ROUTING AND SECURITY IN WIRELESS SENSOR NETWORKS, AN EXPERIMENTAL EVALUATION OF A PROPOSED TRUST BASED ROUTING PROTOCOL

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

NIAZ CHALABIANLOO

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER ENGINERING

FEBRUARY 2013

Approval of the thesis:

ROUTING AND SECURITY IN WIRELESS SENSOR NETWORKS, AN EXPERIMENTAL EVALUATION OF A PROPOSED TRUST BASED ROUTING PROTOCOL

Submitted by **NIAZ CHALABIANLOO** in partial fulfillment of the requirements for the degree of **Master of Science in Computer Engineering Department, Middle East Technical University** by,

Prof. Dr. Canan Özgen
Dean, Graduate School of **Natural and Applied Sciences** _____________________

Prof. Dr. Adnan Yazıcı
Head of Department, **Computer Engineering** _____________________

Assoc. Prof. Dr. Ahmet Coşar
Supervisor, **Computer Engineering Dept., METU** _____________________

Examining Committee Members:

Assoc. Prof. Dr. İbrahim Körpeoğlu
Computer Engineering Dept., Bilkent University _____________________

Assoc. Prof. Dr. Ahmet Coşar
Computer Engineering Dept., ODTÜ _____________________

Assoc. Prof. Dr. Murat Manguoğlu
Computer Engineering Dept., ODTÜ _____________________

Asst. Prof. Dr. Selim Temizer
Computer Engineering Dept., ODTÜ _____________________

Asst. Prof. Dr. İsmail Sengör Altıngövde
Computer Engineering Dept., ODTÜ _____________________

Date: 11.02.2013

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Niaz Chalabianloo

Signature :

ABSTRACT

ROUTING AND SECURITY IN WIRELESS SENSOR NETWORKS, AN EXPERIMENTAL EVALUATION OF A PROPOSED TRUST BASED ROUTING PROTOCOL

Chalabianloo, Niaz
Master of Science, Department of Computer Engineering
Supervisor: Assoc. Prof. Dr. Ahmet Coşar

February 2013, 57 pages

Satisfactory results obtained from sensor networks and the ongoing development in electronics and wireless communications have led to an impressive boost in the number of applications based on WSNs. Along with the growth in popularity of WSNs, previously implemented solutions need further improvements and new challenges arise which need to be solved.

One of the main concerns regarding WSNs is the existence of security threats against their routing operations. Likelihood of security attacks in a structure suffering from resource constraints makes it an important task to choose proper security mechanisms for the routing decisions in various types of WSN applications.

The main purpose of this study is to survey WSNs, routing protocols, security attacks against routing layer of a WSN, introduction of Trust based models which are an effective defense mechanism against security attacks in WSNs and finally, to implement a proposed Trust based routing protocol in order to overcome security attacks.

The study begins with a survey of Sensor Networks, after the introduction of WSNs and their related routing protocols, the issue of security attacks against the network layer of a Sensor Network is described with a presentation of different types of attacks and some of Trust based related works.

In the final chapters of this research, a novel Trust based AODV protocol will be proposed, implemented and examined in a simulation environment. For this purpose, multiple number of scenarios will be simulated on the AODV protocol with and without Trust mechanism, then the achieved results will be compared to derive a conclusion.

Keywords: Wireless Sensor Network, Routing, Security, Trust, AODV

ÖZ

TELSİZ SENSÖR AĞLARINDA YÖNLENDIRME VE GÜVENLİK, ÖNERİLEN GÜVEN BAZLI BİR YÖNLENDIRME PROTOKOLÜNÜN DENEYSEL DEĞERLENDİRİLMESİ

Chalabianloo, Niaz
Yüksek Lisans, Bilgisayar Mühendisliği Bölümü
Danışman: Doç. Dr. Ahmet Coşar

Şubat 2013, 57 sayfa

Sensör ağlarından elde edilen başarılı sonuçlar ile elektronikte ve telsiz haberleşmede sürmekte olan ilerlemeler, TSA bazlı uygulamaların sayısında göze çarpan bir atışa neden olmuştur. TSA'ların artan popülerliğinin yanı sıra daha önceden geliştirilen çözümlerin de daha iyileştirilmesi gerekmekte ve çözülmesi gereken yeni zorluklar ortaya çıkmaktadır.

TSA'lar konusundaki önemli çekincelerden biri bunların yönlendirme işlemlerine karşı mevcut olan güvenlik tehditleridir. Kaynak kısıtları nedeniyle zorlanan bir yapıda güvenlik saldırıları olasılığının bulunması çeşitli TSA uygulamalarında yönlendirme kararları için uygun güvenlik mekanizmalarının seçilmesini önemli bir işlem yapmaktadır.

Bu çalışmanın ana amacı TSA'lar, yönlendirme protokolleri, ve TSA'ların yönlendirme katmanlarına yönelik güvenlik saldırıları üzerinde derleme yapmak, güvenlik ataklarına karşı etkin bir savunma mekanizması olan Güven bazlı modellerin sunulması, ve son olarak da güvenlik saldırılarını engellemek için önerilen Güven bazlı bir yönlendirme protokolünün gerçekleştirilmesidir.

Çalışma TSA'nın ve ilgili yönlendirme protokollerinin tanıtılmasından sonra Sensör Ağlarının üzerinde yapılan derleme çalışması ile başlamaktadır, bir Sensör Ağının ağ tabakasına karşı yapılan güvenlik saldırıları tanımlanmakta ve çeşitli saldırı tipleri ile Güven bazlı ilgili çalışmalar sunulmaktadır.

Araştırmanın sonraki bölümlerinde, yeni bir Güven bazlı AODV protokolü önerilmekte, gerçekleştirilmekte ve çok sayıda senaryo için Güven bazlı güvenlik mekanizmalı AODV protokolü ile incelenmekte ve elde edilen sonuçlar karşılaştırılarak varılan sonuçlar anlatılmaktadır.

Anahtar Kelimeler: Telsiz Sensör Ağları, yönlendirme, Güvenlik, Güven, AODV

Dedicated to my parents for their endless love and support.

ACKNOWLEDGMENTS

The author wishes to express his deepest gratitude and appreciation to his supervisor Assoc. Prof. Dr. Ahmet Coşar for his valuable guidance, advice, criticism, encouragements and insight throughout the research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

With the ongoing tremendous growth in the widespread use of different types of computer systems and the growing demand for newer and more sophisticated applications which highly require communications between computer systems for the purpose of sharing resources and information, the concept of large computer networks consisting of multiple types of interconnected computer systems became a reality. Subsequently, every new technological achievement would bring up a lot of problems and obstacles which need to be solved and dealt with.

Some of the most important problems to solve, are the challenges of finding ways to develop new techniques for implementing large scale computer networks with an optimal working quality and at the same time lowering implementation costs as much as possible. The inevitable need for drawing out maximum performance out of the resources on hand requires making clever decisions in design, manufacturing and implementation process of a computer network.

From the beginning of computer networks era, there has always been a huge demand for using wireless communication between multiple nodes. By using wireless equipment, the process of design and implementation of computer networks and reaching hard to access places became easier and more flexible. At the same time, one of the annoying computer networks problems which is the problem of disorderly connected messy cables which is used in wired networks can be completely avoided by using wireless communication equipment.

Where wired connections require higher expenses and also occupy a lot of space for connecting large number of nodes which are mostly resulted in large quantities of cables disorderly twisted around each other, using wireless equipment has no such problems and is always neat and tidy.

Like almost every other newly developed equipment in electronics and computing, smaller in size and lower in cost is always more preferable and requested by majority of users and application needs. Likewise in the fields of Computer networks, nodes and communication devices, one of the most important issues is to manufacture newer generations of computer and networking equipment in smaller sizes with maintaining performance and lowering energy consumption and costs as much as possible, and at the same time by using wireless communications in order to facilitate access to nodes which might be movable and hard or even impossible to access by means of a wired communication.

All these recent huge advancements in the fields of microelectronics and wireless communication technologies in the past years have led to creation and further successful development in a field called Wireless Sensor Networks. Electronic sensor nodes are autonomous converters used to detect, measure and even analyze physical quantities and convert it to digital data for further processing or pass the observed data through sensor network to another destination and are widely used in multiple applications like industry, military, health, environmental monitoring, etc.

Sensor Networks which are mostly used in a distributed wireless fashion are mainly consist of sensor nodes, processor, transmitter and a power unit. Sensor nodes are highly constrained in processing capabilities and power consumption. The idea of monitoring the environment in a remote place makes them vulnerable to unpredictable hazards and furthermore not being able to easily access nodes to replace a damaged node in case of a critical network failure or to recharge their power source makes Wireless Sensor Networks more likely prone to failure if not taken care of properly.

Wireless Sensor Networks is quite a new field of study and there are lots of open research areas which need to be investigated, identified, studied and improved thoroughly. Most of the concerns about WSNs are related to specific needs and dependencies peculiar only to Wireless Sensor Networks. There are also some other important adversities similar to ones in the traditional computer networks. One of the toughest which might be present in all kinds of traditional and sensor networking applications pertains to taking proper actions against security attacks.

In this study we are going to perform a literature survey of Wireless Sensor Networks from recently published papers and after identifying classification of routing protocols in Wireless Sensor Networks, the issue of Security attacks against a WSNS routing layer will be described.

There are several researches on implementation of security mechanism on Wireless Sensor Networks, most of these researches with promising results apply a security defense, detection and confronting system based on the amount of reliance sensor nodes have on their neighbor nodes.

These security mechanism which are called Trust Based security algorithms are applied on the routing protocol of a Wireless Sensor Network in order to reduce and even prevention of the probable devastating damages caused by security attacks.

In order to study security attacks against Wireless Sensor Networks and to see whether these Trust based algorithms work competently or not, we are going to propose a novel Trust based algorithm based on AODV routing protocol and run it in multiple simulation scenarios. By comparing the results we can derive a final conclusion about the advantage and disadvantages of our Trust based AODV protocol.

1.1 WIRELESS SENSOR NETWORKS

A Wireless Sensor Network is a collection of mostly large quantities of cooperating sensor nodes that are working together in order to gather data about the environment in which they are deployed.

Sensor nodes which are mostly resource constrained are scattered or placed manually on locations where it's hard to access, therefor the collected data should be transmitted to a base station by means of radio signals via tiny built in wireless transmitters.

In terms of networking structure, Wireless Sensor Networks have two types, Structured WSN and unstructured WSN. [1]

In an unstructured Wireless Sensor Network which is generally consists of quite a large number of sensor nodes, node deployment is done randomly into the field [1]. Since the numbers of these widely scattered sensors deployed in a field are too many, network management becomes a difficult task in unstructured Wireless Sensor Networks.

On the other hand, in the structured Wireless Sensor Networks some or even the entire sensor nodes are placed in pre-determined fix locations, in a structured WSN nodes are placed in pre-determined places to obtain an optimal coverage, in this case the number of nodes are dramatically fewer compared to an unstructured WSN and also fewer nodes will result in lower error rates, easier to handle network management and lower costs.

Random placement of sensor nodes are mostly performed in inaccessible or very hard to access environments, like deploying sensor nodes from a helicopter to an enemy territory. [2][3]

One of the main issues in WSNs is that sensor nodes are very limited in resources like power, bandwidth, processing power and data storage capacity.

The size of a WSN depends on the application and the size and other conditions of the environment that is going to be analyzed by a WSN. The number nodes differ from only a few nodes for a small indoor environment to hundreds or even more for a very large field where more nodes are needed to cover and detect the ongoing phenomena in a field with a very large scale.

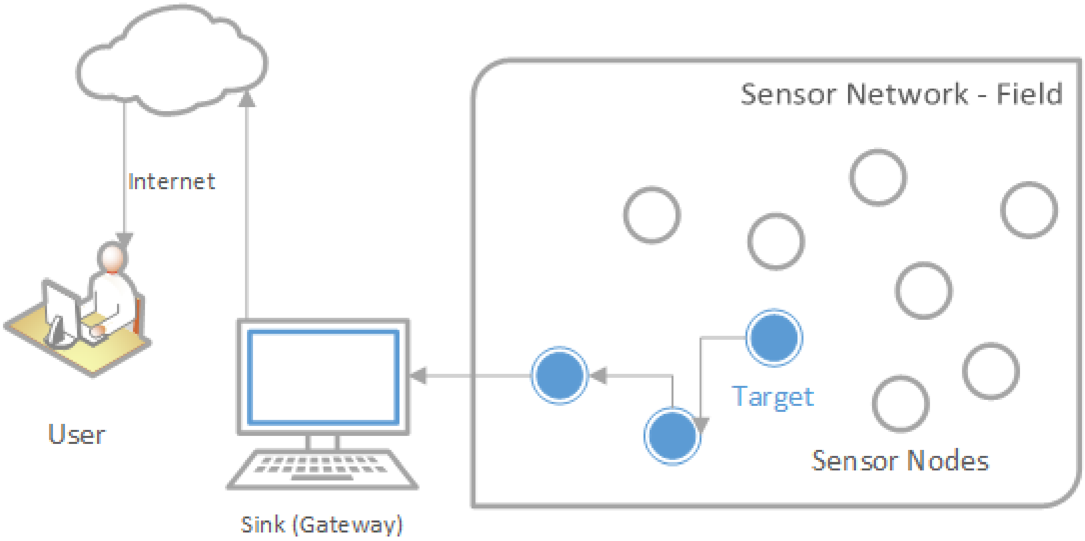


Figure 1. Wireless Sensor Network

One of the specific characteristics of a WSN is their cooperative working capabilities, sensor networks perform some tasks in collaboration with each other, almost in every part of the whole operation when a sensor node detects and senses phenomena, analog signals are converted to digital data, converted data might be too bulky causing heavy overloads and it may cause heavy redundant data with a data acquired by nearby sensors, these problems cause high bandwidth use and a higher bandwidth use leads to too much power consumption.

In order to prevent problems stated above, sensor nodes which are equipped with built in processing units, do some processing tasks, depending on the kind of data and application, the whole processing task or most of or even some part of it are carried out inside sensor nodes or in collaboration with other nodes.

For example in wireless multimedia sensor networks when a visual sensor captures a video from the environment, video compression operation can be carried out inside multiple nodes in a cooperative manner to prevent transmission of bulky raw data thus excessive power consumption is avoided and sensor network can achieve balanced work load among nodes and finally processed data is returned to the sink.

1.2 Hardware Components of a Wireless Sensor Network

Except some main components that are common in all types of WSN, sensor nodes in different types of WSNs deciding which hardware components are required to equip sensor nodes with, depends on application requirements and types of WSN, different applications are totally different in network size, number of nodes, total cost and the amount of power consumption in each node.

With all the new advancements in electronics and wireless communication technology in the past few years, developers and companies march towards building smaller and smaller electronic devices. These achievements led to mass produce of sensor nodes that are really low cost and tiny in size. In some cases sensor node is smaller than 1 cubic centimeter and with total cost of 1 dollar which consumes less than 0.1 mill watts. [4]

Although smaller size and weight is always desired and demanded by most costumers but a node with even a slightly larger size but lower in power consumption and cost is always more preferred than a very tiny node but high in power consumption and cost.

Sensor nodes are generally made up of common parts, these parts are power supply components, processing unit, sensing components, memory and transceiver unit.

A sensor node might also be equipped with some optional components like global positioning system sensor, actuator and mobilizers, imaging and visual sensors. [5][6][7]

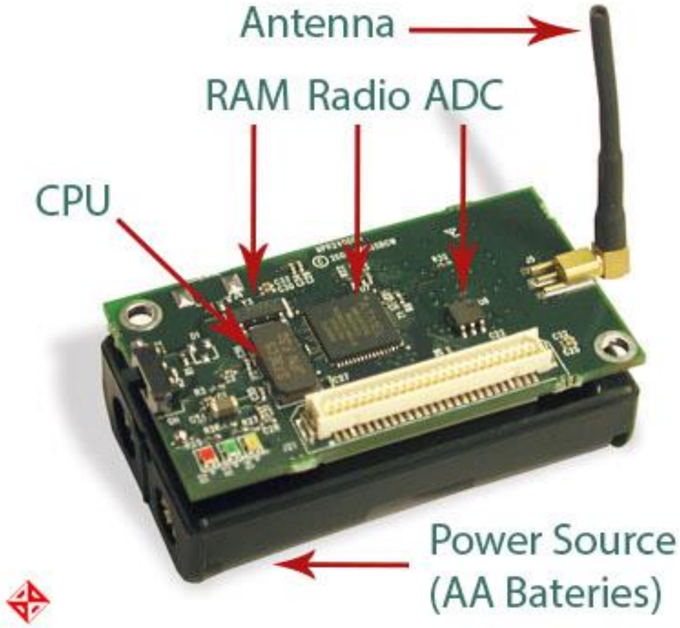


Figure 2. Micaz mote [34]

1.2.1 Power Supply Unit

Energy consumption in sensor nodes is almost the most important issue in WSN that needs to be dealt with carefully. Power supply unit is responsible to provide energy for different parts of working components in a sensor node. Power units can also be equipped with some kind of recharging tools like solar photovoltaic cells to generate energy from light.

All working components must fulfill conditions to operate in a tradeoff condition between consuming lower energy and performing their tasks adequately successful.

In order to reach an optimized energy consumption and to save more power for further operations, different rules are applied like turning off radio transmitters when the node is in idle state and turn it on again it's needed.

1.2.2 Processing Unit (Micro Controller)

Controller unit plays a significant rule in a sensor node. In order to accomplish different processing tasks this unit is consists of multiple built-in units. Deciding when and where to send/receive data to and from, executing miscellaneous programs, signal processing and carrying out other signal related tasks, deciding when and how to use mobilizers, actuators and other subunits.

