Spring 5-1-2015

Secure and Reliable Routing Protocol for Transmission Data in Wireless Sensor Mesh Networks

Nooh Adel Bany Muhammad
University of Southern Mississippi

The University of Southern Mississippi

SECURE AND RELIABE ROUTING PROTOCOL FOR TRANSMISSION DATA IN WIRELESS SENSOR MESH NETWORKS

by

Nooh Adel Bany Muhammad

Abstract of a Dissertation
Submitted to the Graduate School
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

May 2015

ABSTRACT

SECURE AND RELIABE ROUTING PROTOCOL FOR TRANSMISSION DATA IN WIRELESS SENSOR MESH NETWORKS

by Nooh Adel Bany Muhammad

May 2015

Sensor nodes collect data from the physical world, then exchange it, until it reaches the intended destination. This information can be sensitive, such as battlefield surveillance. Therefore, providing secure and continuous data transmissions among sensor nodes in wireless network environments is crucial. Wireless sensor networks (WSN) have limited resources, limited computation capabilities, and the exchange of data through the air and deployment in accessible areas makes the energy, security, and routing major concerns in WSN. In this research, we are looking at security issues for the above reasons. WSN is susceptible to malicious activities such as hacking and physical attacks. In general, security threats are classified depending on the layers: Physical, Transport, Network, Data link, and the Application layer. Sensor nodes can be placed in an unfriendly environments and it has lower power energy, computation and bandwidth, are exposed to failure, and the WSN topology is dynamically unstable. The recent wireless sensor protocols are intended for data communication transmission energy consumption. Therefore, many do not consider the security in WSN as much as they should and it might be vulnerable to attacks. Standard crypto systems methods aim to protect the authentication and integrity of data packets during the transmission stage between senders and receivers. In this dissertation, we present Adel, which is a novel routing protocol for exchanging data through wireless sensor mesh networks and uses Ant

Colony Optimization (ACO) algorithm. Adel enhances security level during data transmission between sender party and receiver party in wireless network environment. Once the sensor nodes are deployed in a network, they need to inform their location and their data related to the security for further communication in the network. For that purpose, an efficient mechanism is implemented in order to perform better communication among sensor nodes. Adel generates dynamic routing table using ACO algorithm with all the necessary information from network nodes after being deployed. Adel works with minimum routing restrictions and exploits the advantages of the three multicast routing styles: unicast, path, and mesh based. Since it takes a routing decision with a minimum number of nodes using the shortest path between the sender and the receiver nodes, Adel is applicable in static networks. Four essential performance metrics in mesh networks, network security analysis, network latency time, network packets drop, network delivery ratio, and network throughput, are evaluated. Adel routing protocol has met the most important security requirements such as authorization, authentication, confidentiality, and integrity. It also grantees the absence of the cycle path problem in the network. This research reports the implementation and the performance of the proposed protocol using network simulator NS-2. The seven main parameters are considered for evaluation. These experiments are: security trust, packets drop, energy consumption, throughput, end to end delay, and packet delivery ratio. The results show that the proposed system can significantly enhance the network security and connectivity level compared to other routing protocols. Yet, as expected, it did not do so well in energy consumption since our main goal was to provide higher level of security and connectivity.

The University of Southern Mississippi

SECURE AND RELIABE ROUTING PROTOCOL FOR TRANSMISSION DATA IN WIRELESS SENSOR MESH NETWORKS

by

Nooh Adel Bany Muhammad

A Dissertation
Submitted to the Graduate School
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

Approved:

Dr. Dia Ali_____
Committee Chair

Dr. Bikramjit Banerjee_____

Dr. Chaoyang Zhang_____

Dr.Jonathan Sun_____

Dr. Ras Pandey_____

Dr. Karen Coats_____
Dean of the Graduate School

May 2015

ACKNOWLEDGMENTS

This is to thank all of those who have assisted me in this effort. I wish to express my fruitful thanks and sincere appreciation to Dr. Dia Ali, committee chairman, for his academic supervision, scientific discussion, helping, guiding, and his continuous valuable support throughout this work. I also thank Dr. Chaoyang Zhang, Dr. Bikramjit Banerjee, Dr. Ras Pandey, and Dr. Jonathan Sun, the members of my graduate committee, for their guidance and suggestions. I also thank the School of Computing staff, especially Ms. Crystal McCaffrey; without their knowledge and assistance, this study would not have been successful. I would like to thank my family members, especially my Father, Adel Bany Muhammad, my Mother, Um Ashraf, for supporting and encouraging me to pursue this degree.

TABLE OF CONTENTS

LIST OF TABLES

Table

LIST OF ILLUSTRATIONS

Figure

LIST OF PSEUDOCODE

Pseudocode

CHAPTER I

INTRODUCTION

Gathering information from the surrounding environment makes wireless sensor networks (WSN) apply to major areas in our life. Due to the continuously low cost of developing sensors and the ease of deploying and building networks of sensors, WSN became more commonly used in wide areas of technology applications. Sensor networks are important in various applications, mainly in applications dealing with monitoring real time data such as battlefield surveillance for the military, geo-fencing of gas, oil pipelines and child location [1]. The subject of "Sensor Networks" can be illustrated from its title, which is composed of two broad subjects of interest. This means the sensor nodes in any establishment, and the communicating network among them. The functionality term used for describing such systems is "Process Control." In process control, sensors are coupled with actuators. The sensors are responsible for capturing physical reading in a specific medium, while the actuators are responsible for changing the magnitude of the physical property. For example, in an air conditioning system, thermometers are used to capture the temperature of a room. If the room temperature decreases below a certain value, a mini-chip processor sends a signal to the actuator (AC engine) to reduce burning of the Freon. In more complicated applications like monitoring physical properties of radioactive materials, there are bigger structures of networks. What is known as wireless sensor networks can be illustrated using Figure 1. In this figure, the triangles represent the sensors that are accompanied with a particular location. Each set of sensors is responsible for monitoring one physical property in one room. The figure shows two sets of three triangles; therefore, two different rooms. The two rectangles of the second

branch of the tree is the mother node of the network. There are two mother nodes in the network that receive reading from the two sets of sensors, and ultimately convey the readings to the root node. This tree structure is the most common sensor network topology according to Mayank Saraogi [2].

