L., 2015. Security and privacy in localization for underwater sensor networks. *IEEE Communications Magazine* **53(11)**, pp. 56–62.

Li, J., Wang, D., & Wang, Y., 2018. Security dv-hop localisation algorithm against wormhole attack in wireless sensor network. *IET Wireless Sensor Systems* **8(2)**, pp. 68–75.

Li, X., Xu, J., Dai, H., Zhao, Q., Cheang, C. F., & Wang, Q., 2015. On modeling eavesdropping attacks in wireless networks. *Journal of Computational Science* **11**, pp. 196 – 204.

Lightner, E. M. & Widergren, S. E., 2010. An orderly transition to a transformed electricity system. *IEEE Transactions on Smart Grid* **1(1)**, pp. 3–10.

Lin, X., Lu, R., Zhang, C., Zhu, H., h. Ho, P., & Shen, X., 2008. Security in vehicular ad hoc networks. *IEEE Communications Magazine* **46(4)**, pp. 88–95.

Liu, Y., Dong, M., Ota, K., & Liu, A., 2016. Activetrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security* **11(9)**, pp. 2013–2027.

Luan, X., Zheng, Z., Wang, T., Wu, J., & Xiang, H., 2015. Hybrid cooperation for machine-to-machine data collection in hierarchical smart building networks. *Communications, IET* **9(3)**, pp. 421–428.

Mahajan, M., Reddy, K., & Rajput, M., 2016. Design and simulation of a blacklisting technique for detection of hello flood attack on leach protocol. *Procedia Computer Science* **79**, pp. 675–682.

McDaniel, P. & McLaughlin, S., 2009. Security and privacy challenges in the smart grid. *IEEE Security and Privacy* **7(3)**, pp. 75–77.

Mishra, A. K. & Turuk, A. K., 2016. A comparative analysis of node replica detection schemes in wireless sensor networks. *Journal of Network and Computer Applications* **61**, pp. 21 – 32.

Mokdad, L., Ben-Othman, J., & Nguyen, A. T., 2015. Djavan: Detecting jamming attacks in vehicle ad hoc networks. *Performance Evaluation* **87**, pp. 47 – 59.

Mokhtar, B. & Azab, M., 2015. Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal* **54(4)**, pp. 1115 – 1126.

Molderink, A., Bakker, V., Bosman, M. G. C., Hurink, J. L., & Smit, G. J. M., 2010. Management and control of domestic smart grid technology. *IEEE Transactions on Smart Grid* **1(2)**, pp. 109–119.

Molisch, A. F., Tufvesson, F., Karedal, J., & Mecklenbrauker, C. F., 2009. A survey on vehicle-to-vehicle propagation channels. *IEEE Wireless Communications* **16(6)**, pp. 12–22.

Nabar, R. U., Bolcskei, H., & Kneubuhler, F. W., 2004. Fading relay channels: performance limits and space-time signal design. *IEEE Journal on Selected Areas in Communications* **22(6)**, pp. 1099–1109.

Niyato, D. & Wang, P., 2012. Cooperative transmission for meter data collection in smart grid. *Communications Magazine, IEEE* **50(4)**, pp. 90–97.

Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C., 2017. Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. *Computer Networks* **113**, pp. 94 – 110.

Pereira, P. R., Casaca, A., Rodrigues, J. J. P. C., Soares, V. N. G. J., Triay, J., & Cervello-Pastor, C., 2012. From delay-tolerant networks to vehicular delay-tolerant networks. *Communications Surveys Tutorials, IEEE* **14(4)**, pp. 1166–1182.

Perkins, C., Belding, E., & SR, D., 2002. Ad hoc on-demand distance vector (aodv) routing **3561**.

Pu, C. & Lim, S., 2018. A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: Design, analysis, and evaluation. *IEEE Systems Journal* **12(1)**, pp. 834–842.

Puccinelli, D. & Haenggi, M., 2005. Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE Circuits and Systems Magazine* **5(3)**, pp. 19–31.

Qu, F., Wu, Z., Wang, F. Y., & Cho, W., 2015. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems* **16(6)**, pp. 2985–2996.

Rani, T. & Jayakumar, C., 2017. Unique identity and localization based replica node detection in hierarchical wireless sensor networks. *Computers & Electrical Engineering* **64**, pp. 148 – 162.

Rashid, B. & Rehmani, M. H., 2016. Applications of wireless sensor networks for urban areas: A survey. *Journal of Network and Computer Applications* **60**, pp. 192 – 219.