One of the most important rules of the processing unit is to perform management of processes related to sensor nodes cooperating with other nodes in order to accomplish appointed tasks with an optimal functionality.

1.2.3 Memory

Sensor nodes must be equipped with RAM to store the data captured from a sensor for further processing, although random access memories are fast and also require lower energy consumption compared to read only memories, but in case of a power disruption, all their content will be deleted, to overcome this issue, EEPROMs and Flash memories are used as ROM (Read Only Memory) which can retain their data when there is a power failure, ROM is also used to store program data.

1.2.4 Communication and Transceiver Unit

Transceiver unit is used to establish a connection between sensor nodes in a network. Transmission media in wireless sensor networks are either radio frequencies which are the most useful choice, optical medium, ultrasound or infrared. Most of the currently in use sensor nodes are equipped with radio frequency based transceiver circuits. [8]

Unlike infrared, Radio Frequency transceivers do not require a direct line between sender/receiver to perform the send/receive operations. Compared to other methods RFs use slightly lower energy and they provide high bandwidth and transmit data to a higher and longer range.

Since most of the energy consumption in a sensor node takes place in transceiver unit, transceivers switch between ON, OFF and IDLE states in order to conserve more energy.

1.2.5 Sensing Unit

Sensors are some kind of energy converters which senses the environment by measuring the physical quantities of a nearby phenomenon.

Measured physical quantity will then turn into signals, since these signals are analog, they must be converted to digital data by analog to digital converters (ADC), and then the resulting digital signals are sent to processing unit for further analysis. [9]

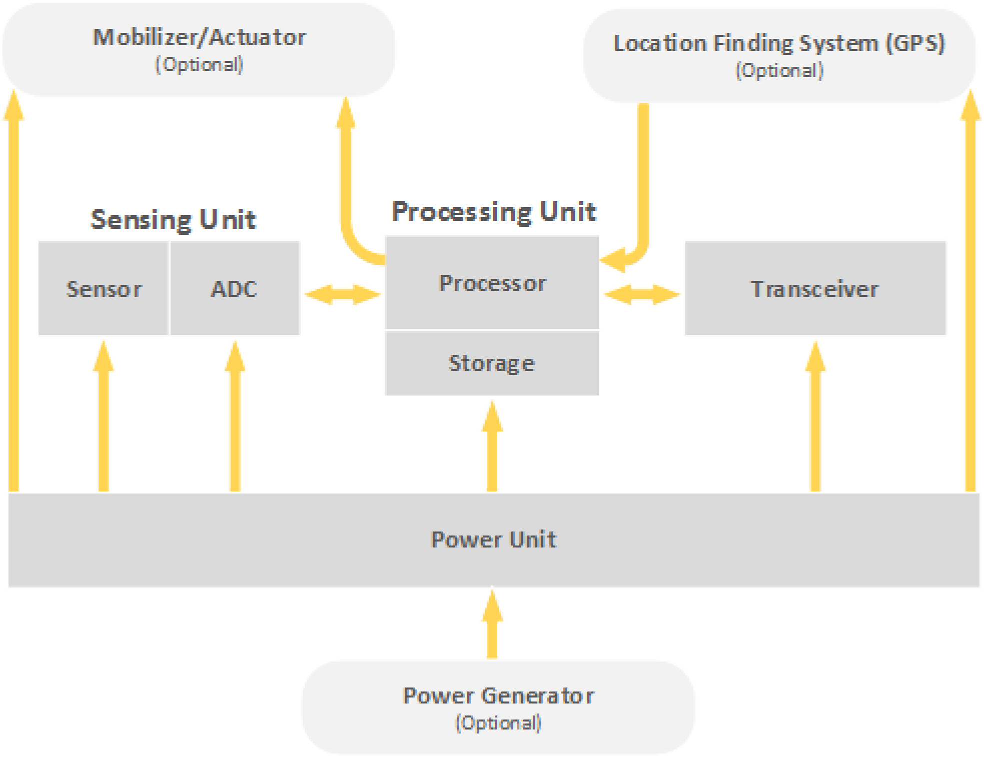


Figure 3. Sensor Node Architecture

1.3 WSN Applications

Among numerous applications for Wireless Sensor Networks, most of them belong to two main classes of applications which are monitoring and tracking applications. There are multiple fields and instances for each class; for example, there are WSN applications for health monitoring to monitor patients' vitals in hospitals [10]

WSNs are largely being used, researched and funded by military, in the military branch WSNs are used to monitor battle fields, surveillance, reconnaissance, espionage …

In the environmental monitoring applications, to reduce hazards and prevention of environmental disasters like floods, fire, earthquakes, avalanches or tsunamis, WSN are used for early warning and alerting, or even for taking actions in remote places by means of actuators. [11]

As an example for tracking applications, there are cases that WSNs are used to track animals to obtain a better understanding of their migration habits. [12]

While traditional WSNs have monitoring and tracking applications, Wireless Multimedia Sensor Networks introduce various new applications by using capabilities of Video/Audio sensors.

1.4 Wireless Multimedia Sensor Networks

With newer developments and advancements in the field of imaging sensors and microphones there is been a huge boost in production of low cost and low power multimedia sensors in recent years. [13][14]

Using imaging sensors (CMOS) and acoustic sensors (microphones) in sensor nodes brought up the whole idea of wireless multimedia sensor networks. Traditional Wireless Sensor Networks and Wireless Multimedia Sensor Networks are almost the same thing except the latter are equipped with multimedia sensors to retrieve and capture video, photo, and audio of events taking place in the environment under study.

Multimedia sensors can be tiny and very low power [15] or very high tech with high power demands.

Wireless Multimedia Sensor Networks have elevated traditional WSN performance by adding several new types of applications.

Since camera sensor nodes mostly operate in one direction by capturing a scene they are pointed to, in order to cover a large area and to avoid overlapped views as much as possible they are mostly placed in structured predetermined fix locations to ensure an optimal performance.

Using of multimedia sensors in wireless sensor networks has greatly expanded the capabilities of WSNs in the fields of monitoring and tracking applications. [16]

Multimedia and mostly camera sensors can increase monitoring-tracking performance by their unique ability to capture the case under study from different angles and being able to zoom on subjects to get a clear and more enhanced view of the subject being tracked/monitored and by cooperation of multiple sensors with overlapped fields of views, they can provide different streams and captures of a single target from different angles.

Local and Collaborative Processing: Raw data can be large in size and it's full of unnecessary, useless and redundant information.

Any attempt to transmit raw and uncompressed data will lead to high error rates, excessive power-bandwidth consumption.

To overcome these obstacles WSNs are equipped with unique processing algorithms, depending on application requirements, network architecture and sensors built in processors speed, these algorithms utilize mixture of disparate techniques on raw data, depending on data size and level of complexity this operation can be performed in a single node or in case of complex large raw data, processing can be performed among multiple nodes in a collaborative way. [17]

1.4.1 Heavy Bandwidth and Storage requirements:

In some cases WSN applications may require high bandwidth needs, for example transmission of large data like a video file requires a bandwidth which is much more higher than bandwidth used by traditional WSNs, for example nodes in Zigbee’s Micaz note which is widely used in wireless sensor networks has a maximum data rate of 250 kbps whereas in a multimedia sensor network streaming a high resolution video may require a bit rate higher than tens of mbits.

Nowadays sophisticated wireless sensor networks which are used in multimedia applications use ultra wide band (UWB) radio technology to achieve extremely high data transmission rates. [18] UWB uses very low energy for short range communications with up to 480 mbps data rate.

CHAPTER 2

WSN ARCHITECTURE

Sensor nodes are distributed in the environment, either randomly or in a predetermined manner, if the field under study is too large, hard to access manually and nodes are low cost and tiny in size non deterministic random deployment methods are used to setup the sensor network, on the other hand pre planned methods are used mostly on applications which need expensive and more sophisticated sensors, for example most multimedia sensor networks are placed in fixed locations to collect data in a direction they are pointed to.

Based on the distance between the source and base station (sink) collected data is transmitted to the base station by number of multi hop or single hop transmissions.

2.1 Planning Factors for an Optimal Sensor Network

There are multiple factors to gain an optimal sensor network performance in different types of sensor applications; most factors are common between all types of sensor networks. Some of the most important factors are: QoS, Energy Consumption Efficiency, manufacturing costs, scalability, fault tolerance and robustness.

2.1.1 Fault Tolerance and Robustness

State of being a fault tolerant robust system is that wireless sensor networks should not stop functioning in case of a failure in one or even more nodes. Node failure may occur if a node runs out of power, in such cases sensor networks should be able to maintain their functionalities by taking proper actions to avoid throughout network failure. For example a transmission failure may occur in a multi hop transmission where node A transmits its data to B and node B passes the same data to C, when node B stops working or is out of access, A-B-C multi hop is broken. [19]. in such cases wireless sensor network must keep working by finding another routing pass from node A to C.

2.1.2 Scalability

Wireless Sensor Networks may consist of a large number of sensor nodes. Scalability dictates that WSN must be able to sustain performance regardless of the growth in network size. Most of the research in WSNs and scalability is based on traditional sensor networks in which sensor nodes are homogeneous. These networks are mostly flat and research on scalability is concentrated on how to maintain performance when node density is high.

2.2 A WSN Architecture Scenario

Traditional sensor networks are mostly single tier networks composed of homogenous sensors performing same sort of functions in a centered or distributed processing way.

Conserving energy consumption and keeping network alive as long as possible is the main issue to overcome in homogenous sensor networks, in order to consume less energy low power sensors are used although there is been a lot of development in sensor technologies but higher functionalities require high energy consumption and high end sensors can perform more sophisticated tasks with a price of dramatically higher power consumption yet low power nodes yield lower functionalities.

By deploying more quantities of sensor nodes, tasks like processing and routing and thus energy consumption is divided between sensors and therefore network lifetime increases but meantime in a sensor network with higher numbers of sensor nodes, latency becomes higher because more nodes will go to sleep state and every wakeup call increases the total latency.

Issues stated above clearly shows that in order to keep a homogenous sensor network in an optimal working state, there must be a tradeoff between all design goals and that’s why traditional homogenous sensor networks are not suitable enough for sophisticated sensor networks like a multimedia sensor network in which there is excessive need for higher processing power, higher bandwidth and higher power consumption.

2.3 Multitier Sensor Networks

A multi-tier sensor network is a collection of heterogeneous sensors with various functions and capabilities working in a hierarchical order, in a multi-tier sensor network each tier undertakes a series of tasks, sensors in lower tiers are of a group of lower power and functionality sensors and their job is to perform simple tasks which need lower resources, similarly higher performance nodes are of higher tiers. Nodes in higher tiers have more powerful sensing and processing units with almost no energy limits. [20]

CHAPTER 3

ROUTING PROTOCOLS FOR WSN

The main function of the network layer in WSN is to find and handle routes for the purpose of data transmission from nodes to sink and all across the sensor network.

Since sensor nodes are not equipped with IP addresses, therefore routing protocols in WSNs are different from traditional IP based protocols.

3.1 Taxonomy of Routing Protocols in WSN

Since the beginning of WSN era there is been quite a lot of research on designing routing protocols suitable for different architectures of WSNs with different application scenarios, that's why routing protocols for WSNs can be classified in a lot of distinct ways.

Routing protocols for Wireless Sensor Networks are mainly differentiated based on network architecture and conditions, WSN operations, data-node centric, location based and QoS.

3.1.1 Data Centric (Flat) Protocols

In a lot of applications for WSNs it is almost impossible to assign an ID like a traditional IP for each and every node in the network, lacking such and identifier makes it very difficult to choose what set of nodes should be selected for query and transmission, in this case data is transmitted through all nodes causing heavy bandwidth and power consumption with a lot of redundancy.

In data centric routing protocols, queries are sent to specific locations and the data which has attribute-based naming is sent back by the sensors on selected locations.

SPIN is an example for data centric routing in which sensors negotiate data witch each other by means of data advertising to neighbor nodes and exchanging Meta data for the purpose of data routing with lower energy consumption and less redundancy.

Directed Diffusion is another data centric routing protocol, in DD algorithm data with attribute-value naming is diffused through nodes.

Nodes in directed diffusion can perform data aggregation inside sensor networks by using a minimum steiner tree

Query driven routing protocols cannot be used on all kind of applications, for example a monitoring application which needs continuous data transmission to the base station won't perform its job properly because queries are sent on demand and not continuously. [21]

3.1.2 Hierarchical Routing Protocols

High density of sensor nodes in a single tier network can cause heavy overloads and consequently a dramatic increase in power consumption, latency and network failure rate. That's why single tier networks are not suitable enough for sophisticated applications that need high density sensor networks.

In a hierarchical approach nodes are grouped to form several clusters inside the sensor network, in each cluster one of the nodes acts as a cluster head.

Hierarchical routing is mostly used on multi-tier networks with heterogeneous nodes, usually the most powerful nodes are selected as cluster heads, data aggregation and other processing tasks like data compression in image sensors are performed inside each cluster, by doing so, energy consumption becomes sufficiently acceptable. [21]

LEACH is a hierarchical routing protocol for wireless sensor networks. In the LEACH algorithm instead of all nodes only cluster heads act as a router to transmit data from and towards the base stations.

3.1.3 Location Based Protocols

Since global addressing like IP based addresses is not applicable for sensor nodes, but on the other hand in order to calculate the estimated energy consumption in a transmission between two nodes, routing protocols for WSNs need to know where sensor nodes are located, if the location of a sensed data is known, then the routing process can be very energy efficient by setting up node to node transmission in a way that data is transmitted only to that specific region.

Location based routing protocols are also called geo centric, in a geo centric algorithm knowing the geographical location of nodes is the key element for the purpose of finding ways for an efficient routing.

Some of the geo centric (location based) protocols are mainly used in mobile ad hoc networks.

Location based protocols in unstructured sensor networks can use sensor nodes built it GPS sensors to obtain the geographical information.

GAF (Geographical adaptive fidelity): is a geo centric routing algorithm that uses GPS information to locate nodes, GAF is also an energy aware algorithm and switches the sensor node radios between idle and active modes, sensor radios are only active when they are needed to perform a transmission. [21]

3.1.4 QoS Routing Protocols

In QoS bases routing protocols data transmission paths are set up considering delivery latency, end to end delivery ratio and energy expenditure.

The aim is to achieve a balanced level of having lesser latency in a high data delivery rate by using less energy.

QoS aware routing protocols can be classified in three groups with different metrics: QoS aware routing based on network situation, QoS aware routing based on packet priorities and traffic classes, (in this group, data types have variant rate of priorities. QoS aware routing protocols specialized for streaming data in a real time manner. (Mostly used in multimedia sensor networks). SPEED and MMSPEED are two QoS protocols with streaming support. [13]

Another categorization on routing protocols for WSNs and ad hoc networks is based on the method sensor networks use to obtain and preserve the data and how to calculate route paths based on the obtained information.

This classification is relying on the manner in which source nodes discover and maintain paths to destination.

3.1.5 Proactive Routing Protocols

Proactive Routing Protocols which are also called as table driven routing protocols are based on intermitted propagation of routing info to sustain stable and precise routing tables among all nodes in WSN.

Proactive routing protocols set routing paths up ahead of any request for routing transmission and paths are preserved even if there is no need for transmission at that moment.

In the proactive routing protocols in order to preserve valid routing information, nodes must send control messages intermittently and this can cause a lot of bandwidth waste since these control messages are unnecessary when there is no need for a transmission. On the other hand the main privilege of proactive routing protocols is that nodes can quickly acquire routing path information to establish a connection almost immediately.

OLSR (Optimized Link State Routing) and B.A.T.M.A.N (Better Approach To Mobile Ad hoc Networking) are two examples of proactive routing protocols.

3.1.6 Reactive Routing Protocols

Reactive Routing Protocols which are also known as "on demand" protocols do not need to keep route information of all nodes in the network when there is no need for a communication. Instead, setting up routes between nodes is relying on series of queries in which nodes are performing dynamic inspection by broadcasting a control message as a query for the purpose of finding route paths.

The transmission can be established after finding a route path. This method can reestablish new route paths in case of a failure but dealing with control queries can produce high rates of latency.

DSR (Dynamic Source Routing), AODV (Ad hoc on demand Distance Vector Routing) and ABR (Associativity Based Routing) are three examples of on demand (Reactive) routing protocols.

3.1.7 AODV (Ad-hoc On Demand Vector routing protocol)

AODV is a widely used famous reactive protocol for ad hoc, mobile and wireless sensor networks. AODV uses traditional distance vector tables and also keeps a track of destination addresses and sequence numbers to hinder entering loops and also to check whether the routing paths are fresh or old. In the AODV routing protocol neighbor nodes will be informed if a route failure occurs and finding routes from source to destination is done by a road request message broadcasted from the source node and receiving back a unicast route reply message from the destination node. [22]

Four kinds of control messages are used in AODV:

- Route Request message (RREQ)
- Route Reply message (RREP)
- Route Error message (RERR)
- Hello message

Route Request message

RREQ is broadcasted from a source node when it does not have a path to a certain destination and wants to find one.

Every time when a new RREQ is broadcasted by the source, req ID in the table above is incremented by one, upon obtaining a RREQ packet, nodes will first check to see whether this RREQ has been received before by checking the req ID and source address, if it has, then the RREQ message will be ignored and discarded, if not it will be flooded to their neighbors.

Route Reply message

If the node that is the receiver of RREQ message is the destination or if this node has got a route to it, the RREQ message will be discarded and a PREP unicast message will be sent back towards the source node. Next receiver of the PREP message which is one hop closer to destination will update the route table and send it back again to the source node, by doing so a route will be created between the source and the destination. On the other hand if the receiver of a RREQ message has no route to the specified destination it must update and broadcast the RREQ message again.