In any application depending on sensors, where the data is transferred from sensors to nodes, to other nodes, and then ultimately to the root nodes, the data has to be secured. Failure to secure the data can cause failure to stabilize the actuators coupled with the sensors and eventually a problem with the medium under control. The majority of security algorithms provide a good limit of security but none of them provide full security levels as most security systems disregard the effect of physical attacks. It is therefore important to emphasize security measures that can be joined with robust algorithms to prevent such a problem. In this Dissertation I will give an executive summary of my research that will include my own methods combined with existing methods for securing wireless sensor mesh network activities.

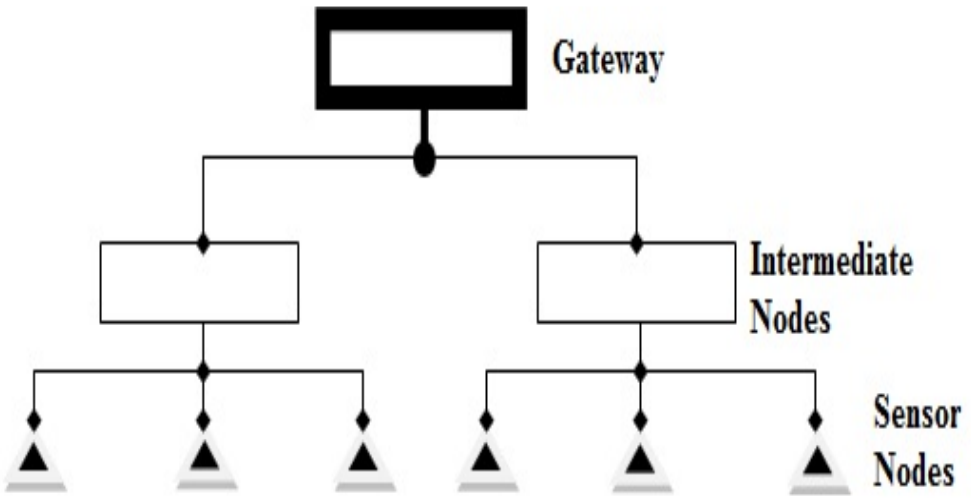


Figure 1. Common wireless sensor network topology.

Problem Statement

Sensor nodes collect data from the physical world then exchange it until it reaches the intended destination. This information can be sensitive, such as monitoring the environment, geo-fencing, and battlefield surveillance. Therefore, providing a secure and continuous data transmission between sensor nodes in wireless network environments is significantly crucial. Various routing protocols have been designed for wireless sensor networks. There are quite a few routing protocols which can provide significant benefits to wireless sensor networks in terms of security and reliability. The keys used to encrypt or decrypt messages during data transmission in wireless sensor networks are the most important elements in making the network communication secured. Many of the current cryptographic schemes are computationally expensive for sensor nodes. Due to the facts that sensor nodes have limited resources and can be deployed in unfriendly environments, creating and managing cryptographic keys are challenging tasks.

To validate this work, network simulator NS-2 software under Linux environment is used to develop a wireless sensor network to run the routing protocol.

CHAPTER I

Background

A wireless sensor network is a built in network of small sensor nodes which can communicate among themselves using radio signals and that can measure various characteristics of the surrounding environment. Wireless sensor network is an advanced communication tool used in many applications recently. For an area such characteristics can include phonic and video information [44]. Every sensor node made with a small processor to process the tasks and a wireless communication antenna to communicate with the remaining network. In addition to that, sensor node has two main resources that are external memory for storing the program data and power source, which is small battery. Generally, these sensor devices are randomly placed around a sensing area to gather information about their circumference [44]. For example, Military and transportation sector.

Once the sensor nodes are placed in a WS network, they need to inform their location and their data related to the security for further communication in the network. For that, an efficient mechanism needs to be implemented in order to perform better communication among sensor nodes. In the networking terminology, this mechanism is named as “Routing protocol.” So, a routing protocol can route the message packet from authenticated source node to particular authenticated destination node securely and prepare route tables for each sensor node in whole wireless sensor network. So, routing protocol is the backbone of the wireless sensor network.

Every sensor node in a network has some resource constraints in the form of power (Battery life), Memory (storage capacity), and Security. Sensor node as hardware device contains less storage, less processing power and it does not have any in-built security features. To design a routing protocol we have to consider all these constrains. Protocol should satisfy these requirements for every sensor device. If any routing protocol failed to satisfy these constrains then performance of Wireless sensor network is degraded. In addition to that, protocol should also have reliability, that is, packet sending and receiving should be done very speedily and efficiently.

Usually wireless sensor networks have huge number of sensor nodes. There are various applications of WSN such as seismic sensing, military applications, health applications, home applications and environmental applications. Wireless sensor networks applications can be categorized into monitoring and tracking and other commercial applications.

Wireless Sensor Networks Classifications

WSN, can be divided according to the nodes capabilities and localization as follows:

- Capabilities:
    1. Homogenous sensor networks: where all sensor nodes are identical and have the exact same specifications within the network, as illustrated in Figure 2.