Rehan Rasheed, M., Khan, M., Naseem, M., Ajmal, A., & M. Hussain, I., 2010. Performance of routing protocols in wimax networks. *International Journal of Engineering and Technology* **2(5)**, pp. 412–417.

Ren, J., Zhang, Y., Zhang, K., & Shen, X., 2016. Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications* **15(5)**, pp. 3718–3731.

Rendong Bai & Singhal, M., 2006. Doa: Dsr over aodv routing for mobile ad hoc networks. *IEEE Transactions on Mobile Computing* **5(10)**, pp. 1403–1416.

S Kaushik, S. & R Deshmukh, P., 2009. Comparison of effectiveness of aodv, dsdv and dsr routing protocols in mobile ad hoc networks. *International Journal of Information Technology and Knowledge Management* **2(2)**, pp. 499–502.

Santa, J., Gómez-Skarmeta, A. F., & Sánchez-Artigas, M., 2008. Architecture and evaluation of a unified v2v and v2i communication system based on cellular networks. *Computer Communications* **31(12)**, pp. 2850 – 2861. Mobility Protocols for ITS/VANET.

Schweitzer, N., Stulman, A., Margalit, R. D., & Shabtai, A., 2017. Contradiction based gray-hole attack minimization for ad-hoc networks. *IEEE Transactions on Mobile Computing* **16(8)**, pp. 2174–2183.

Sheikh, S. S. & Sharma, S., 2011. Design and implementation of wireless automatic meter reading system. *International Journal of Engineering Science & Technology* **3(3)**, pp. 2329–2334.

Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A., 2018. Reato: Reacting to denial of service attacks in the internet of things. *Computer Networks* **137**, pp. 37 – 48.

Tiruvakadu, D. S. K. & Pallapa, V., 2018. Confirmation of wormhole attack in manets using honeypot. *Computers & Security* **76**, pp. 32 – 49.

Tomić, I. & McCann, J. A., 2017. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal* **4(6)**, pp. 1910–1923.

Wang, Q., Leng, S., Fu, H., & Zhang, Y., 2012. An ieee 802.11p-based multichannel mac scheme with channel coordination for vehicular ad hoc networks. *Intelligent Transportation Systems, IEEE Transactions on* **13(2)**, pp. 449–458.

Wang, W., Xu, Y., & Khanna, M., 2011. A survey on the communication architectures in smart grid. *Computer Networks* **55(15)**, pp. 3604 – 3629.

Yadav, N. & Yadav, R., 2009. The effects of speed on the performance of routing protocols in mobile ad-hoc networks. *Int. Journal of Electronics, Circuits and Systems* **1**, pp. 79–84.

Yan, Y., Qian, Y., Sharif, H., & Tipper, D., 2013. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys Tutorials* **15(1)**, pp. 5–20.

Yick, J., Mukherjee, B., & Ghosal, D., 2008. Wireless sensor network survey. *Computer Networks* **52(12)**, pp. 2292 – 2330.

Zamalloa, M. Z. n. & Krishnamachari, B., 2007. An analysis of unreliability and asymmetry in low-power wireless links. *ACM Trans. Sen. Netw.* **3(2)**.

Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., & Hassan, A., 2010. Vehicular ad hoc networks (vanets): Status, results, and challenges. *Telecommunication Systems* **50**, pp. 1–25.

Zhao, X., Zhu, J., Liang, X., Jiang, S., & Chen, Q., 2017. Lightweight and integrity-protecting oriented data aggregation scheme for wireless sensor networks. *IET Information Security* **11(2)**, pp. 82–88.

Zhu, J., Zou, Y., & Zheng, B., 2017. Physical-layer security and reliability challenges for industrial wireless sensor networks. *IEEE Access* **5**, pp. 5313–5320.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L., 2016. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE* **104(9)**, pp. 1727–1765.

Other Publications

Abdollahi, A., Dehghani, M., & Zamanzadeh, N., 2007. Sms-based reconfigurable automatic meter reading system. In *Control Applications, 2007. CCA 2007. IEEE International Conference on*. pp. 1103–1107.

Ashna, K. & George, S., 2013. Gsm based automatic energy meter reading system with instant billing. In *Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on*. pp. 65–72.

Beaulieu, R., Treatman-Clark, S., Shors, D., Weeks, B., Smith, J., & Wingers, L., 2015. The simon and speck lightweight block ciphers. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. pp. 1–6.

Bilgin, B. E. & Gungor, V. C., 2011. On the performance of multi-channel wireless sensor networks in smart grid environments. In *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*. pp. 1–6.