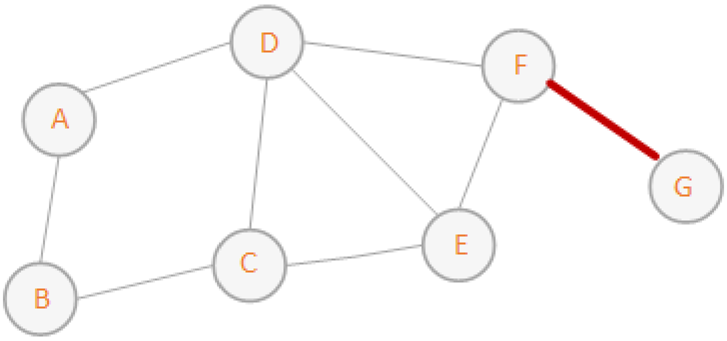
Route Error message

In case of a route breakage, a list of inaccessible nodes will be created and neighbor nodes will be informed of these broke routes by receiving RERR messages.

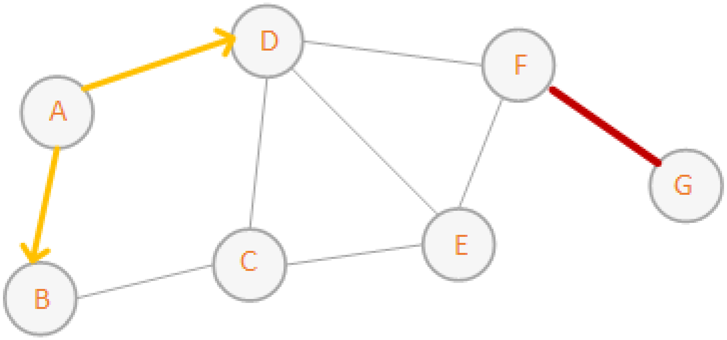
Hello messages

Hello messages are simple packets to determine link status, to check whether the connectivity between nodes is still available or not, hello messages are transmitted intermittently.

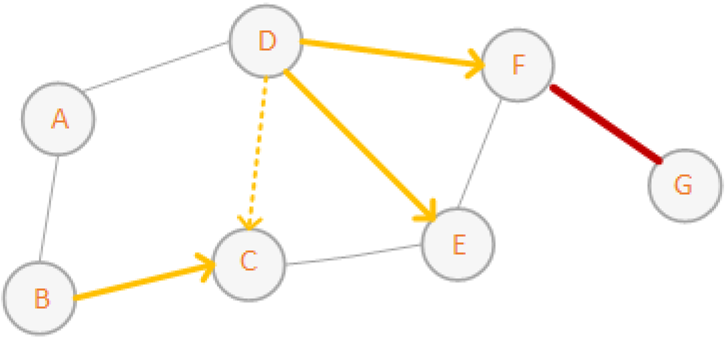
Figures in the next 3 pages show an example of RREQ, RREP and RERR messages in action where node A wants to send data packets to node G. [39]



- Node A needs to send a data packet to Node G
- Assume Node F knows a current route to Node G
- Assume that no other route information exists in the network (related to Node G)

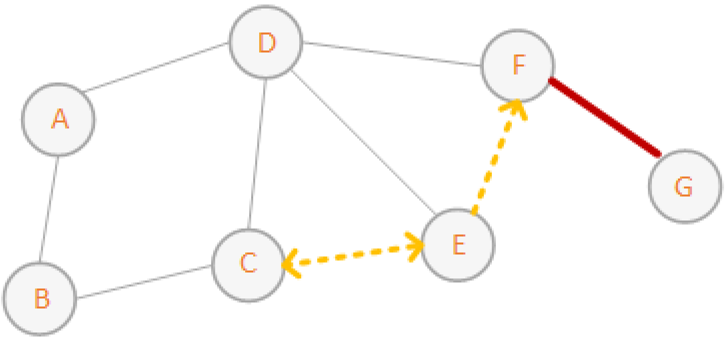


- Node A sends a RREQ packet to its neighbors
- source_addr = A
- dest_addr = G
- broadcast_id = broadcast_id + 1
- source_sequence_# = source_sequence_# + 1
- dest_sequence_# = last dest_sequence_# for Node G

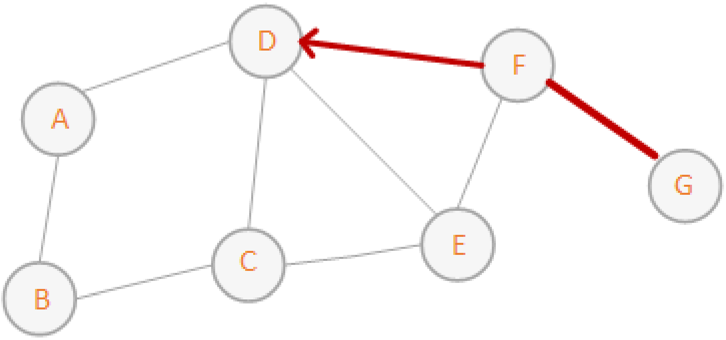


- Nodes B and D verify that this is a new RREQ and that the source_sequence_# is not stale with respect to the reverse route to Node A
- Nodes B and D forward the RREQ
  - -Update source_sequence_# for Node A
  - -Increment hop_cnt in the RREQ packet

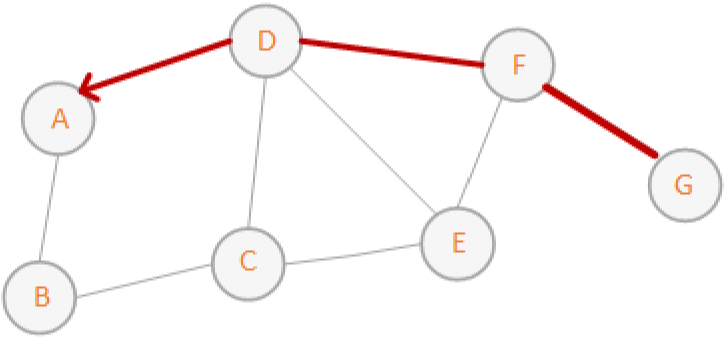
Figure 4. Example of AODV RREQ messages



- RREQ reaches Node F, which knows a route to G
  -Node F must verify that the destination sequence number is less than or equal to the destination sequence number it has recorded for Node G
- Nodes C and E will forward the RREQ packet, but the receivers recognize the packets as duplicates

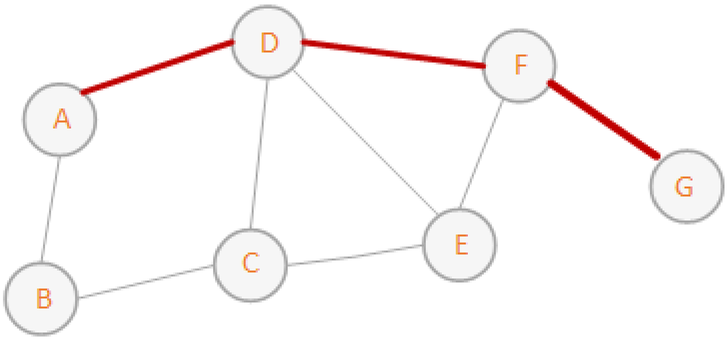


- Node F knows a route to Node G and sends an RREP to Node D
  -source_addr = A
  -dest_addr = G
  -dest_sequence_# = max(own sequence number, dest_sequence_# in RREQ)
  -hop_cnt = 1



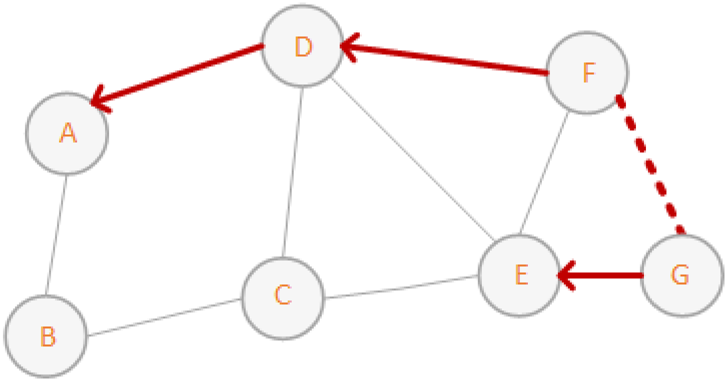
- Node D verifies that this is a new route reply (the case here) or one that has a lower hop count and, if so, propagates the RREP packet to Node A
  -Increments hop_cnt in the RREP packet

Figure 5. Example of AODV RREP messages



- Node A now has a route to Node G in three hops and can use it immediately to send data packets
- Note that the first data packet that prompted path discovery has been delayed until the first RREP was returned

- Route changes can be detected by...
  - -Failure of periodic HELLO packets
  - -Failure or disconnect indication from the link level
  - -Failure of transmission of a packet to the next hop (can detect by listening for the retransmission if it is not the final destination)
- The upstream (toward the source) node detecting a failure propagates an route error (RERR) packet with a new destination sequence number and a hop count of infinity (unreachable)
- The source (or another node on the path) can rebuild a path by sending a RREQ packet



- Assume that Node G moves and link F-G breaks
- Node G issues an RERR packet indicating the broken path
- The RERR propagates back to Node A
- Node A can discover a new route

Figure 6. Example of AODV RERR message

CHAPTER 4

NETWORK SECURITY

Since the beginning of computer networking network security considerations is one of the most important issues that need to be dealt with carefully. At the same time it is one of the hot open topics in research area.

4.1 Security Requirements

After designing any kind of network, in order to make it make sure that the data communications are safe and secure, five general security requirements should be considered and at least one or more should be implemented. [23]

4.1.1 Availability

For any computer network to work properly, its services and information must be available to access when needed. This means that a networking system with its communication channels used to access the information must be always operational and remain available even in case of hardware, power failures or attacks like a DOS attack.

4.1.2 Authenticity

Authenticity is the proof of identity; detecting authenticity in the information security is in two parts: 1. Entity authentication, which is to identify the real identity of the entity that is participating in a transmission, accessing data or requesting service. 2. Data origin authentication, it is necessary to make sure that the data and information sources are genuine.

4.1.3 Confidentiality

Disclosure of information should only be accessible to the authorized individuals. Confidentiality is and assurance (essential but not sufficient) that information is only accessible to authorized entities.

4.1.4 Integrity

Integrity is the assurance that data should not be altered in a transmission and it should remain entire and intact. Data should be protected from any change and alteration by unauthorized entities.

4.1.5 Non Repudiation

It is the assurance that in a network communication both parties cannot later deny their participation. It should be verifiable for a secure network that the sender and receiver in a transmission are really the parties who conducted to do the transmission.

4.2 Network Security Threats

Some of the most common network threats are:

Masquerading: the attacker pretends to have somebody else’s identity.

Eavesdropping: when an attacker node listens to data packets transmitted entire the network to steal valuable information which may be unencrypted.

Location disclosure: an attack in which the attacker can find a specific node or even the whole network structure by analyzing factors like network traffic. Location disclosure can also be performed by eavesdropping.

Security attacks can be targeted against different layers of a network protocol stack.

In order to protect security and neutralize these threats many defensive mechanisms have been proposed and developed. Most of these mechanisms are based on cryptography based algorithms in which data encryption is applied on transmissions and key exchange between nodes.

4.3 Security in Wireless Sensor Networks

Although security solutions like cryptography based algorithms perform pretty well in traditional networks but applying these solutions on wireless sensor networks is almost impossible because of the following reasons:

- Wireless Sensor Networks are highly constrained in resources such as memory, processing capabilities and energy, the resource constraint is a rigid obstacle against applying traditional security mechanism like cryptography solutions which need too much processing power and thus leading to heavy energy consumption.
- The limited energy resources on sensor nodes make them an attractive target for the attackers, in sensor nodes intentionally are forced to carry out security mechanisms repeatedly over and over, this will cause extra power consumption causing victim nodes to quickly run out of energy. The result of this kind of attack is almost equal to denial of service attacks.

4.3.1 DoS Attacks

Generally denial of service attacks aim to disable network services through causing too much pressure on network resources by over using them. In a wireless sensor network the attacker can focus the attacks on an important group of nodes like those near the base station which are mostly needed in routing processes, by destroying these nodes sensor network will become impaired failing to work properly.

Attacks can be targeted against different layers of a wireless sensor network, for example radio jamming is a type of attack against the physical layer of a sensor network in which wireless signals are jammed to make sensor network disabled.

4.3.2 Network Layer Attacks in Wireless Sensor Networks

There are multiple kinds of attacks against network layer of a WSN in which routing procedure is targeted.

Black Hole attacks: in a Black Hole attack the attacker node acts like normal nodes to participate in routing processes, then direct paths to itself and then drops it, or it may act selfish by refusing to pass any traffic at all. [24]

In distance vector based protocols like in AODV, in order to drop data packets the Black Hole attacker node can advertise routing paths by pretending to have exclusively good routes to the base station (higher seq#).

Modification attacks: attacker node can create false route paths by modification of a part or the entire of either the routing packets or data packets. In the presence of false routing paths, data traffic cannot be transmitted to the sink.

The attacker node can create false loops; nodes enter these loops, waste a lot of energy and exhaust which will result in complete depletion. Modification attack may also be against data packet contents.

Sybil attacks: in this type of attack the hostile nodes have got several fake characteristics and pretend to be in numerous locations at the same moment.

Wormhole attacks: in wormhole attacks in order to interrupt routing two attacker nodes cooperate to plot an attack

4.4 Trust mechanism for WSN

Considering WSNs have their own challenges and constraints, applying Security models designed for traditional networks is not enforceable on wireless sensor networks, that's why wireless sensor networks should have Security models of their own, methods specially designed for wireless sensor networks.

This is why it's needed to implement new security mechanisms specially designed for Wireless Sensor Networks.

To overcome these threats and to take appropriate actions against these hostile attacks in Wireless Sensor Networks a mechanism has been proposed which is based on a status mostly used in human relationships in a real life, called as "TRUST". [25]

In this approach, nodes build a relationship based on trust, in this trust based relationship between nodes, establishment of the routing paths in addition to other routing information is also based on the amount of trust they have in their neighbor nodes.

Trust based models are used for routing, data aggregation, choosing cluster head in hierarchical protocols and key exchange. [26]

Trust management approaches are powerful mechanisms for the purpose of diagnosing misbehaving nodes (either intentionally adversary nodes or nodes with failures).

When these unfavorable nodes are identified their neighbor nodes can decide not to cooperate with these nodes in a routing action, data aggregation or other cooperative tasks anymore.

Nowadays Trust is a very hot topic in different kinds of networks like ad hoc, peer to peer and Sensor Networks. A security mechanism based on Trust is more powerful than a traditional cryptography based approaches and it solves obstacles which cryptography methods cannot, like judging on node behavior.

Trust management is an essential need designing secure and trustworthy applications of Wireless Sensor Network.

Along with the development of Wireless Sensor Networks, Trust mechanism are getting more and more attention, nevertheless designing a fully comprehensive and practical model is a difficult task.

As mentioned earlier, Trust is simply the amount of confidence of a node A that a node B will accomplish its tasks as it is expected to do. Evaluation of trust and confidence of a neighbor node is carried out by monitoring neighbors' behaviors; a node may also the opinion of other neighbors about the trustworthiness of a certain node.

The procedure in which trustworthiness of a node is evaluated is called Trust Model.

Trust models are divided into two groups:

4.4.1 Centralized and Distributed Trust models

- Centralized Trust models: in this method one node which is considered to be trustworthy is referred to as a head. This head node evaluates the measure of other nodes trustworthiness. This assessment is performed based on the information collected by the head node itself or the information captured from other nodes. In this approach mostly the head node is the most potent resource rich node in a sensor network. In a better design, sensor network is designed as a heterogeneous hierarchical network and cluster heads which are the most potent nodes are selected as head nodes.

- Distributed Trust models: in a distributed Trust model each node evaluates trustworthiness of its neighbor nodes based on the collected data. Later, routing decision of each node is influenced by the results of those assessments. The advantage of this approach is that further processing and energy expenses of trust assessment are divided entire the network.

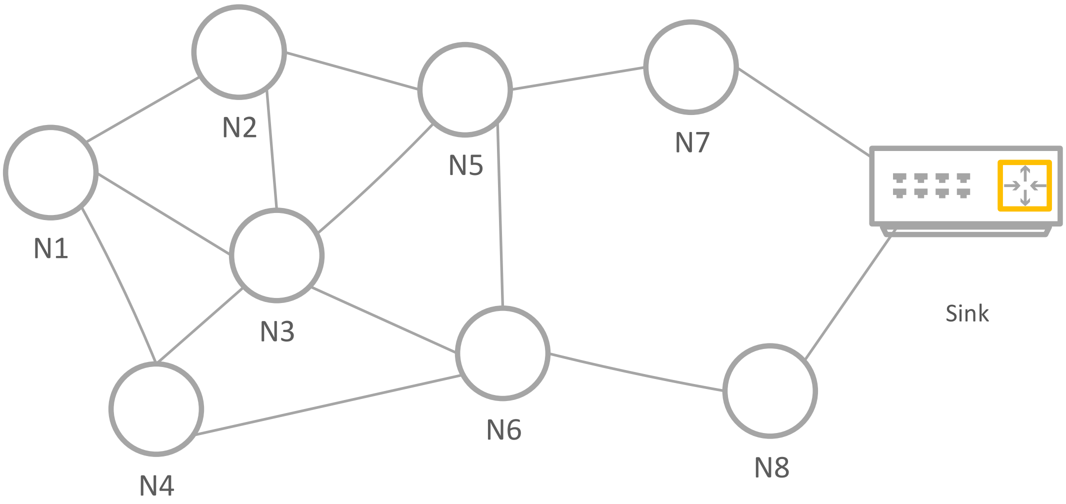


Figure 7. Simple example of a Trust evaluation

For example every time that node N1 in Figure 5 chooses node N3 for transmitting its data, it checks to see whether this transmission was prosperous or not, after a couple of collaborations and data exchange with node N3, node N1 which is considered as the source node here can evaluate the functioning quality of the routing protocol by comparing total number of successfully transmitted packets by node N3 with the total number of transmitted packets.