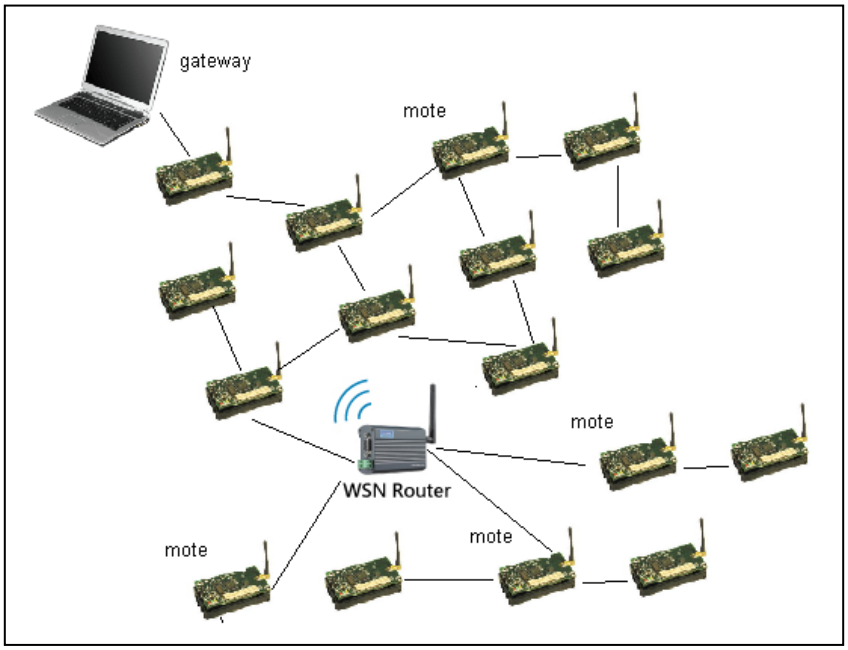


Figure2. Homogenous sensor network.

2. Heterogeneous sensor networks: Within the same network there are more than one type of sensor with different specifications. For example; Martin Stehhlik[10] has illustrate the difference between two types of sensor nodes MicaZ and TelosB, upon the four main components as shown in Table 1.

Table 1

Specifications of MicaZ and TelosB sensor nodes.

Platform	MicaZ	TelosB
1. Microcontroller	T1 MSP430, 8MHz,4KB RAM	Armel A Tmega 128L 8

2. Flash memory	512 KB	1024 KB

Table 1 (continued).

Platform	MicaZ	TelosB
3. Radio	T1 CC 2420 2.4 GHz, 250kbps	T1 CC 2420 2.4 GHz, 250kbps
4. Battery	2 X AA (3v)	2 x AA (3V)

- Localization:
    1. Static wireless sensor networks: in static WSN, all nodes once it deployed will not move from their position.
    2. Dynamic wireless sensor network: in dynamic WSN, the nodes can be reorganized and have the abilities to self reorganized after they have been deployed.

Wireless Sensor Networks Topologies

Based on the routing structure the multicast protocols for WSN-ad hoc networks are sorted into two categories:

- Tree based wireless sensor network protocols
- Mesh based wireless sensor network protocols

Tree based wireless sensor network protocols

One single path connects between any sender sensor nodes to intended receiver sensor nodes.

1. It has the advantage of multicast performance efficiency, which is can be outlined as the ratio of the total number of message packets received by all receiver nodes to the total number of all message packets transmitted or retransmitted by senders or intermediate nodes).
2. Tree based WSN protocols are not completely strong against regular topology or the environmental change and the packet delivery ratio which is well-defined as the ratio of the all data packets delivered to all the intended receivers' nodes to the number of message packets it given to be received by all receivers) drops at high mobility, illustrated in Figure 3.

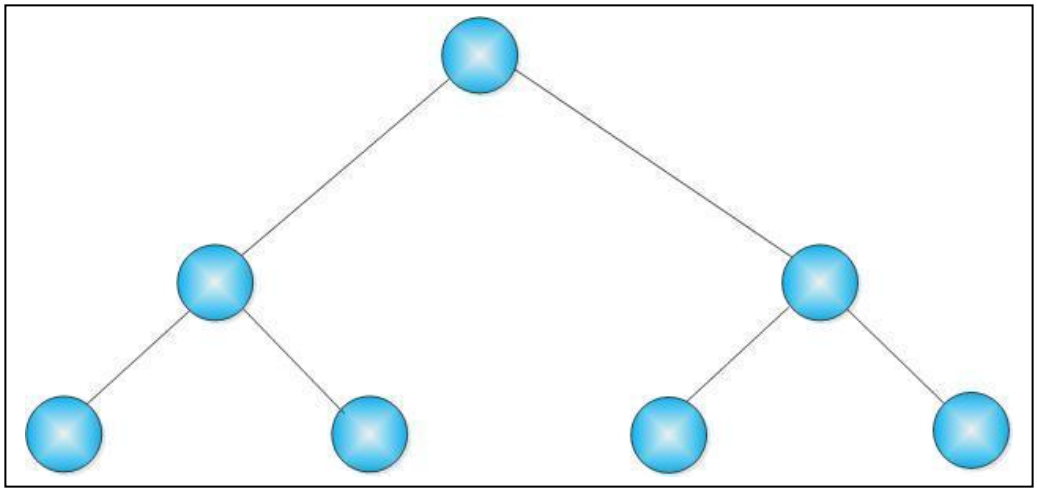


Figure 3. Tree topology.

Mesh based wireless sensor network protocols

1. Mesh based WSN protocols provide more than one routes for maintaining connectivity to throughout the network.

2. The problem caused by link failures called LOW PACKET DELIVERY RATIO PROBLEM is made less severe by redundant routes. However, redundant routes cause low multicast efficiency.
3. Mesh based WSN protocols are robust to sensor nodes mobility.