Cerpa, A., Busek, N., & Estrin, D., 2003. Scale: A tool for simple connectivity assessment in lossy environments. technical report, University of California.

Choi, M., Ju, S., & Lim, Y., 2008. Design of integrated meter reading system based on power-line communication. In *Power Line Communications and Its Applications, 2008. ISPLC 2008. IEEE International Symposium on*. pp. 280–284.

Deshmukh, S. R., Chatur, P. N., & Bhople, N. B., 2016. Aodv-based secure routing against blackhole attack in manet. In *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*. pp. 1960–1964.

Elmahdi, E., Yoo, S., & Sharshembiev, K., 2018. Securing data forwarding against blackhole attacks in mobile ad hoc networks. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. pp. 463–467.

Ganesan, D., Krishnamachari, B., Woo, A., Culler, D., Estrin, D., & Wicker, S., 2002. Complex behavior at scale: An experimental study of low-power wireless sensor networks.

Härri, J., Filali, F., Bonnet, C., & Fiore, M., 2006. Vanetmobisim: generating realistic mobility patterns for vanets. pp. 96–97.

Hwang, R. J. & Huang, Y. Z., 2017. Secure data collection scheme for wireless sensor networks. In *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. pp. 553–558.

IETT, 2014. Bus line detail. http://mobil.iett.gov.tr/sa/mobil/hatarama/hatdetayi.

Islam, K., Shen, W., & Wang, X., 2012. Wireless sensor network reliability and security in factory automation: A survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* **42(6)**, pp. 1243–1256.

Jain, S. & Khuteta, A., 2015. Detecting and overcoming blackhole attack in mobile adhoc network. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. pp. 225–229.

Javadi, S. & Javadi, S., 2010. Steps to smart grid realization. In *Proceedings of the 4th WSEAS International Conference on Computer Engineering and Applications*, CEA'10. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), pp. 223–228.

Kerk, S., 2005. An amr study in an indian utility. In *Power Engineering Conference, 2005. IPEC 2005. The 7th International*. pp. 1–142.

Kim, S., 2006. Automatic meter reading system and method using telephone line. US Patent 7,102,533.

Koay, B., Cheah, S., Sng, Y., Chong, P., Shum, P., Tong, Y., Wang, X., Zuo, Y., & Kuek, H., 2003. Design and implementation of bluetooth energy meter. In *Information, Communications and Signal Processing, 2003 and Fourth Pacific Rim Conference on Multimedia. Proceedings of the 2003 Joint Conference of the Fourth International Conference on*, vol. 3. pp. 1474–1477 vol.3.

Kunisch, J. & Pamp, J., 2008. Wideband car-to-car radio channel measurements and model at 5.9 ghz. In *2008 IEEE 68th Vehicular Technology Conference*. pp. 1–5.

Miao, D., Xin, K., Wu, Y., Xu, W., & Chen, J., 2009. Design and implementation of a wireless automatic meter reading system. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, IWCMC '09. New York, NY, USA: ACM, pp. 1345–1349.

NS-2, 2011. The network simulator. http://www.isi.edu/nsnam/ns/index.html.

Park, B., Hyun, D., & Cho, S., 2002. Implementation of amr system using power line communication. In *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, vol. 1. pp. 18–21 vol.1.

Patidar, K. & Dubey, V., 2014. Modification in routing mechanism of aodv for defending blackhole and wormhole attacks. In *2014 Conference on IT in Business, Industry and Government (CSIBIG)*. pp. 1–6.

Perkins, C. E. & Royer, E. M., 1999. Ad-hoc on-demand distance vector routing. In *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*. pp. 90–100.

Razaque, A., Abdulghafour, M., & Khan, M. J., 2017. Detection of selfish attack over wireless body area networks. In *2017 IEEE Conference on Open Systems (ICOS)*. pp. 48–52.

Reindl, P., Nygard, K., & Du, X., 2010. Defending malicious collision attacks in wireless sensor networks. In *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*. pp. 771–776.

Rua, D., Issicaba, D., Soares, F., Almeida, P., Rei, R., & Peas Lopes, J., 2010. Advanced metering infrastructure functionalities for electric mobility. In *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES*. pp. 1–7.

Shi-Wei Lee, Cheng-Shong Wu, Meng-Shi Chiou, & Kou-Tan Wu, 1996. Design of an automatic meter reading system [electricity metering]. In *Industrial Electronics, Control, and Instrumentation, 1996., Proceedings of the 1996 IEEE IECON 22nd International Conference on*, vol. 1. pp. 631–636 vol.1.