This method is called direct evaluation of Trust where in an indirect method nodes can also ask other neighbor nodes opinions on Trust evaluation of a certain node to make a judgment about its trustworthiness. for example in Figure 5 Node N1 can ask N2 and N4s Trust evaluation of N3, and by obtaining their opinion and observing N3s behavior by N1 itself, N1 can make a decision about N3s Trustworthiness.

CHAPTER 5

RELATED WORKS

Trust based routing protocols is a hot research topic and there are some pretty successful mechanisms published in the recent papers.

In this part some of the most important Trust management mechanism in Wireless Sensor Networks routing protocols and their cons and pros are briefly mentioned.

5.1 TARF

This mechanism which is presented in implements multi hop routings in wireless sensor network with the trust evaluation of neighbor nodes. TARF identifies the unreachable nodes and skips them in routing decisions.

TARF is an energy efficient and trustworthy routing protocol which is concentrated on a type of attacks in which the attacker node tries to route data traffic towards wrong destinations by creating fake identities.

The advantage of TARF is that it does not need to know nodes geographical information; it is also implemented as a low overhead module in Tiny Os and can be easily executed on existing routing protocols. TARFs main objectives are high throughput, energy awareness and scalability.

Disadvantage of TARF is that it is almost useless against DOS attacks, does not care about having a low latency and balanced traffic load, upon detecting an adversary node in a route TARF establishes a new route path from the beginning. [27]

5.2 TILSRP

Trust integrated link state routing protocol for Wireless Sensor Networks is a new algorithm for establishing a trustworthy route from the source node to the sink with the help of direct and indirect evidences. This model is based on LSR protocol. It’s persistence against different types of attacks has not been evaluated. [28]

5.3 ATSR

A fully distributed algorithm to assess node trustworthiness, in this algorithm nodes collect direct evidence trust by observing their neighbor behaviors based on a series of trust metrics. ATSCR also uses indirect evidence and by adding these two together calculates the total trust value. [29]

5.4 TRUSTEE

TRUSTEE is a routing mechanism based on Trust for WSN with energy constraints. TRUSTEE is a flexible approach for the quality assessment of difficult routes, and then the route which is the most secure one is selected for routing.

In this approach it is presumed that every node has information about its neighbors in addition to that, in order to provide a more secure connection a mechanism of key exchange is also applied between nodes.

TRUSTEE not only lowers the memory-energy consumption and processing overhead it also performs really acceptable against external attacks with its more secure node identity recognition mechanism. [30]

5.5 Trusted GPSR

In this approach the GPSR (Greedy Perimeter Stateless Routing) protocol is developed to make use of Trust, every time a node transforms a packet it waits until its retransmission is also done by the neighbor, and then it rates its neighbors by evaluating their rate of successful or failed transmissions. [31]

5.6 TRANS

In order to avoid unsecure paths in TRANS routing paths are selected from nodes based only on trust information and not based on hop counts and other info. However it is presumed that every node is aware of its geographical location so it also uses that for taking geographical routing decisions.

A trusted neighbor is the one who can decipher the encrypted requests and trustworthy enough (based on its previous transmission results assessed by the sink and other nodes).

A sink sends out packets only to its trusted nodes, upon receiving the packets, nodes forward these packets to a neighbor who is the nearest to the destination. By doing so, packets get to their destinations via a reliable path. [32]

CHAPTER 6

A NOVEL IMPLEMENTATION OF A TRUST BASED AODV

Here in this part we propose a simple yet novel implementation of AODV routing protocol for wireless sensor networks. And then by simulating our proposed Trust Based AODV with the results obtained from the original AODV protocol and comparing simulation results, the advantages and disadvantages of both protocols against Black Hole and modification attacks will be thoroughly studied and evaluated.

The reason for the selection of AODV protocol is that it is one of the most popular protocols for the ad hoc and sensor networks and there are a wide range of papers and research in the past and recent years both in academic and industry focused on uses of AODV in sensor networks.

AODV is fully supported in NS-2 simulator which is by far one of the best simulators which is free and open to use for educational and research purposes.

The reason for choosing to study a security mechanism is that along with latest developments in traditional and sensor networks, security concerns are also growing bigger and more threatening.

Providing security requirements for sensor networks is a demanding subject and an open research and study area which needs more attention to achieve new developments and more improvements on the currently designed mechanism.

6.1 A Proposed Trust Based AODV

The idea behind our proposed Trust based mechanism can be implemented on most routing protocols to overcome multiple types of security attacks against routing protocols in wireless sensor networks.

In this thesis I have chosen AODV for the routing protocol and the Black Hole and modification attacks for the security attacks against my wireless sensor network.

Although the attack types are implemented in our simulation are only for the black hole attacks, but theoretically our mechanism is fully capable of acting against other types of packet dropping and data modification attacks like the Grey Hole attacks. It is only ineffective against eavesdropping attacks because of the lack of any cryptography algorithms.

The idea behind the mechanism for trustworthiness evaluation of neighbor nodes in our thesis is very simple but with promising satisfactory results.

In order to identify adversaries in its neighbor nodes, each node sends out a trust assessment packet containing a data to its neighbor nodes in a predefined periodic time which in our implementation is every 2 seconds.

The data inside the trust evaluation packet can be anything, a simple text data or a multimedia file, but in the implementation of our Trust based AODV protocol and in its simulation we've decided that the data is just a random number.

Neighbors are supposed to receive this data, apply a predefined change on the data and send it back to the node. (In this implementation the data which is a random number would be incremented by one).

The reason for sending out trust assessment packets with the data inside is to see whether the neighbor node delivers this data back to the destination or not, and also to check whether the data delivered back is intact or not.

By performing the increment operation which is in fact a very simple processing task, nodes are being examined to make sure whether data packets are opened and correctly processed before the retransmission or not.

6.2 Implementation

In addition to RREQ, RREP, RERR and Hello messages which are the original route discovery and maintenance packets in AODV, we provide our Trust based AODV algorithm with another extra packet to evaluate the amount of trustworthiness in neighbor nodes. We can call this packet the Trust Assessment packet or simply Security Test packet.

First of all each node ranks its neighbor nodes with the Trust value of 100%, then for every packet that it does not receive back in time, it reduces 10% from the sender nodes Trust value and if the data is received back but its changed not as expected, then it reduces 20% from the sender nodes Trust value.

After several number of failed exchanges when the Trust value of a malicious node reaches to 0%, the source node puts it into its blacklist and totally blocks this neighbor from future transmissions.

The reason that there is 10% reduction for not receiving the security test packet back and 20% for the reception of data with an unexpected change is that in the first case when the data is dropped and not received back although it can be a clear sign of an ongoing Black Hole attack but in few conditions such a problem might also be as a result of a temporary failure in transmission media, noise failure, or it might even be stuck and waiting inside a queue.

On the other hand, an unexpected change in the content of the data looks mostly like an adversary node that is modifying the data intentionally.

Upon putting a neighbor node in the black list, it is identified as an adversary node and no packet would be forwarded to it afterwards.

An attacker node can also produce corrupt data or even false route reply messages to advertise wrong routes to a destination, so any packets received from a blacklisted node must also be dropped because of the very probable risk of being a corrupted data.

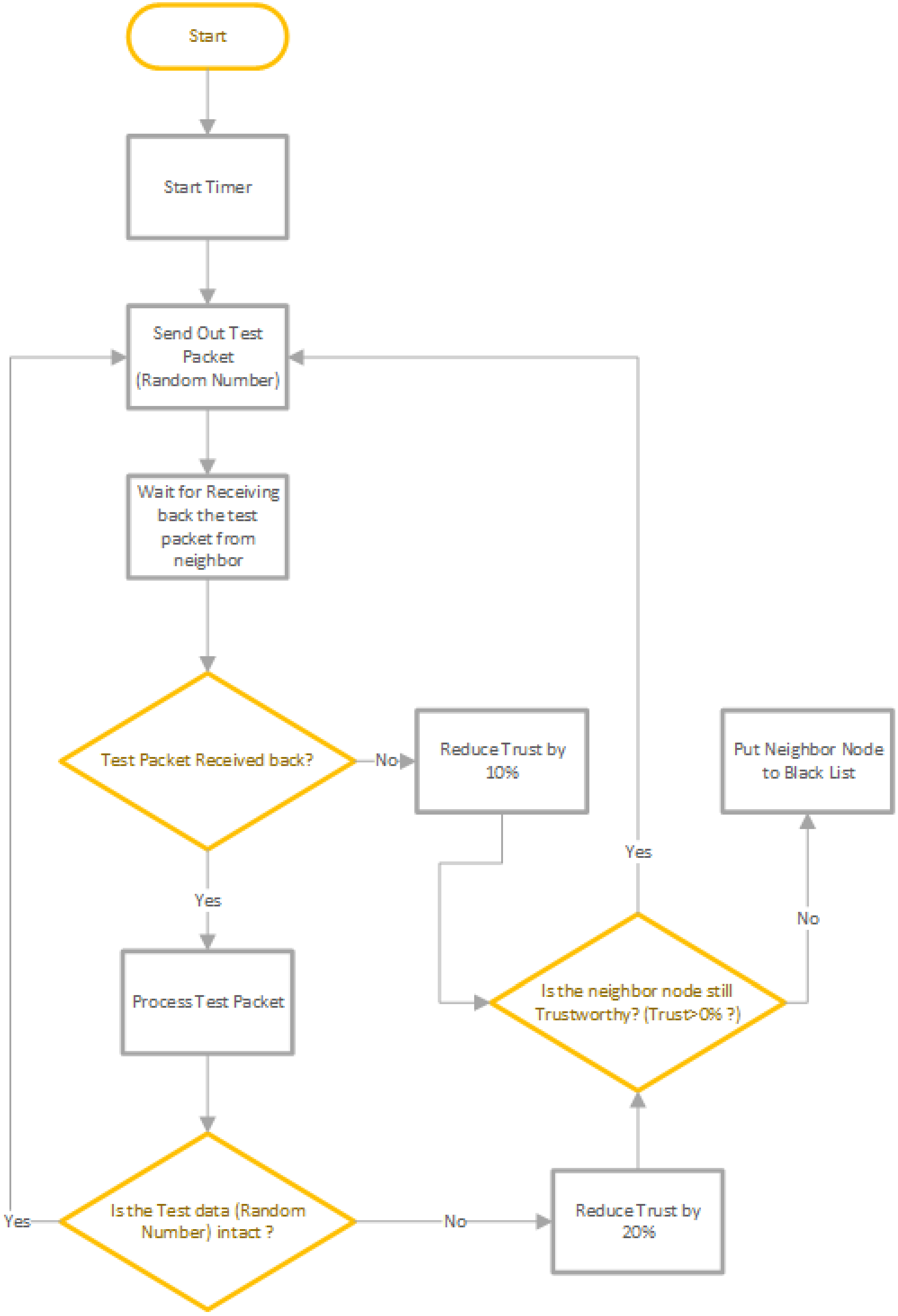

Start
Start Timer
Send Out Test Packet (Random Number)
Wait for Receiving back the test packet from neighbor
Test Packet Received back?
No
Reduce Trust by 10%
Put Neighbor Node to Black List
Yes
Yes
No
Process Test Packet
Is the neighbor node still Trustworthy? (Trust>0% ?)
Yes
Is the Test data (Random Number) intact ?
No
Reduce Trust by 20%

Figure 8. Process of identifying malicious nodes

As shown in the figure above, the Trust evaluation process starts with sending out a test packet to neighbor nodes, waiting for receiving it back in time with the random number inside it incremented by one. After each trust reduction, the algorithm checks to see whether the amount of trust value reached zero and it’s time to block the neighbor node as an adversary node or if it’s still too soon to lose trust in a neighbor.

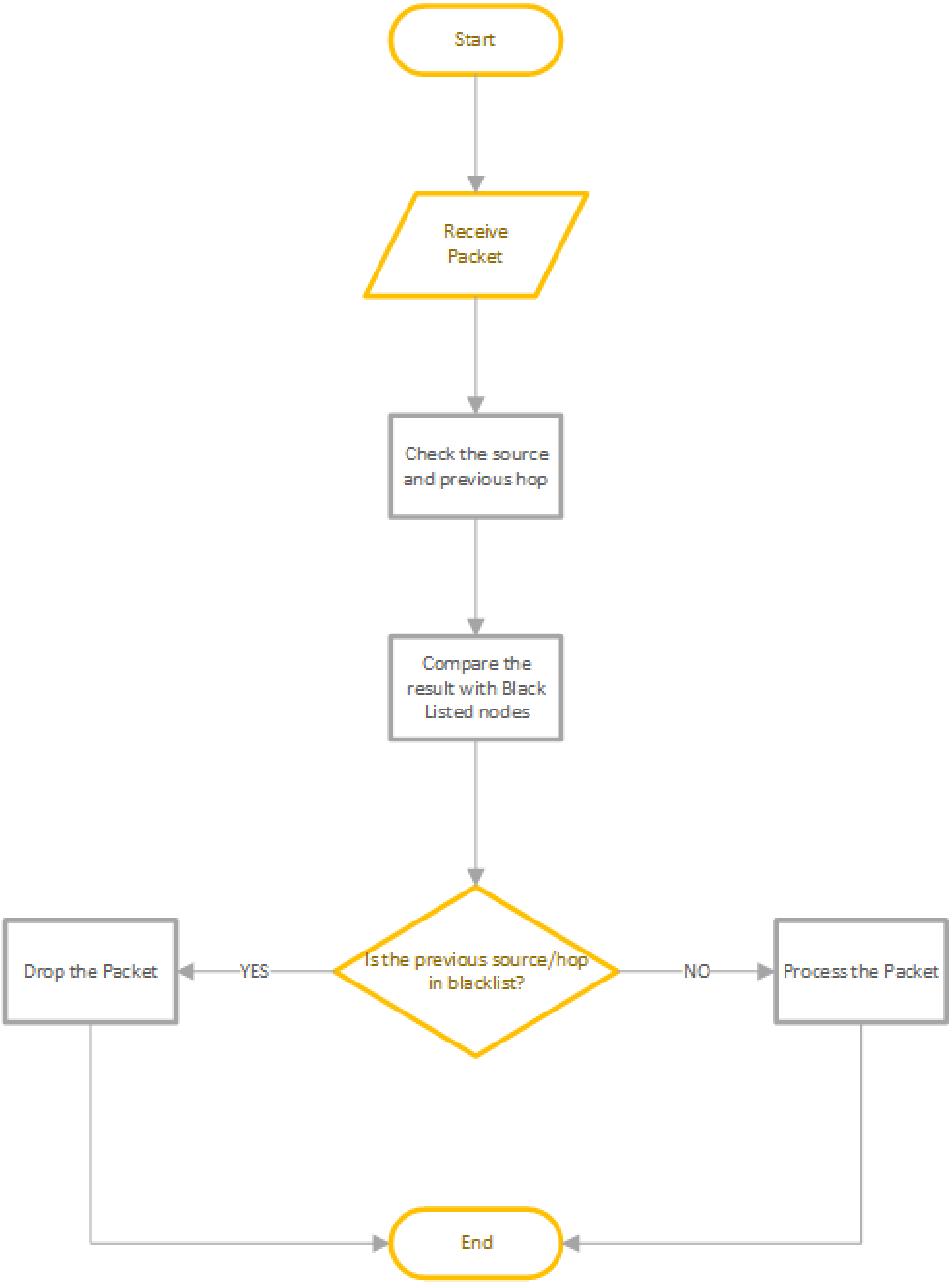

Start
Receive Packet
Check the source and previous hop
Compare the result with Black Listed nodes
Is the previous source/hop in blacklist?
YES
Drop the Packet
NO
Process the Packet
End

Figure 9. Dropping defective packets received from adversary nodes

Figure above demonstrates an additional security gimmick to identify and drop defective packets received from already black listed nodes. This process is efficiently effective against those attacker nodes which may produce false data packets or pretend to have a fresh route with low number of hops to a destination by advertise false routing request messages. These false data and route advertisement are methods applied by most recent security attacks which were described earlier. These types of attacks not only drop the packets but also tend to sabotage the network and its output results by producing corrupted data deliberately. This process ensures that our Trust based algorithm can be effective against multiple types of security attacks.

CHAPTER 7

SIMULATION

In the fields of communication and computer networks technology, a network simulation technique is where a software tool models the total comportment of a computer network and gives a user the ability to get a better understanding of how the planned network even if it is too complex and in a large scale will perform under multiple conditions in a real world scenario without any need for an actual physical implementation of expensive network equipment.

7.1 Simulator selection

Computer networks simulation is a branch of knowledge in computer science and network engineering that has gained a widespread use and is of substantial importance in the design and evaluation of multiple types of computer networks.