Mesh network topology illustrated in Figure 4.

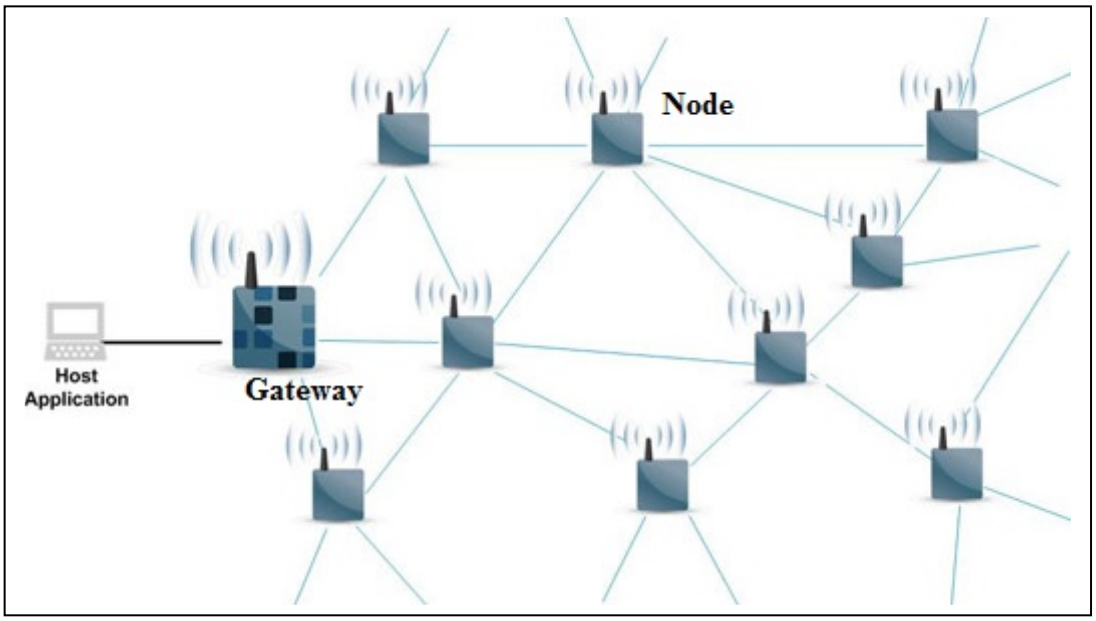


Figure 4. Mesh topology.

Wireless Sensor Networks Threats and Problems

Nowadays, the dynamic WSN is useful and applied in many applications in our lives as stated by Sai Ji, Liping Huang and Jin Wang [5]. (1) Transportation sector: In this sector, the sensors in WSN can be useful in many ways like monitoring the traffic on the streets and providing the information about the status of vehicle; (2) Logistics services: Pre-installed sensor nodes in specific positions used to track and count sold out goods in stores, using these sensors makes it faster and easier to manage big store and make the right decisions on products; (3) Health care: Sensors help doctors to have a better understanding of a patient's status by monitoring the patient's body; (4) In the military

field, WSN is used in many applications. It helps getting the information needed continuously of the status of enemies, which for the leaders is the key to build military plans and strategies.

Due to the fact that WSN has limited resources, limited computation capabilities, exchange data through the air and deployed in accessible areas makes the energy, security and routing become major concerns in WSN. In this research, we are looking at Security issues for the above reasons, WSN is susceptible to malicious activity such as hacking and physical attacks, in general security threats classified depending on the layers into five layers as describe in Table 2.

Table 2

Security threats

Layer	Attacks
1. Physical layer	Jamming, Tampering
2. Data link layer	Jamming, Collision
3. Network layer	Spoofing routing information, Selective forwarding Sinkhole, Sybil attacks, Wormhole attacks, flooding
4. Transport layer	Injection attacks, Synchronization attacks
5. Application layer	Attacks on reliability

The following are common attacks on WSNs [3], [6], [8], [9], [11], [12], [16], [26], [28], [30], [32]-[34].

Jamming and tampering

Jamming and tampering are the most common types of denial of service (DoS) attacks on physical layer, adversary at this layer attacks the radio frequencies of the wireless sensor network by using the same radio waves between the network nodes, in some cases the adversary uses a strong radio waves which can affect the whole network or more most of it and in some cases the radio waves is weak which is can affect small part of the network, this attack called jamming while Tampering attack is a direct physically attack at nodes which may cause damage, replaced with compromised node or extract sensitive information.

Collision Attack

A collision occurs when more than one node tries to send data using the same radio frequency at the same time. As a result of too many collisions the network resources will be exhausting. However, Attackers keep retransmitting corrupted packets to exhaust the resources.

Spoofed, altered, or replayed routing information

At network layer adversaries can spoof routing information and change it by targeting the routing protocols between nodes during exchange date to create false loop, this could cause error messages, latency and may attract the traffic to false node instead of the right one.

Selective Forwarding

At selective forwarding attack, attackers create a malicious node to act like a black hole. What it does is listening to the other nodes in the network and convincing the target node that it has the shortest path, then once the malicious node get the data packets it drops part of it and send the rest to the next node or drop all of it. This causes huge loss in amount data.

Sinkhole Attack

Basically sinkhole attack is a selective forwarding attack but in a complex form. The adversary creates a malicious node with abilities to attract surrounding nodes to route all data packets through it, then the adversary has a complete control over these data. In some cases if the malicious node closer to base station (BS) it may appear to the other nodes as the BS, it's illustrated in Figure 5.