Soh, S. & Kerk, S., 2005. The electricity and metering trends in singapore. In *Power Engineering Conference, 2005. IPEC 2005. The 7th International*. pp. 1–152.

Spencer, Q., 2008. An information-theoretic analysis of electricity consumption data for an amr system. In *Power Line Communications and Its Applications, 2008. ISPLC 2008. IEEE International Symposium on*. pp. 199–203.

Tan, A., Lee, C., & Mok, V., 2007. Automatic power meter reading system using gsm network. In *Power Engineering Conference, 2007. IPEC 2007. International*. pp. 465–469.

Tuna, G., Gungor, V. C., & Gulez, K., 2011. Unmanned vehicle-aided automated meter reading. In *Broadband and Biomedical Communications (IB2Com), 2011 6th International Conference on*. pp. 289–293.

U.S. Department of Energy, 2002. National transmission grid study. https://www.energy.gov/oe/downloads/national-transmission-grid-study-2002.

U.S. Department of Energy, 2008. The smart grid: An introduction. https://www.energy.gov/oe/downloads/smart-grid-introduction-0.

Wesnarat, A. & Tipsuwan, Y., 2006. A power efficient algorithm for data gathering from wireless water meter networks. In *Industrial Informatics, 2006 IEEE International Conference on*. pp. 1024–1029.

Zerfos, P., Meng, X., Wong, S. H., Samanta, V., & Lu, S., 2006. A study of the short message service of a nationwide cellular network. In *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, IMC '06. New York, NY, USA: ACM, pp. 263–268.

Zhao, J. & Govindan, R., 2003. Understanding packet delivery performance in dense wireless sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, SenSys '03. New York, NY, USA: ACM, pp. 1–13.

Zigbee, 2009. Zigbee alliance. http://www.zigbee.org. [accessed 2014].

CURRICULUM VITAE

Name Surname :	Bilal Erman BİLGİN
Date and Place of Birth :	13 November 1987 Fatih/İstanbul
B.S. :	Bahçeşehir University, Computer Engineering (Major), 2009
B.S. :	Bahçeşehir University, Industrial Engineering (Double Major), 2009
M.S. :	Bahçeşehir University, Computer Engineering, 2011
Ph.D. :	Bahçeşehir University, Computer Engineering, 2019
Publications :	Bilgin, B. E., & Baktir S., 2019. A light-weight solution for blackhole attacks in wireless sensor networks, 2019. Turkish Journal of Electrical Engineering & Computer Sciences. 27(4) pp. 2557-2570. - Bilgin, B. E, Baktir, S., & Gungor, V. C., 2016. Collecting smart meter data via public transportation buses. Intelligent Transport Systems. 10(8) pp. 515-523. - Bilgin, B. E, Baktir, S., & Gungor, V. C., 2016. A novel data collection mechanism for smart grids using public transportation buses. Computer Standards & Interfaces. 48 pp. 19-29. - Yigit, M., Bilgin, B. E., & Karahoca, A., 2015. Extended topology based recommendation system for unidirectional social networks. Expert Systems with Applications. 42(7), pp. 3653-3661. - Bilgin, B.E., & Gungor, V. C., 2013. Performance Comparison of IEEE 802.11p and IEEE 802.11b for Vehicle-to-Vehicle Communications in Highway, Rural, and Urban Areas. International Journal of Vehicular Technology. 2013 pp. 1-10. - Bilgin, B.E., & Gungor, V. C., 2012. Adaptive error control in wireless sensor networks under harsh smart grid environments. Sensor Review. 32(3) pp. 203-211. - Bilgin, B.E., & Gungor, V. C., 2012. Performance evaluations of ZigBee in different smart grid environments. Computer Networks. 56(8) pp. 2196-2205. - Bilgin, B.E., & Gungor, V. C., 2011. On the performance of multi-channel wireless sensor networks in smart grid environments. in Proc. 2011 Proceedings of 20th Int. Conf. on Com. Commun. and Net. (ICCCN). pp. 1-6.
Work Experience :	- BELBİM Elektronik Para ve Ödeme Hizmetleri A.Ş., Test and Documentation Chief, Ongoing since Sept. 2016 - BELBİM Elektronik Para ve Ödeme Hizmetleri A.Ş., Software Developer, Nov. 2010 - Sept. 2016 - Bahçeşehir University, Research Assistant, Sept. 2009 - Nov. 2011