7.1.1 NS-2

Ns-2 is a free software publicly available under the GNU GPLv2 license for research, development, and use. Ns-2 provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

NS2 is a discrete event simulator that is written in C++, it has got an OTCL interpreter shell which is used as a user interface allowing simulation TCL scripts to be ran. Most of the networking principles in NS2 are designed as classes in an object oriented manner. [33]

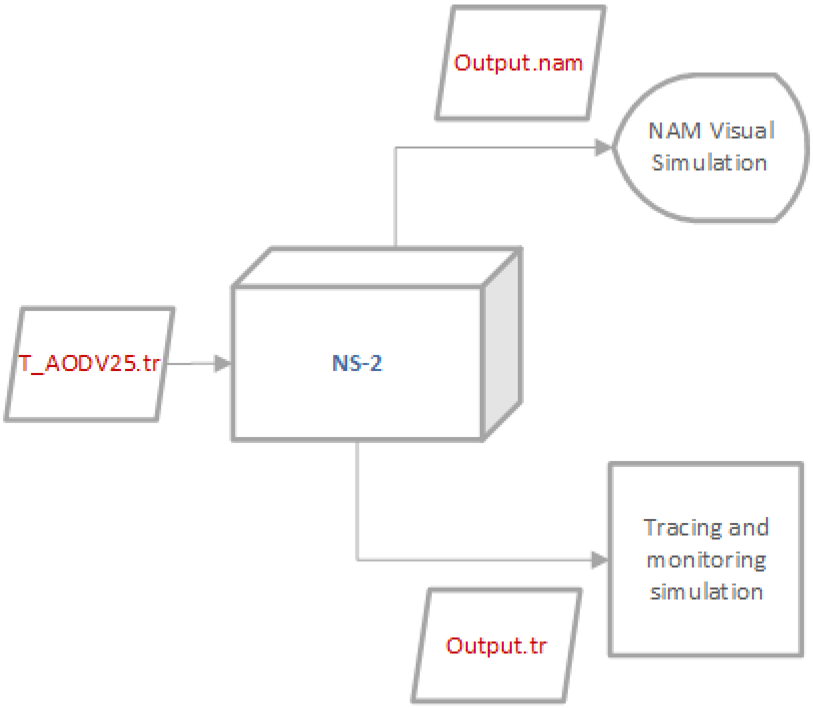


Figure 10. Flowchart of events for a simulation in NS -2

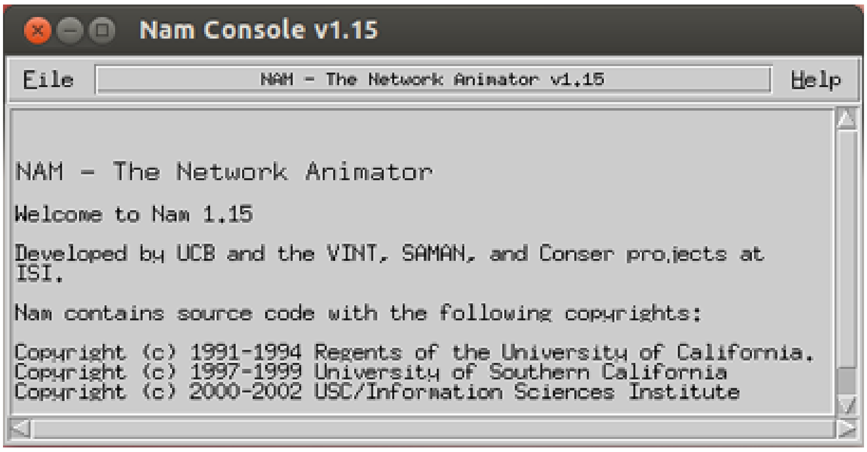
Ns-2s output files are .nam graphical animation output and .tr trace files. The first one is associated with Nam which is the Ns-2s Network Animator, when the simulation is complete, Ns-2 attempts to run a Network Animator visualization of the simulation on the screen.

.tr trace files can be used in tools like xgraph and Gnuplot or be analyzed by means of python or AWK scripts. We have used AWK scripts to extract useful data from our huge in size trace result files.

7.1.2 Nam Network Animator

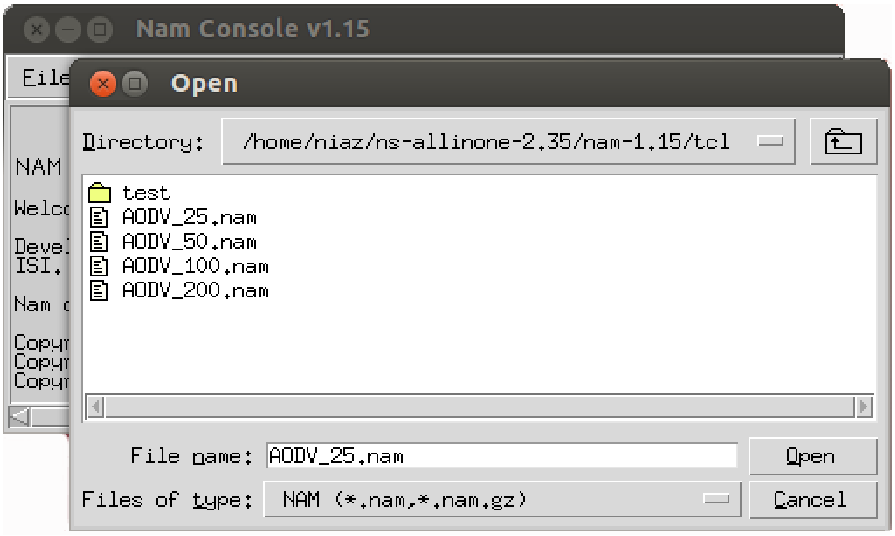
Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet traces. Nam is used to visualize ns-2 simulations and is mainly intended as a companion animator to the ns simulator.

It supports topology layout, packet level animation, and various data inspection tools.



```
NAM - The Network Animator
Welcome to Nam 1.15
Developed by UCB and the VINT, SAMAN, and Conser projects at
ISI.
Nam contains source code with the following copyrights:
Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Figure 11. The Network Animator Console in NS-2



Directory: /home/niaz/ns-allinone-2.35/nam-1.15/tcl

```
test
AODV_25.nam
AODV_50.nam
AODV_100.nam
AODV_200.nam
```

File name: AODV_25.nam

Files of type: NAM (*.nam,*.nam.gz)

Figure 12. Opening nam trace files in NS-2s Network Animator NAM

The first step to use nam is to produce a nam trace file. The nam trace file should contain topology information like nodes, links, queues, node connectivity etc as well as packet trace information. [35]

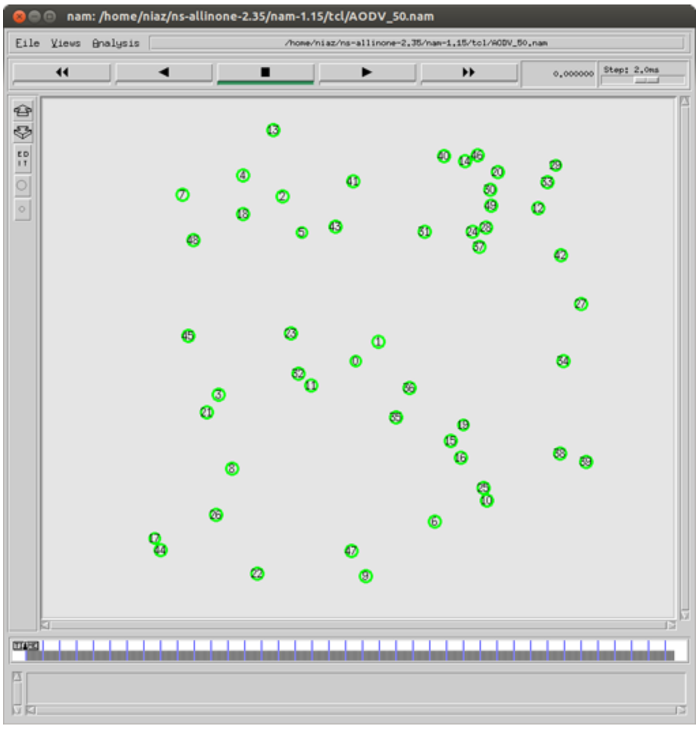

nam: /home/niaz/ns-allinone-2.35/nam-1.15/tcl/AODV_50.nam
File
Views
Analysis
/home/niaz/ns-allinone-2.35/nam-1.15/tcl/AODV_50.nam
0.000000
Step: 2.0ms

Figure 13. Nam console in a scenario with 50 nodes. Idle state

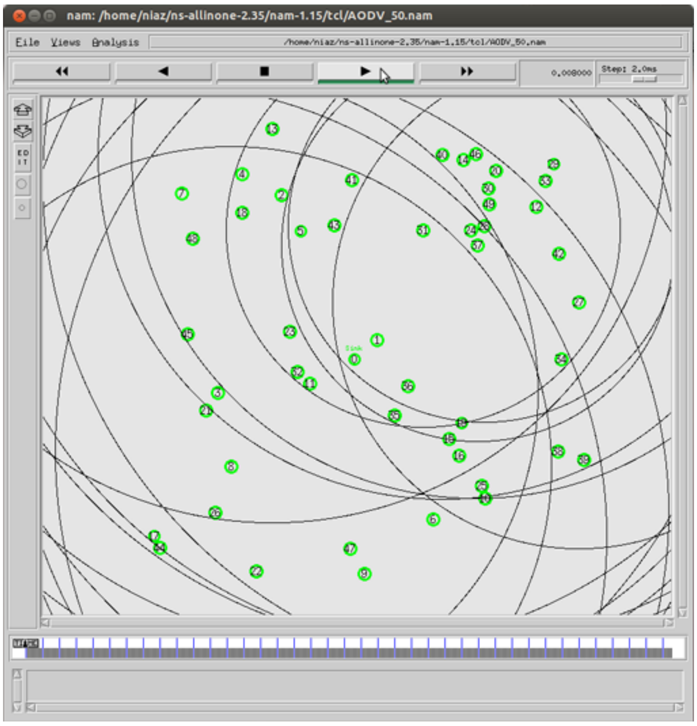

nam: /home/niaz/ns-allinone-2.35/nam-1.15/tcl/AODV_50.nam
File
Views
Analysis
/home/niaz/ns-allinone-2.35/nam-1.15/tcl/AODV_50.nam
0.008000
Step: 2.0ms

Figure 14. Nam console in a scenario with 50 nodes. CBR-UDP transmission

7.2 Simulation setup, results and analysis

In this part of our work we will present a thorough demonstration of simulation results in 8 different scenarios of Trust based and simple AODV routing protocols against Black Hole and modification attacks.

In order to obtain and demonstrate a conclusion on how our proposed Trust based routing protocol will perform in real life, and to get to know its advantages and disadvantages, each scenario will be analyzed and discussed separately and thoroughly by evaluating protocol behavior with 3 different performance metrics in each scenario.

After making comparisons in each different scenario a final conclusion will be derived to sum up the end of the story.

We have developed 8 main scenarios in wireless sensor networks, in the first four scenarios which will be simulated on 25, 50, 100 and 200 fixed nodes.

The number of malicious nodes in each scenario is 5, the first four scenarios is to evaluate what are the differences in the influences of 5 malicious nodes in a network with lower and higher number of nodes running AODV and a Trust based AODV against 5 malicious nodes performing Black Hole or modification attacks and how does the proposed Trust based model treats with 5 adversary nodes in sensor networks with 25, 50, 100 and 200 nodes.

In the second four scenarios the number of malicious nodes will be gradually increased from 10 to 20, 30 and finally 40 malicious nodes in sensors with 25, 50, 100 and 200 nodes to analyze the effects of a sudden increase in the number of hostile nodes with different ratio of malicious to friendly nodes on the proposed Trust based algorithm and compare the results with the same setup running with the AODV.

In all scenarios the area size is 120 x 120 m and simulation time for each scenario is 1000 seconds with constant bit rate traffic.

Table 1. Parameters and Values for the first four scenarios

Parameters	**Values**
Area Size	120 x 120
Traffic Service	CBR (Constant Bit Rate)
Number Nodes	25, 50, 100, 200
Node Types	Fixed
Packet Size	50 Kb
Transmission Rate	0.1 mbps
Interval	2 milliseconds
Simulation Time	1000 seconds

Adversary nodes are manually selected for each scenario in a separate Ns2 TCL script before the simulation. The location of all nodes except node 0 are random by using a sequence of random numbers for each scenario, but in order to make sure that the comparison between our proposed Trust based AODV and the normal AODV is completely fair with same the conditions in which all nodes in two simulation are exactly in the same locations, we should use the same sequence of random numbers for every two scenario for AODV and TB-AODV.

Node 0 which acts as our Sink node is always located at the center of the area.

All other nodes are supposed to direct data towards the sink Adversary nodes are running Black Hole attacks, Black Hole attacks try to act as normal nodes to receive the data, an adversary node running Black Hole tries to disable routing procedure by dropping packets.

In newer version of Black hole attacks which is a kind of combination between Grey Hole and modification attacks, the attacker node attracts route paths to itself with advertising wrong higher sequence numbers and lower hop numbers to say that they have new good paths to destination with low number of hops.

The latter can also be prevented by decreasing trustworthiness value and eventually blocking nodes which perform intentional data modification on our trust assessment packet.

Table 2. A Quick look into some lines of our Trust Based AODV algorithm

Setting up Trust timer

```
void
TrustTimer::handle(Event*) {
  agent->sendTrust();
  double interval = TRUST_INTERVAL;
  assert(interval >= 0);
  Scheduler::instance().schedule(this, &intr, interval);
}
```

Sending out Trust Assessment Packet

```
void
AODV::sendTrust() {
   Packet *p = Packet::alloc();
   struct hdr_cmn *ch = HDR_CMN(p);
   struct hdr_ip *ih = HDR_IP(p);
   struct hdr_aodv_trust *tr = HDR_AODV_TRUST(p);

   #ifdef DEBUG
   fprintf(stderr, "sending TRUST from %d at %.2f\n",
index, Scheduler::instance().clock());
   #endif // DEBUG

   tr->tr_type = AODVTYPE_TRUST;
   tr->seqno = trustSeqno++;
   tr->source = index;
   tr->number=Random::uniform(0.0,3.0);

   AODV_Trust *trust = tr_lookup(tr->source,tr->seqno);
   if(trust == 0) {
      tr_insert(tr->source,tr->seqno,tr->number);
   }
   else {
      if(tr->number-1.0 != trust->number){
         AODV_Neighbor *nb=nb_lookup(tr->source);
         if(nb){
            nb->decreaseTrust();
            nb->decreaseTrust();
         }
      }
      trust->update();
   }

   // ch->uid() = 0;
   ch->ptype() = PT_AODV;
   ch->size() = IP_HDR_LEN + tr->size();
   ch->iface() = -2;
   ch->error() = 0;
   ch->addr_type() = NS_AF_NONE;
   ch->prev_hop_ = index;          // AODV hack

   ih->saddr() = index;
   ih->daddr() = IP_BROADCAST;
   ih->sport() = RT_PORT;
   ih->dport() = RT_PORT;
   ih->ttl_ = 1;

   Scheduler::instance().schedule(target_, p, 0.0);
}
```

Receive and Evaluation of Trust Assessment Packet

```
void
AODV::recvTrust(Packet *p) {
   struct hdr_cmn *ch = HDR_CMN(p);
   struct hdr_ip *ih = HDR_IP(p);
   struct hdr_aodv_trust *tr = HDR_AODV_TRUST(p);
   AODV_Trust *trust;
   trust = tr_lookup(tr->source,tr->seqno);
   if(trust != 0) {
      trust->update();
   }else{
      Packet *p0 = Packet::alloc();
      struct hdr_cmn *ch0 = HDR_CMN(p0);
      struct hdr_ip *ih0 = HDR_IP(p0);
      struct hdr_aodv_trust *tr0 = HDR_AODV_TRUST(p0);

      tr0->tr_type = AODVTYPE_TRUST;
      tr0->seqno = tr->seqno;
      tr0->source = tr->source;
      tr0->number=tr->number+1.0;
 // ch->uid() = 0;
      ch0->ptype() = PT_AODV;
      ch0->size() = IP_HDR_LEN + tr0->size();
      ch0->iface() = -2;
      ch0->error() = 0;
      ch0->addr_type() = NS_AF_NONE;
      ch0->prev_hop_ = index;          // AODV hack

      ih0->saddr() = index;
      ih0->daddr() = tr->source;
      ih0->sport() = RT_PORT;
      ih0->dport() = RT_PORT;
      ih0->ttl_ = 1;

      Scheduler::instance().schedule(target_, p0, 0.0);
   }
   Packet::free(p);
}
```

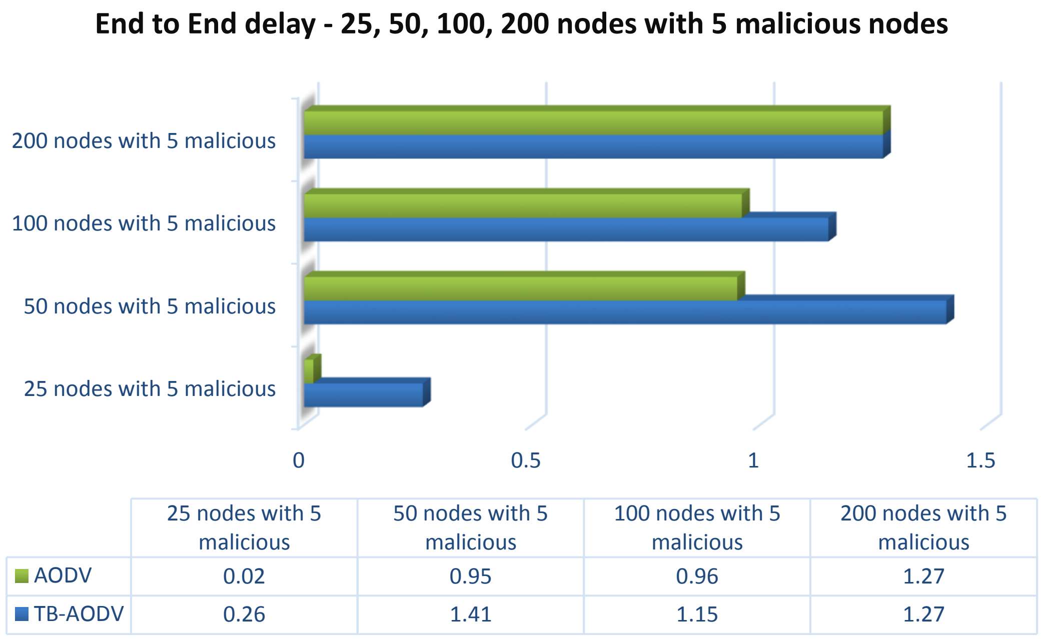
Reducing Trustworthiness Value