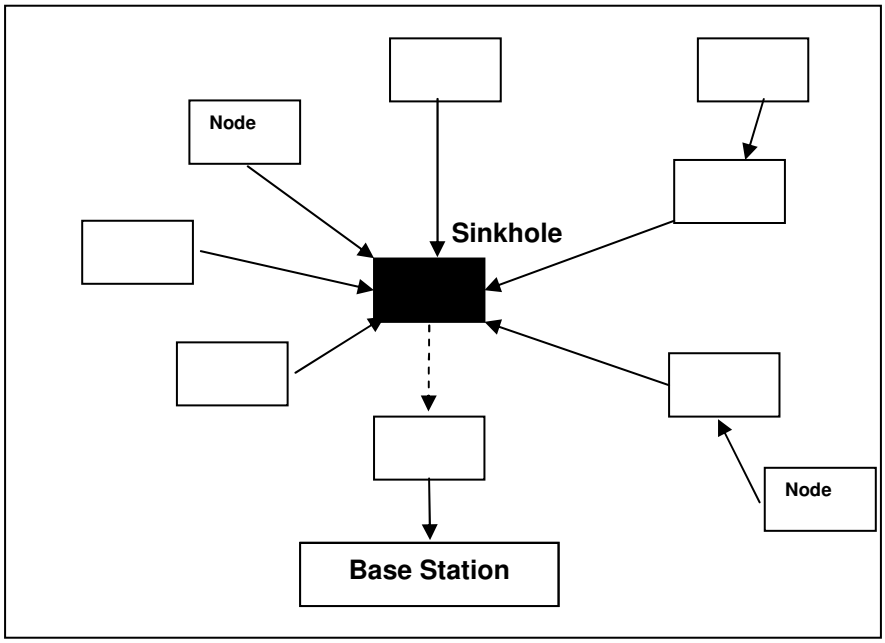


Figure 5. Sinkhole attack.

Sybil Attack

Each node in WSN should have a unique identity. But when a compromised node simulates multiple nodes and fake multiple identities to attack routing protocols then this attack called a Sybil attack.

Wormhole Attack

To create a wormhole attack the attacker needs to create two powerful malicious nodes or more compared to the other normal nodes. These malicious nodes have the abilities to establish faster communication tunnels between them comparing to the other normal nodes. Attacker uses these compromised nodes to confuse the other nodes and make the long paths appears to them as a short paths, which would interrupt the routing scheme and sends replayed packets to other nodes and it may cause a sink hole, as illustrated in Figure 6.

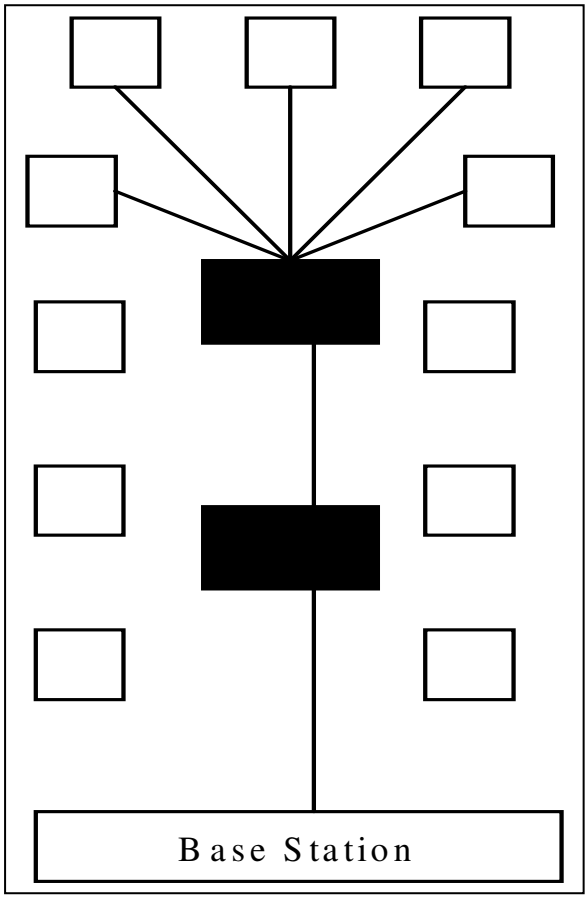


Figure 6. Wormhole attack.

The Broadcast Storm Problem in a Sensor Network

In a Wireless Sensor ad hoc network to resolve any issues due to host mobility broadcasting type of operations are executed more frequently (such as sending an alarm signal for specific host). The Sensor Computing is made possible due to the progression in wireless excellent communication throughout the network and efficient economical, portable computing devices. The design of wireless network (WN) is the most attracted research issue recently.

The broadcast storm problem is reduced by inhibiting some sensor nodes from rebroadcasting to minimize the number of redundant message packets, conflict and inconsistency and by assuming that the sensor hosts in the WN share a one public channel with carrier sense multiple access (CSMA), but no collision detection (CD). To do so it provides five schemes, which differ how a sensor host estimates redundancy. The problem faced when a sensor node tries to rebroadcast a message are that the rebroadcast message may be blocked by busy medium, now when this happens it triggers a back off procedure, and other queued messages. The other problem is that before the sensor node actually starts transmitting the message, the intended receiver may get the same repeated message again and again from other rebroadcasting sensor nodes.

Flooding Attack

Also known as hello flooding attack. In common protocols, nodes get to start communicating between each other by sending hello message. Attacker can use fake hello messages by malicious node with capability of powerful transmission to illusion the

BS and the other nodes by making them think that it's their own neighbor, however it causes a useless traffic on the network. This type of attacks considered as one of DoS attacks.

Therefore with the existence of a sensor network system, it is crucial to couple it with a robust security plan that enables the sensors to communicate with less danger.

As a result of the above factors, different networks face different security threats depending on the environment it surrounded by, technology it uses, and the network topology. In our case wireless sensor networks need special requirements [2], [4], [15], [19], [20].