```
void decreaseTrust(){trustDegree-=0.1;}
```

Putting an Adversary Node in Black List

```
void
AODV::bl_insert(nsaddr_t id) {
   AODV_BlackList *bl = new AODV_BlackList(id);
   assert(bl);
   LIST_INSERT_HEAD(&blackList, bl, bl_link);
}
```

7.2.1 End to end delay



	25 nodes with 5 malicious	50 nodes with 5 malicious	100 nodes with 5 malicious	200 nodes with 5 malicious
🟩 AODV	0.02	0.95	0.96	1.27
🟦 TB-AODV	0.26	1.41	1.15	1.27

Figure 15. End to End delay - 25, 50, 100, 200 nodes with 5 malicious nodes (Bar Chart)

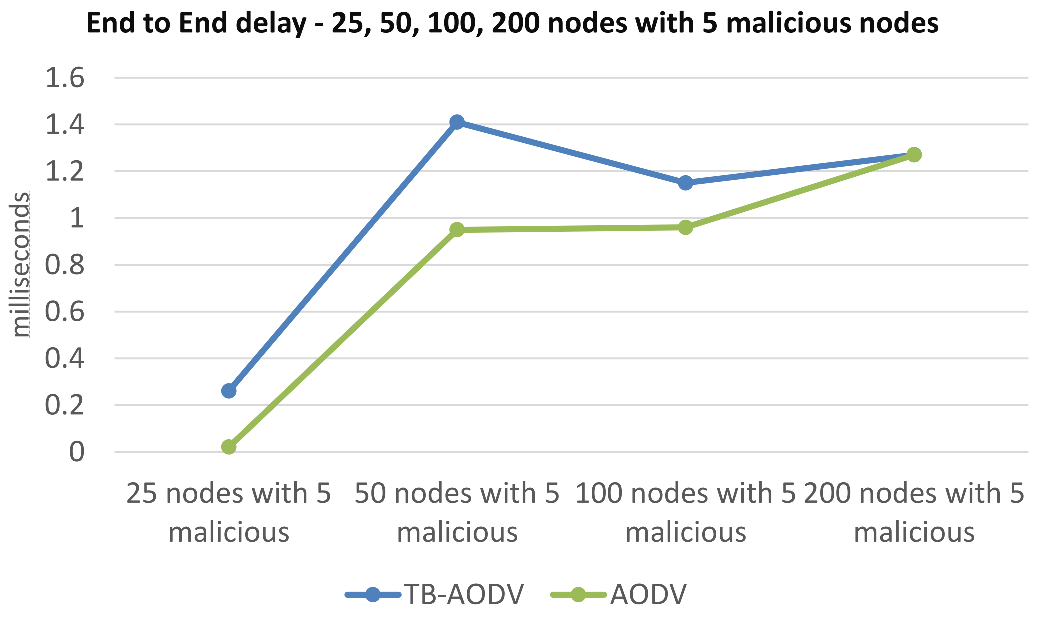


Figure 16. End to End delay - 25, 50, 100, 200 nodes with 5 malicious nodes (Line Chart)

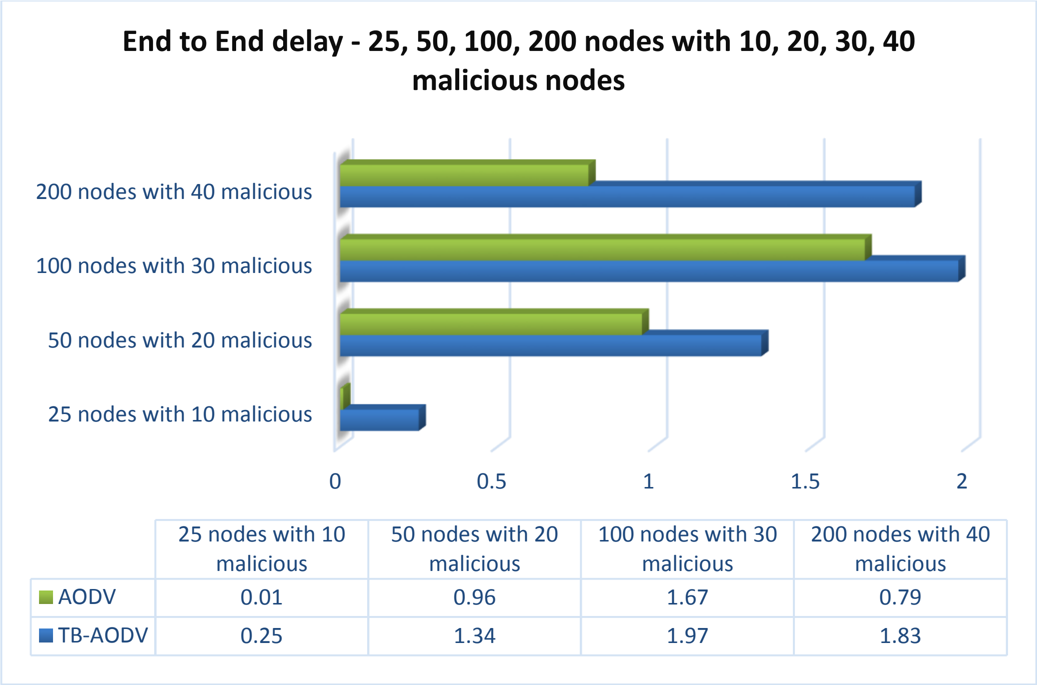
It is both logically and practically obvious that the amount of the End to End value in a protocol in which there are more processing tasks must be higher.

Getting a higher delay in a world where lower delay is always preferable is clearly a disadvantage but the amount of delay here in our simulation and its difference with the original AODV protocols End to End value which are only differences in milliseconds should not be considered as a big deal and can easily be tolerated in exchange of a higher security and lesser packet loss.

In the first four scenarios with 25, 50, 100, 200 nodes where there are only 5 malicious nodes among them, although our Trust Based AODV has a higher End to End value that is in some cases several times higher than the original AODV, but both graphs above clearly show that the difference between the amount of the delays in AODV and Trust based AODV becomes less and less when the number of nodes grow higher, interestingly in the scenario with 200 nodes and 5 malicious nodes, the value for End to End delay is equal and it shows that a higher growth in number of nodes in AODV with only 5 malicious nodes will led to higher values of end to end delay.

The reason for higher end to end delays in TB-AODV is that the Trust based protocol has to send an extra trust evaluation packet and also has to perform extra processing tasks to evaluate trust values in order to perform transmission based on Trust.

Assessment of this Trust evaluation takes time and makes Trust based AODV perform with more delay rates in scenarios with the stated number of friend and foe nodes.



	25 nodes with 10 malicious	50 nodes with 20 malicious	100 nodes with 30 malicious	200 nodes with 40 malicious
🟩 AODV	0.01	0.96	1.67	0.79
🟦 TB-AODV	0.25	1.34	1.97	1.83

Figure 17. End to End delay - 25, 50, 100, 200 nodes - 10, 20, 30, 40 malicious (Bar)

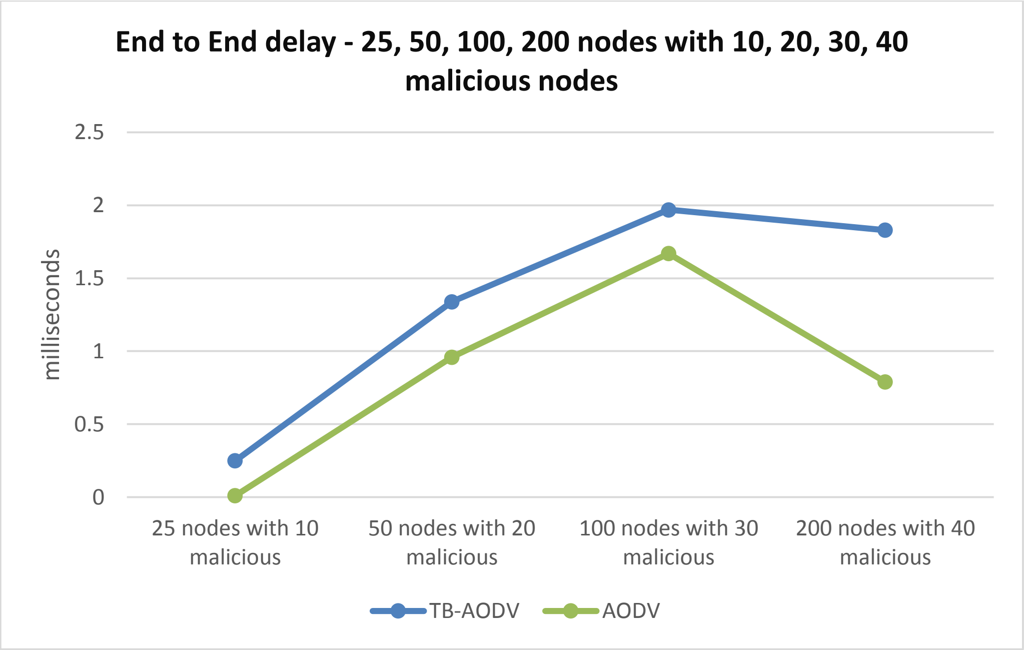


Figure 18. End to End delay - 25, 50, 100, 200 nodes - 10, 20, 30, 40 malicious (Line)

In the last four scenarios with 25, 50, 100, 200 nodes with 10, 20, 30 and 40 malicious nodes Trust based AODV still acts as it's expected.

In the with 200 nodes and 40 attacker nodes the End to End value of Trust based AODB is nearly two times higher than the AODV.

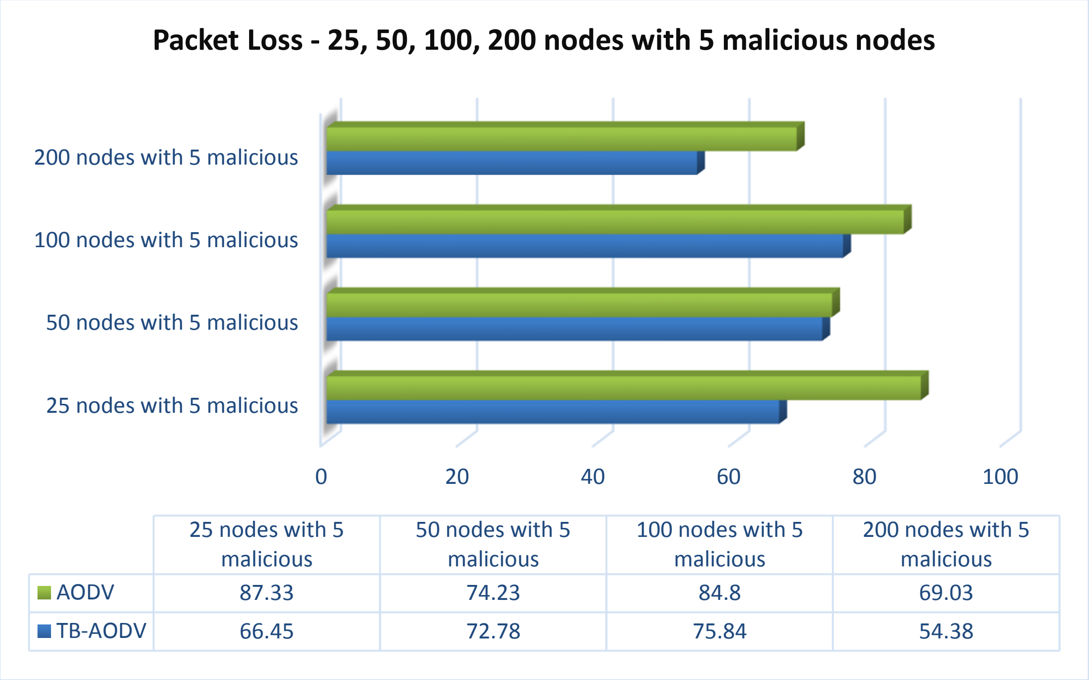
In the last two scenarios with higher number of nodes which is 30 and 40, by closely observing the results presented in the graphs above, it can be concluded that by increasing node numbers where the number of malicious nodes are also increasing by a higher rate, the ratio of End to End delay in Trust Based AODV to the original AODV is also getting higher and its plausible that in a scenario with a much more number of nodes there might be End to End values for TB-AODV multiples times higher than the End to End value for the same scenario with the original AODV protocol.

As mentioned earlier the main reason for higher End to End values in TB-AODV, might be because of the extra packet containing a random number that is used to assess neighbor node values.

Extra Trust assessment packets, extra waiting for getting a reply for these packets, extra processing and all these extra stuff for obtaining a higher security causes more delay values than a protocol without a security mechanism.

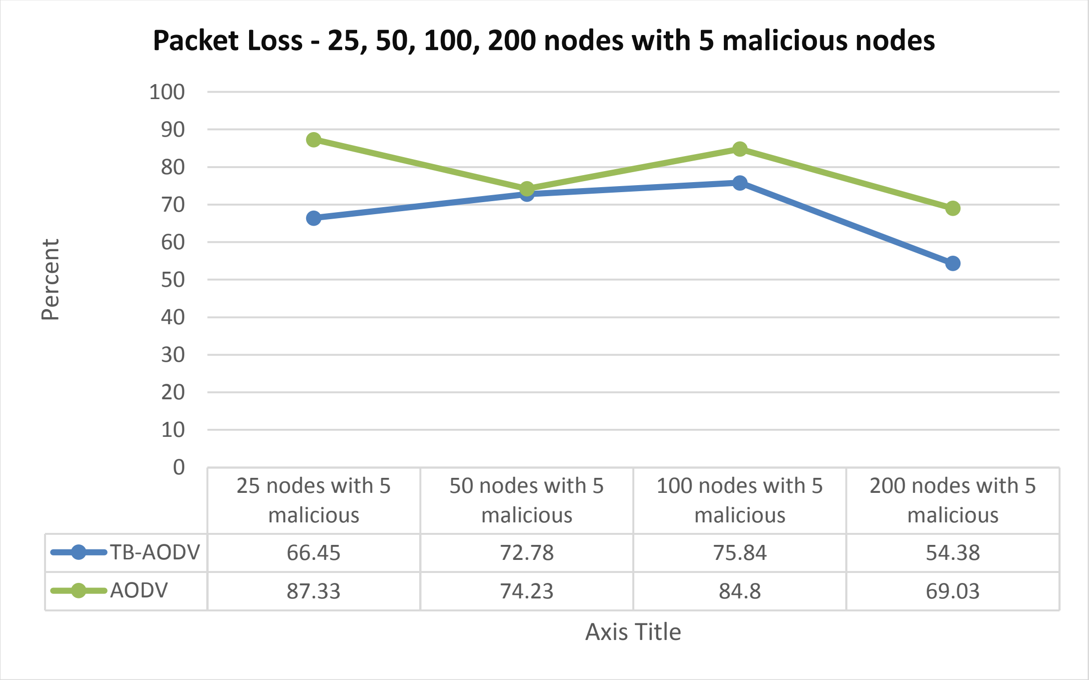
7.2.2 Packet Loss

Packet loss is the number of packets dropped by nodes, the reason could be simple errors like collisions and time out failures but in a scenario when there are adversary nodes performing Black Hole attacks, most of the dropped packets are related to enemy nodes, in a Black Hole attack packets are dropped intentionally by attacker nodes.



	25 nodes with 5 malicious	50 nodes with 5 malicious	100 nodes with 5 malicious	200 nodes with 5 malicious
🟩 AODV	87.33	74.23	84.8	69.03
🟦 TB-AODV	66.45	72.78	75.84	54.38

Figure 19. Packet Loss - 25, 50, 100, 20

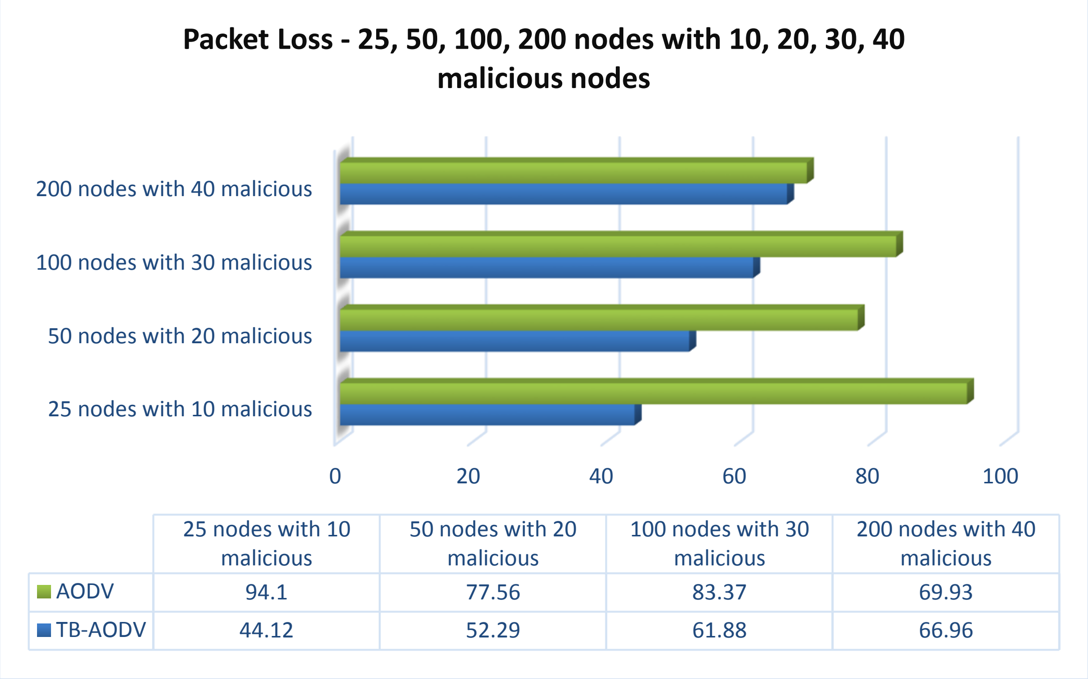


	25 nodes with 5 malicious	50 nodes with 5 malicious	100 nodes with 5 malicious	200 nodes with 5 malicious
TB-AODV	66.45	72.78	75.84	54.38
AODV	87.33	74.23	84.8	69.03

Figure 20. Packet Loss - 25, 50, 100, 200 nodes with 5 malicious nodes (line Chart)

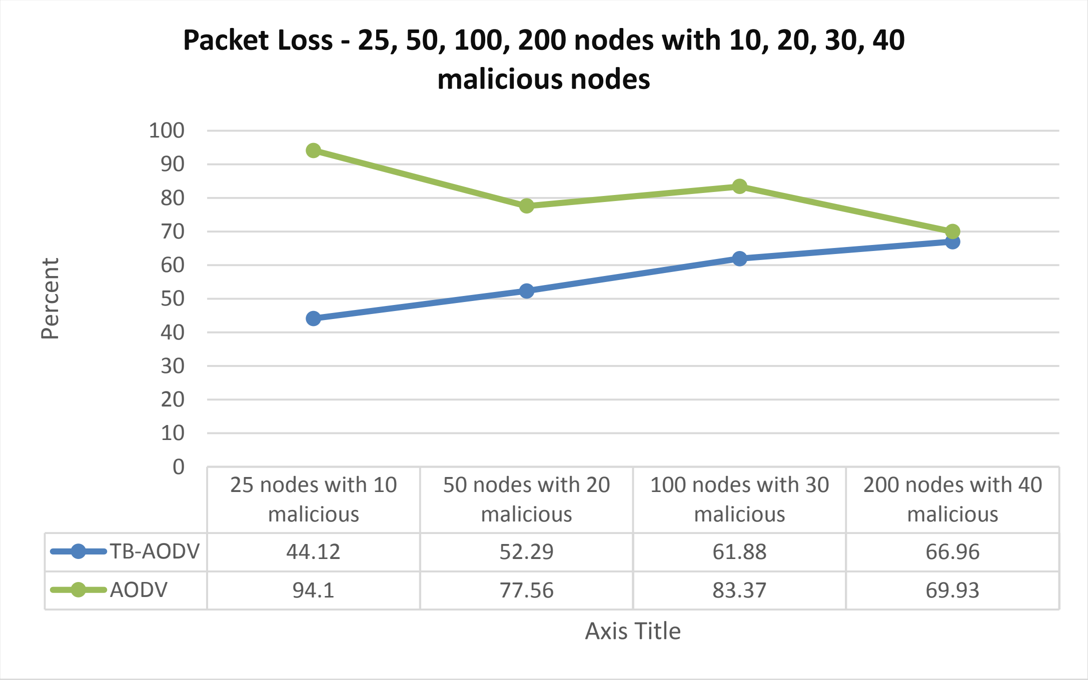
First two graphs represent packet loss value in the first four scenarios of our simulation with 25, 50, 100, 200 nodes, all with 5 malicious nodes.

In all scenarios TB-AODV has a significantly better performance in packet loss rate with the use of its Trust based security mechanism to defend routing procedure against Black Hole attacks which are targeted against routing protocols with the aim of dropping and altering the data. A lower data loss proves that TB-AODV is successful against Black Hole attacks.



	25 nodes with 10 malicious	50 nodes with 20 malicious	100 nodes with 30 malicious	200 nodes with 40 malicious
🟩 AODV	94.1	77.56	83.37	69.93
🟦 TB-AODV	44.12	52.29	61.88	66.96

Figure 21. Packet Loss - 25, 50, 100, 200 nodes - 10, 20, 30, 40 malicious nodes (Bar)



	25 nodes with 10 malicious	50 nodes with 20 malicious	100 nodes with 30 malicious	200 nodes with 40 malicious
TB-AODV	44.12	52.29	61.88	66.96
AODV	94.1	77.56	83.37	69.93

Figure 22. Packet Loss - 25, 50, 100, 200 nodes - 10, 20, 30, 40 malicious nodes (Line)

Like previous 4 scenarios, same story continues with TB-AODV acting better than AODV with a lower rate of data loss when the number of adversary nodes grows higher.

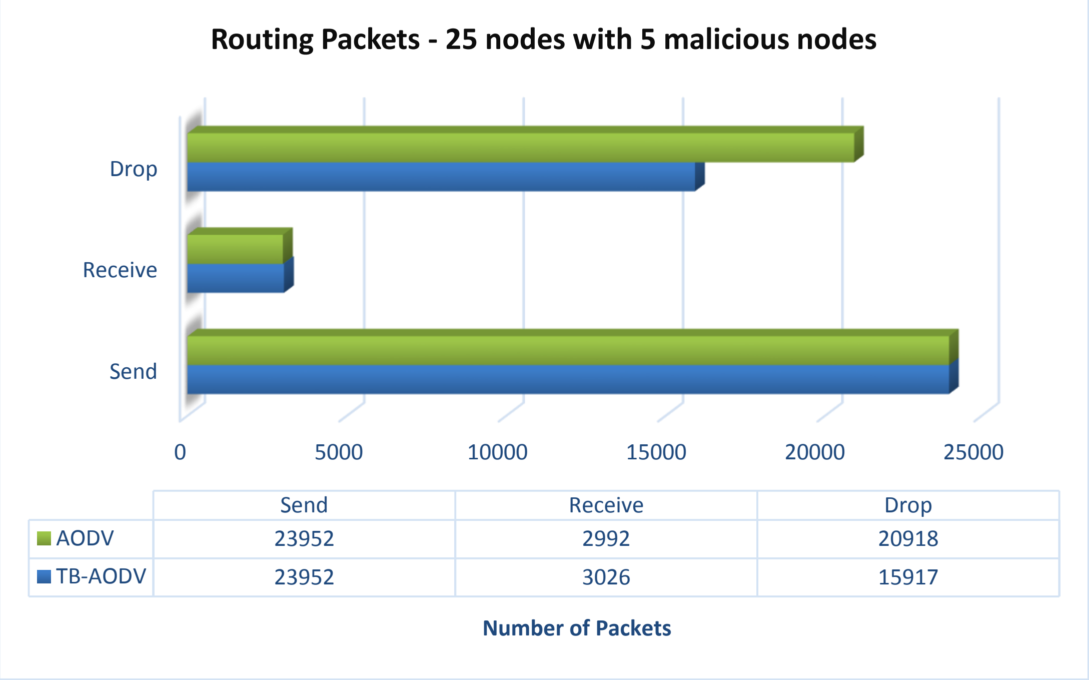
For example in the scenario with 25 nodes and 10 malicious nodes, although 40 percent of the sensor nodes are malicious but TB-AODV has got two times lower rates of packet loss.

TB-AODV is still the winner protocol and easily outperforms AODV by a much lower rate of data loss.

This clearly proves that TB-AODV is successful in neutralizing Black Hole attacks and lowering packet drops and thus getting a lower data loss ratios.

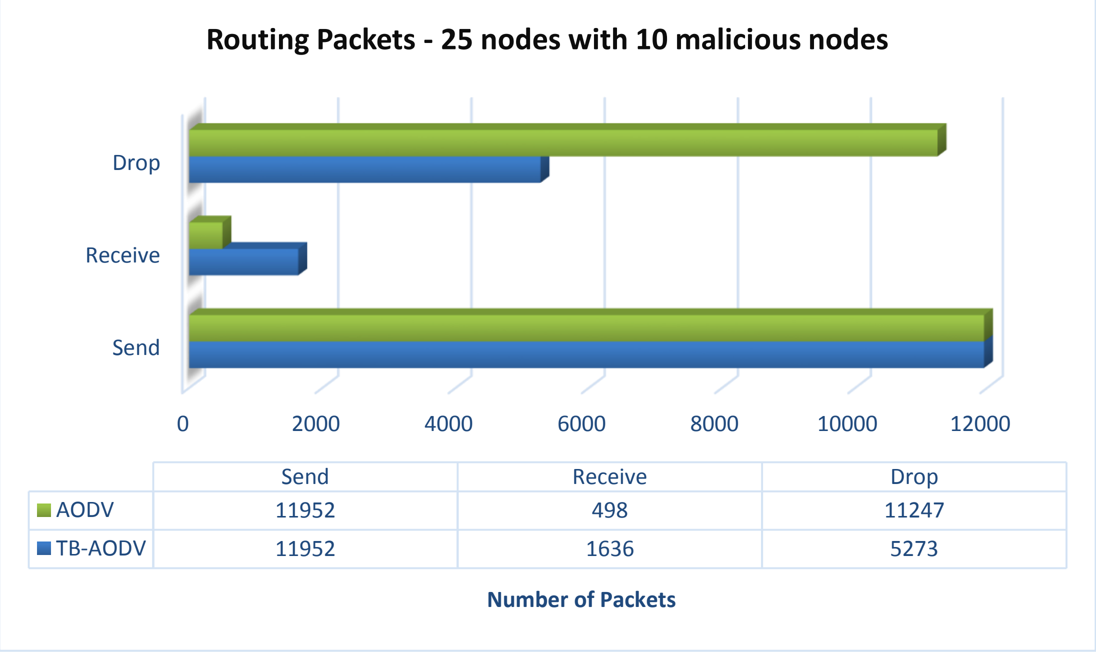
7.2.3 Routing Packets

Shows the total number of packets sent, received and dropped during the simulation time, for both protocols these numbers may vary because of the fact that in Trust based AODV there are extra overhead tasks which may cause some delays more than packets life time and reduce the number of received packets but by a lower data loss rate mentioned earlier, TB-AODV would have a lower drop rate by avoiding Black Hole attacks.



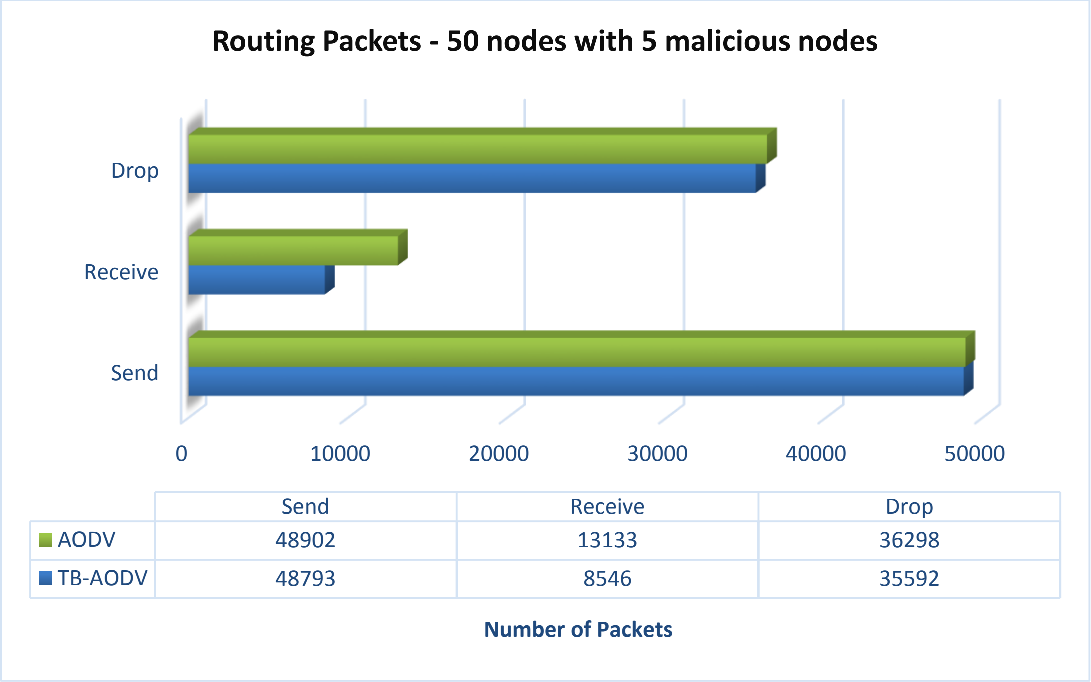
	Send	Receive	Drop
🟩 AODV	23952	2992	20918
🟦 TB-AODV	23952	3026	15917

Figure 23. Routing Packets - 25 nodes with 5 malicious nodes



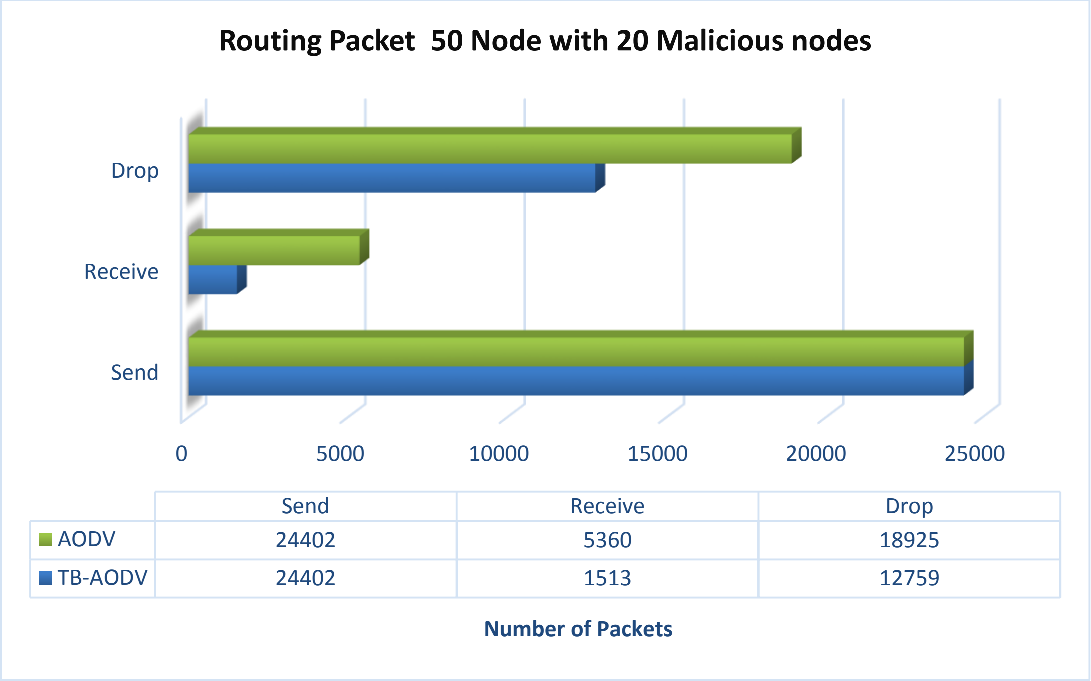
	Send	Receive	Drop
🟩 AODV	11952	498	11247
🟦 TB-AODV	11952	1636	5273

Figure 24. Routing Packets - 25 nodes with 10 malicious nodes



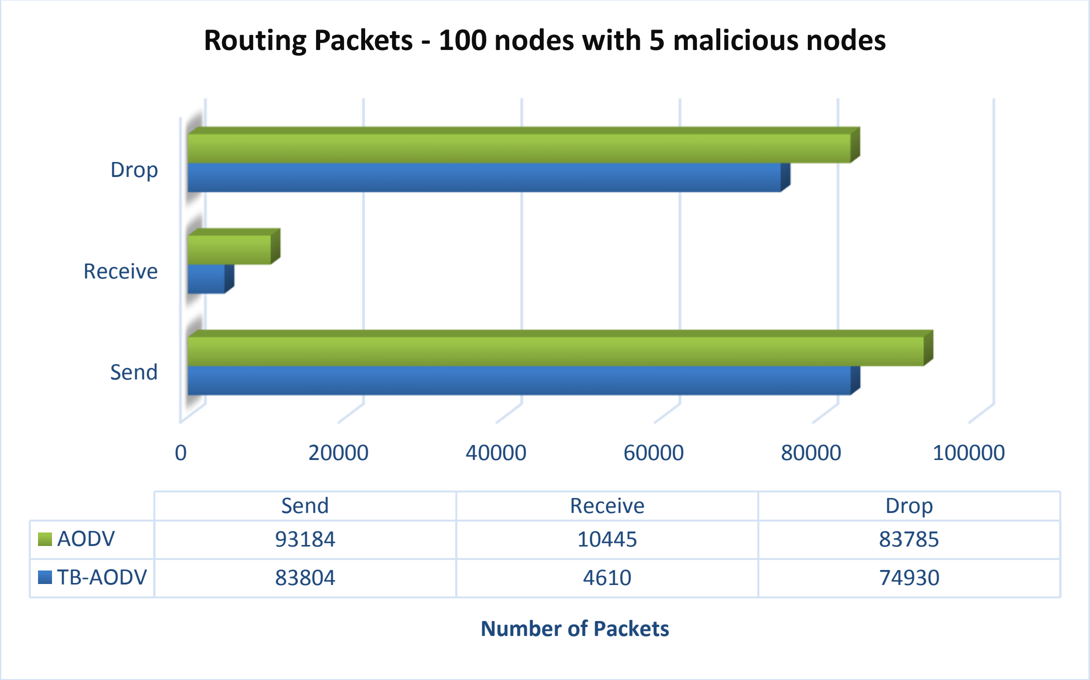
	Send	Receive	Drop
🟩 AODV	48902	13133	36298
🟦 TB-AODV	48793	8546	35592

Figure 25. Routing Packets - 50 nodes with 5 malicious nodes



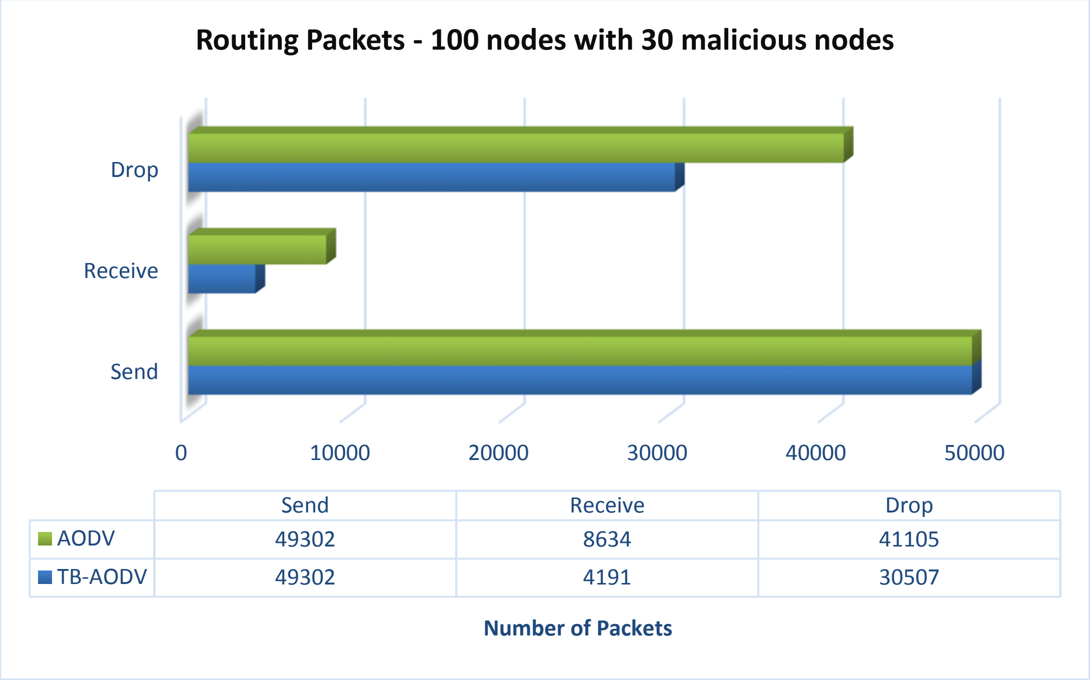
	Send	Receive	Drop
🟩 AODV	24402	5360	18925
🟦 TB-AODV	24402	1513	12759

Figure 26. Routing Packets - 50 nodes with 20 malicious nodes



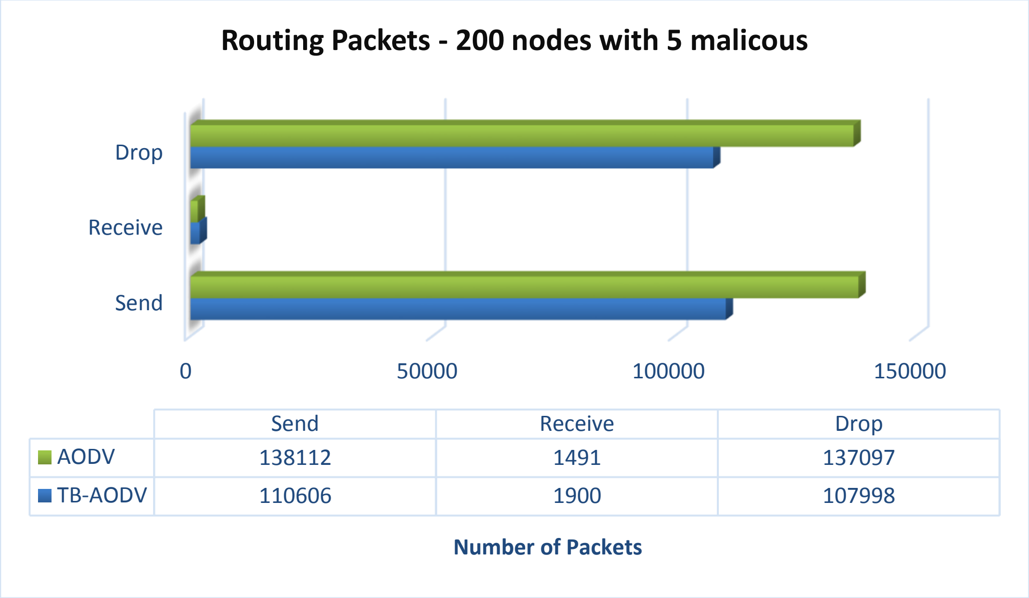
	Send	Receive	Drop
🟩 AODV	93184	10445	83785
🟦 TB-AODV	83804	4610	74930

Figure 27. Routing Packets - 100 nodes with 5 malicious nodes



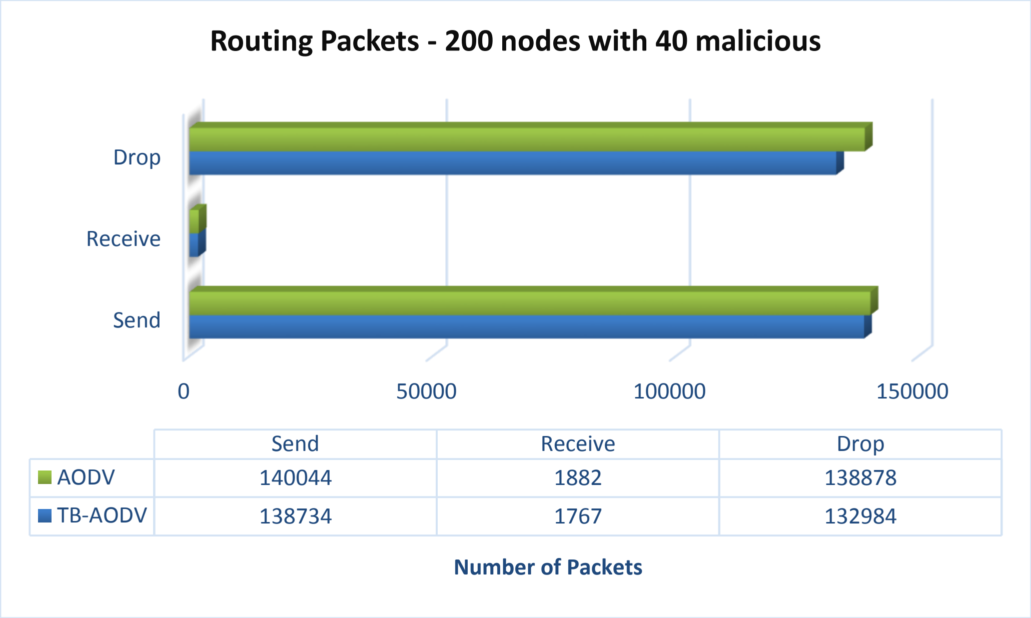
	Send	Receive	Drop
🟩 AODV	49302	8634	41105
🟦 TB-AODV	49302	4191	30507

Figure 28. Routing Packets - 100 nodes with 30 malicious nodes



	Send	Receive	Drop
🟩 AODV	138112	1491	137097
🟦 TB-AODV	110606	1900	107998

Figure 29. Routing Packets - 200 nodes with 5 malicious nodes



	Send	Receive	Drop
🟩 AODV	140044	1882	138878
🟦 TB-AODV	138734	1767	132984

Figure 30. Routing Packets - 200 nodes with 40 malicious nodes

In all 8 scenarios Drop rates in TB-AODV is lower than the original AODV. In some of the scenarios TB-AODV has a lower number of sent and received packets compared to AODV but at the same time AODV has more drops, this shows that the adversary nodes have been successful in planning Black Hole attacks against these two protocols but in TB-AODV malicious nodes have been identified and the rate of dropped packets decreased.

In some scenarios the number of dropped and received packets is not equal to total number of sent messages, it is because there are two types of packet droppings, one is done by Black Hole nodes and the other is done by other nodes when there are errors in data packets, for example in case of a checksum error, the packet must be dropped.

CHAPTER 8

CONCLUSIONS

In order to summarize the study and derive a conclusion whether the proposed TB-AODV protocol worth further study and future work or not, we should take decisions based on simulation studies and the evaluation of final results and also compare different scenarios in different performance metrics.

After performing multiple sets of simulation on different scenarios on the proposed Trust based AODV protocol, it is obvious that our proposed algorithm works pretty fine on detecting and neutralizing Black Hole, Grey Hole and Modification attacks, this conclusion is based on the analysis of number of routing packets and data loss performance metrics.

TB-AODV performed as expected in detecting security attacks and avoiding packet drops.

Although in the End to End metric TB-AODV has worse results compared to AODV because of its extra processing and packet transmission tasks to identify attacker nodes, depending on the application in which Trust based AODV would work on, if security measures are important to take, and the application in which our protocol is implemented on data packets contain critical data where even a tiny amount of difference in packet loss may change the total observation and monitoring results that is important in decision making in a base station, every WSN designer prefers to have more security and less dropped packages in exchange for longer end to end delays which is a difference in milliseconds.

TB-AODV proved to be successful against Black Hole attacks where packets are dropped, it is also effective Grey Hole attacks because in a Grey Hole attack packets are dropped randomly, and although in this condition the attacker node stays unknown for a longer period of time but at the time when its Trust value reaches zero, it would also be blocked.

TB-AODV is also effective against modification attacks where packets are modified by the adversary nodes, by sending out a trust packet and evaluation of whether a neighbor node changes the random number stuffed in the trust packet or not, attacker nodes would be identified and blocked eventually.

CHAPTER 9

FUTURE WORK

Study on the possibility of designing an algorithm for routing decisions which choses the route paths based on combination of both the trust value of the neighbor nodes and the freshness of a route with lower number of hops and Finding the way on how to do the this tradeoff between route freshness and route trustworthiness to get an optimal result.

Improving the proposed TB-AODV algorithm by performing more simulations in different conditions and by tuning up trust decision making mechanisms if possible.

Finding a way to prevent blocked nodes from eavesdropping and study on the implementation of different kinds of security attacks against proposed Trust based protocol.