Wireless Sensor Networks Requirements

Data Confidentiality

Keeping the Data secure from adversaries is the main aspect in securing any network. Data confidentiality aim to provide privacy for communication channels all over the network so content of network communications remain secret from eavesdropping operations.

Authentication

WSN can be compromised by different ways such as, injecting additional nodes or injecting additional packets into it. So it's very important for receiver to make sure that the data originates from the intended source.

Integrity and Freshness

The integrity requirement ensures that nothing has been altered during the network communications. This includes nodes and messages. Sometimes it's not necessary for

adversary to steel messages to compromise the network. For example, adversary can add more packets to the data.

Freshness aims to prevent attacks such as replay attacks by insuring that the messages are recent and not old the ones. Although authentication and data confidentiality can be granted, we also have to grantee the freshness of every single message.

Availability and Reliability

These two requirements ensure the ability to have available and reliable service all over the WSN includes any part of WSN even a single node within the network in different state of continuous changing in the network structure and data transmission.

Authorization

Authorization is simply intended to ensure all WSN entities involved in any specific operations are authorized.

Time Synchronization

Time Synchronized is very important to WSN since sensor nodes have limited resources then Power consumption and energy efficiency become an important concerns for WSN. Using time synchronization conserve power (e.g. for data fusion, individual sensor's Synchronize sleep periods by turning the radio off, etc.). Also it can be a great benefit for performing operation during data transmission among the network, like calculating packets delay time.

Basic Cryptographic Key Algorithms

The following are the basic cryptographic algorithms for the common recent cryptographic algorithms.

RSA Algorithm.

The RSA cryptosystem is one of the most basic algorithms used to generate public keys. RSA stands for Ron Rivest, Adi Shmir and Leonard Adleman, who first publicly described the algorithm in 1977 at Massachusetts Institute of Technology. RSA technique is to encrypt a message packets and exchange it without the need to switch a secret keys. The security of the RSA algorithm is based on the fact that the generating of the large integers is very difficult and in some cases it is not possible to do so.

The RSA uses two keys (Public key and Private Key), one for encryption of messages at sender side and another one is used for decryption of the encrypted message at the receiver side. So that data transmitted securely over the network without attacked by any attacker. This algorithm implemented by selecting two large prime numbers (p, q), calculating their product (N), and producing the public key and private key based on some modulus operations. Then by using these keys sender and receiver communicate very securely over any network medium.

Working with a public-key encryption system has mainly three phases:

1-Key Generation: Every person who wants to send or receive secret messages should have a public key and a private key. The process of developing keys should be in such a way that it will be difficult for others to find the private key by using their public key.

2-Encryption: A process of encrypting a secret message by using their public key.

3-Decryption: A process of decrypting the secret message by using the private key of the person who is being addressed.

RSA work as follows:

If you take X and Y are two persons want to communicate over the network, then simply X sends the message to Y by encrypting it with Y's public key and Y can see the encrypted message by decrypting it with his/her own private key, which Y knows only. RSA implementation is very simple to understand but calculations take more time for simple computer [36].

Implementation of RSA:

RSA algorithm generates a public key and a private key by using the following steps:

- Select the two prime numbers (p , q) which should be large like over 154 digits long.
- Find the product of the prime numbers N=p*q.
- Calculate the Ø = (p-1)(q-1).
- Select the integer E that does not divide the Ø evenly (E is relative prime of Ø).
- Find the number D which satisfies the following operation

  E*D=1mod Ø.
- The pair (E, N) is public key to encrypt the plaintext and convert to cipher text.
- The pair (D, N) is private key to decrypt the cipher text (Unknown format text).

Given a text T, the encrypted text C called cipher text is created by

$$C = T^E \bmod N. \qquad \ldots\ldots\ldots\ldots 1$$

Given an cipher text C, the original text T is recovered by

$$T = C^D \bmod N. \qquad \ldots\ldots\ldots 2$$

X uses the equation 1 to encrypt the message and Y uses Equation 2 to decrypt the message. Here (E, N) is available in public key directory but (D, N) is a unique key for everyone.

A simple example to show how RSA is implemented:

- For e.g., choose p = 3 & q = 11
- Then calculate n = p * q = 3 * 11 = 33
- And then find out φ (n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Now choose 'z' such that 1 < z < φ (n) and e and n are co-prime.
- Suppose 'z' = 7
- Calculate the value of d such that (d * z) % φ (n) = 1.

Only this solution can be possibly with d = 3 [(3 * 7) % 20 = 1]

- And Private key as (d, n) => (3, 33)
- We can consider the encryption of m = 2 is c = 27 % 33 = 29
- And the decryption of c = 29 is m = 293 % 33 = 2

To decrypt the cipher-text c, the person who receives the message needs to use his or her own private key and the mod n. If the message M is very long, the sender may choose to use RSA as a block cipher for encrypting the message meant for the receiver.

Strength of RSA:

The difficulty involved in breaking the RSA algorithm is factoring the N value i.e. finding the two large prime numbers for given N value. Brute force attack can do it but

takes thousands of years. Then the number digits of prime numbers increased then the difficulty to find them also increased. So we can derive relation between number of digits and strength of RSA as proportionality. Adding to that, secret-key algorithms in general use less computing power to be generated when compared to equivalent algorithms use to generate private keys and public keys cryptosystems. The advantage of RSA is that it is used for encryption of a message without having a really to exchange the secret key between the sender and receiver nodes. Since complexity arises in factoring the large integers its security is depends on it. Using RSA algorithm can do both digital signatures and public key encryption.