Study and research on the possibility of implementation of Trust based mechanism on multimedia routing protocols like MMSPEED where it's essential for the algorithm to provide real time data streaming and acceptable QoS with near to zero delay rates.

It would also be a nice research area to study on the implementation of route decision making algorithms based on fuzzy logic for the purpose of Trust evaluation of neighbor nodes.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal. "Wireless sensor network survey", Department of Computer Science, University of California. 2008

[2] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J.Sallai, K. Frampton, Sensor network-based countersniper system, in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD, 2004.

[3] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005

[4] C. Berrou. The Ten-Year-Old Turbo Codes are Entering into Service. IEEE Communications Magazine, 41 (8): 110–116, 2003.

[5] C.-Y. Chong, S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges,"Proceedings of the IEEE, Vol. 91, No. 8, Aug. 2003, pp. 1247ff.

[6] A. Salhieh et al., "Power Efficient Topologies for Wireless Sensor Networks," Proceedings of the 2001 International Conference on Parallel Processing (ICPP'01), Valencia, Spain, Sept. 2001, pp. 156ff.

[7] A. Sinha, A. Chandrakasan, "Dynamic Power Management in Wireless Sensor Networks," IEEE Design and Test of Computers, Vol. 18, No. 2, Mar. 2001.

[8] G. J. Pottie and W. J. Kaiser, "Wireless Integrated Network Sensors," Commun. ACM, vol. 43, no. 5, May 2000, pp. 551-58.

[9] V. Raghunathan, C. Schurgers, S. Park, and M. B. "Srivastava. Energy-Aware Wireless MicrosensorNetworks." IEEE Signal Processing Magazine, 19: 40–50, 2002.

[10] C.R. Baker, K. Armijo, S. Belka, M. Benhabib, V. Bhargava, N. Burkhart, A.D. Minassians, G. Dervisoglu, L. Gutnik, M.B. Haick, C. Ho, M. Koplow, J. Mangold, S. Robinson, M. Rosa, M. Schwartz, C. Sims, H. Stoffregen, A. Waterbury, E.S. Leland, T. Pering, P.K. Wright, Wireless sensor networks for home health care, in: AINAW, Ontario, Canada, 2007.

[11] Nachtigall, J. "Wireless Alarming and Routing Protocol for Earthquake Early Warning Systems", 2011

[12] P. Zhang, C.M. Sadler, S.A. Lyon, M. Martonosi, Hardware design experiences in ZebraNet, in: Proceedings of the SenSys'04, Baltimore, MD, 2004.

[13] Ian F. Akyildiz , Tommaso Melodia, Kaushik R. Chowdhury. "A survey on wireless multimedia sensor networks" . 2007

[14] Stanislava Soro andWendi Heinzelman. "A Survey of Visual Sensor Networks". 2009

[15] M. Rahimi, R. Baer, O. Iroezi, J. Garcia, J. Warrior, D. Estrin, M. Srivastava, Cyclops: in situ image sensing and interpretation in wireless sensor networks, in: Proc. of the ACM Conf. on Embedded Networked Sensor Systems (SenSys), San Diego, CA, November 2005.

[16] R. Cucchiara, Multimedia surveillance systems, in: Proc. of ACM Intl. Workshop on Video Surveillance and Sensor Networks, Singapore, November 2005.

[17] B. Girod, A. Aaron, S. Rane, D. Rebollo-Monedero, Distributed video coding, Proc. IEEE 93 (1) (2005) 71–83.

[18] Karapistoli, E.; Gragopoulos, I.; Tsetsinas, I.; Pavlidou, F.N. UWB Technology to Enhance the Performance of Wireless Multimedia Sensor Networks. Presented at the Proceedings of 12th IEEE Symposium on Computers and Communications, ISCC 2007, Aveiro, Portugal, July 1–4 2007; pp. 57-62.

[19] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks" 2009.

[20] Ramesh Govindan, Eddie Kohler, Deborah Estrin, Fang Bian, Krishna Chintalapudi, Om Gnawali, Sumit Rangwala, Ramakrishna Gummadi, and Thanos Stathopoulos,"Tenet: An architecture for tiered embedded networks", Technical Report TR-56, CENS, November 2005.

[21] Kemal Akkaya , Mohamed Younis, "A survey on routing protocols for wireless sensor networks", 2005

[22] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing."RFC 3561, July 2003.

[23] Holgar Karl, Andreas Wilig , "protocols and Architecture for Wireless sensor Networks" Wiley 2009.

[24] Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: IEEE Int. Workshop on Sensor Network Protocols and Applications, pp. 113–127 (2003)

[25] Yannis Stelios, Nikos Papayanoulas, Panagiotis Trakadas, Sotiris Maniatis, Helen C. Leligou, and Theodore Zahariadis, "A Distributed
Energy-Aware Trust Management System for Secure Routing in Wireless Sensor Networks"

[26] Shaik Sahil Babu, Arnab Raha, Mrinal Kanti Naskar, "Trustworthy Route formation Algorithm for WSNs". 2011

[27] Guoxing Zhan, Weisong Shi, Senior Member, IEEE, and Julia Deng , "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs" . 2012

[28] Raha, Arnab Dept. of Electron. & Telecommun. Eng., Jadavpur Univ., Kolkata, India Babu, Shaik Sahil; Naskar, Mrinal Kanti; Alfandi, Omar; Hogrefe, Dieter "Trust integrated link state routing protocol for Wireless Sensor Networks (TILSRP)". 2011

[29] Theodore Zahariadis, Helen C. Leligou, Panagiotis Trakadas and Stamatis Vo liotis, "Mobile Networks Trust Management in Wir eless Sensor Networks", European Transactions on Telecommunications, 2010; 21:386-395.

[30] Cheng Weifang1, Liao Xiangke1, Shen Changxiang2, Li Shanshan1, and Peng Shaoliang1 "A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks", 2011

[31] Theodore Zahariadis · Panagiotis Trakadas, Helen C. Leligou · Sotiris Maniatis · Panagiotis Karkazis. Springer "A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks", 2012

[32] Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy , "Location-centric Isolation of Misbehavior and Trust routing in Energy-constrained Sensor Networks", IEEE International Conferen ce on Performance, Computing and communications, 2004

[33] http://nsnam.isi.edu/nsnam/index.php/User_Information
http://en.wikipedia.org/wiki/Ns_(simulator) (last visited on February 2013)

[34]Crossbow ProductOverview (Micaz): http://bullseye.xbow.com:81/Products/productdetails.aspx?sid=164 (last visited on February 2013)

[35] www.isi.edu/nsnam/ns/ (last visited on February 2013)

[36] Wireless Networks and Mobile Systems, "Mobile Networks: IP Routing and MANET Routing Algorithms". www.intel.com/education/highered/Wireless/.../lecture_08_manet.ppt (last visited on February 2013)