Diffie–Hellman Key Exchange (DHKE)

Diffie–Hellman key exchange is a schema of exchanging cryptographic keys. It is also known as mathematical exponent cryptographic key exchange. In this function a digital encryption operation uses the certain power of specific numbers to generate the decryption key. This key exchange method can allow persons to exchange messages between them using the same shared secret key. This one shared secret key can be used to encrypt messages using a symmetric key cipher.

Diffie-Hellman key exchange makes both the sender party and the receiver of the message must have the same key pairs. This method do it by joining one of the person's private key and the other person's public key, we can find out the secret number that is shared by the users. This secret number can be used to transform into a material to create cryptographic key. This material is usually used as a cryptographic key to encrypt a message content as encryption key.

The main purpose of developing this algorithm is not to encrypt the data but to produce same secret key at both the sender and the receiver so that there is no need to

exchange this key from sender to receiver sensor nodes. Though this algorithm is a bit slow but it so popular in encryption key generation. So the attacker in the middle could not find the key over the network [7]. Diffe-Hellman security level depends on the discrete logarithmic problem even the super computers cannot compute. Over a medium of insecure communication it establishes shared secret key between the unknown parties.

The basic idea works as follow:

1. If you have two prime numbers g and p.

2. Then you will select a secret number (a), this key will not be revealed to anyone. Then, you will calculate g^a mod p then send this result to receiver party. (Let's name that as A since it came from a).

3. Then, receiver will also do the same thing but let's name the secret number as b and the calculated number as B. Now the receiver computes g^bmod p then sends to you the result, lets (called "B").

4. Take this number receiver gives and follow the previous procedure for it and that's B^a mod p.

5. Sender does the exact procedure with the result receiver sent. So the result will be A^b mod p.

It is just simple math like following,

$(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$

$(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$

If you observe closely, you will get secret key encryption at the sender side that is

the exact same decryption key at the receiver side. Therefore, the sender and the receiver will do it in different orders. Sender never knows what is exactly secret number receiver used to calculate decryption key and receiver will never know what exactly the number sender used, but both will still get the same keys. They can use the encryption key as the password for any algorithm that they intend to use as a shared secrets. In addition, as a result we can be sure that only the sender and the intended receiver know this key, and at the same time there is no intruder can know this key.

Authentication of DHKE:

The Diffie-Hellman key exchange is very much prone to attacks wherever an attacker tries to interrupt messages during data transmission from the sender to receiver and the identity of the other party is assumed very easily. Eventually, the main goal of Diffie-Hellman algorithm is to be used during the authentication phase to authenticate the sender and the receiver and make sure they share the same symmetric keys.

Advantages and Disadvantages of DHKE:

Every time a new conversation between any 2 people is started, they could choose an all-new random secret key and compute the public key and exchange it.

This algorithm can be considered as safe algorithm against passive attacks, such as eavesdropping, but not much effective over active attacks.

However, it gives new session keys each time. Additional protocols are needed to protect against active attacks they can generate "long-term" public keys alternatively and have them placed in a secure central directory.

The Diffie-Hellman key exchange is failed due to the man-in-the-middle attack. This example of man-in-the-middle attack is explained in [7] as following, when a person

in the middle Z takes X's public value and sends his/her own public value to Y. When Y transmits his/her public value, Z substitutes it with her/his own and sends it to X. Z and X thus know one shared key and Z and Y know another shared key. After this exchange, Z simply decrypts any messages sent out by X or Y, and then reads and possibly modifies them before re-encrypting with the right key and transmitting them to the other user. This failure is present because KHKE algorithm does not authenticate the participants.

Elliptical curve cryptography:

In the year 1985, both Victor Miller and Neil Koblitz have discovered an alternative mechanism for the implementation of the public key cryptography and they named this alternative mechanism as Elliptic Curve Cryptography (ECC).

Elliptic curve cryptography (ECC) is an effective mechanism to generate public keys and it is built on the elliptic curves of the algebra and these elliptic curves are classified over specific fields. The advantages of the ECC mechanism over other public key cryptography algorithms are that the ECC can process digital signatures and it also provides fast decryption.

The power of 163-bit public key in the Elliptic curve cryptography (ECC) is as same as that of a 1024-bit RSA key. Taking a point on the elliptic curve and then multiplying it with any random number to create a public key in the ECC algorithm. In this the random number become the private key. The strength of this ECC cryptography system is that it is very hard for anyone to figure out the private key even if they come to know the public key.

In the Elliptic Curve Cryptography (ECC) the public key can be used in various ways to encrypt or decrypt messages. The functionality of the ECC is similar to that of the RSA algorithm. The computing power of the Elliptic Curve Cryptography (ECC) is very less when compared to that of the RSA algorithm. So, it is a good idea to implement the ECC instead of the RSA in smaller devices like PDA's or cell phones because both are similar and the ECC uses less computational power [22].

The elliptic curves in the Elliptic Curve Cryptography (ECC) can be defined by using a small equation and these curves usually consists of the set of real numbers (x, y) and the ECC equation can be explained as following:

$$\mathbf{y^2 = x^3 + ax + b}$$

By changing the values of a and b we can change the shape of the elliptic curve and if we make some small changes in the parameters, there will be a huge difference in the set of (x, y) solutions.

Text message encryption and decryption by ECC as explained in [70].

Algorithm: elliptic curve encryption Input:

Parameters field of elliptic curve (p, E, P, n), Public key Q, K random integer Plain text m

Output: Cipher text (C1, C2)

Begin

1. Represent the message m as a point M in E (F p)

2. Select k □ R [1,n−1].

3. Compute C1 = k P

4. Compute C2 = M+ k Q.

5. Return (C1, C2)

End

Algorithm: elliptic curve decryption

Input: Parameters field of elliptic curve (p, E, P, n), Private key d,

Cipher text (C1, C2)

Output: Plain text m

Begin

1. Compute M = C2 – dC1, and m from M.

2. Return (m).

End

The previous algorithm gives the clear picture of encryption and decryption of a text message over an insecure communication.

Strength of ECC**:**

The Elliptic Curve Cryptography uses smaller keys and operates faster than RSA providing the same level of security. The important thing is that ECC is built on elliptic curve discrete log method so that it becomes harder for the middle man or the third party to crack which is harder than the factoring integers. Above all these advantages, we can say that ECC is more secure than any other public key scheme.

Comparison of WSN algorithms

Recent studies [7], [9], [13] show that by choosing the right encryption algorithms to generate public keys using the right parameters make these crypto systems public keys based applicable to WSN. The searched public key based algorithms include RSA, ECC and diffie-helman key exchange. Data and code size, power consumption and processing

time make it difficult for public key based crypto systems mechanism such as Diffe-Hellman key exchange to put it to use in for WSN. In other words out of these algorithms, Diffie-Helman key exchange is very slow and less secure when man-in-middle attack comes. Most Developers consider RSA or ECC algorithms. The advantage of ECC is that it provides equal security compared to RSA but with a smaller key size, so it reduces the processing time and communication overhead. According to [18] RSA with 1024-bit secret keys provide an acceptable level of security for many applications in the world of WSN, also it provides an equivalent strength to ECC with 160 bit keys. Also it suggested that to provide better data transmission security from the year 2010 and beyond to use RSA with 2048-bit keys to give same strength of ECC 224 bit keys.

Researchers like Mr. Alese, B. K., Philemon E. D. and Falaki, S. O have considered in their research [21] the execution time to be measured on the average median for the point multiplication used in ECC and the RSA modular exponential. ECC with 160-bit key takes 0.81 seconds where as RSA public key operation with 1024 bit key takes 0.43 seconds and for private key operation takes 10.99 seconds. ECC with 224-bit key takes 2.19 seconds where as RSA public key operation with 2048 bit key takes 1.94 seconds and for private key operation takes 83.26 seconds. So the RSA algorithm operations generate private key are slow while ECC is faster which makes ECC preferred for WSN.

In the client/server model, client starts the communication then the server responds to client calls by verifying the client signature with help of RSA or ECC signature algorithms. In this RSA with 1024 bit key consumes 304 mj for sign and 11.9 mj for verifying the signature where as ECC with 160-bit key consumes 22.82 mj for sign

and 45.09 mj for verifying the signature. But For key exchanging between client and server, RSA consumes 15.4 mj at client side and 304 mj at server side. ECC consumes equal energy 22.3 mj on the both ends. So when comparing RSA cryptography system with ECC, not only the ECC provide less processing time but also it significantly provide better security the RSA crypto based system.

Certicom software and hardware solutions [14] compared ECC with RSA algorithm in matter of encryption key size and the result in the following table.

Table 3

Key size comparison between ECC and RSA

	ECC Key Size	RSA Key Size	Key-Size Ratio	AES Key Size
1.	163	1,024	1:6	n/a
2.	256	3.072	1:12	128
3.	384	7,680	1:20	192
4.	512	15.360	1:30	256

Note. Key sizes in bits. Source: Certicom, NIST.

The above table shows the keys sizes for each algorithm used with the specific key. The efficiency of public key algorithms of a microprocessor is mainly measured by the total clock cycles numbers that are needed to perform a one command. RSA algorithms typically uses more computation time and energy rigorously. On contrary, crypto systems symmetric key based algorithms utilize much less computation time and acceptable energy when compared to public key based algorithms.

The public key algorithms compared here include RSA, elliptic curve cryptography (ECC) and Diffe-Hellman key exchange. The most important advantage of ECC is that it offers the same security level using an encryption key with smaller size, which reduce processing time and communication overhead.

The secure key exchange protocol is a simple version of the secure sockets (SSL) handshake, SSL Handshake involves client and server; a client start the connection transmission and a server responding to this transmission. In handshake process, client and server authenticate each other's certificate first then they will start negotiate the session keys that is supposed to be used between the client and server during the data transmission communication.

Multicasting Routing Protocols for Wireless Sensor Networks

The two major types of protocols are 'PROACTIVE' and 'REACTIVE' Protocols.

PROACTIVE: In proactive routing protocols all destinations nodes and their routes paths are computed throughout the network and saved in routing tables, these information are shared between the source node and the intended destination node.

REACTIVE: In reactive routing protocols all routes are found based on the sender request as whenever it demands it, by sending requests to route throughout the network. Then the source receives back the most suitable route to the intended destination

AD hoc On-Demand Distance Vector Routing

For the operation of typical ad hoc networks the Ad hoc On Demand Distance Vector Routing (AODV) has been presented as a novel algorithm. Each Sensor node operates as a separate router and all message packets routes are generated as needed is on demand. AODV was developed by Elizabeth M Belding-Royer, Charles E Perkins

and Samir R. Das, in a project between Nokia Research Center and the University of California, Santa Barbara and University of Cincinnati in 2003.

The AODV algorithm primary aims to:

- To transmit message packets to discover routes between sender and receiver nodes only and only when necessary.
- To recognize the network links connectivity as following.
    1. Neighbor links.
    2. The rest of the network links.
- To scatter and update information if any changes happens in the links connectivity among the network to the nodes that needed to start transmission message packets.

For the message to replay back to the sender a reverse path has to be maintained for a certain time to allow the request replay to reach the original sender node. But if there is a new route then the sensor has to find the destination sequence number, once it finds it then it has to compare it with the current route destination sequence number.

Dynamic Source Routing (DSR):

DSR is a one of the reactive routing protocols. This protocol behave different than AODV routing protocol, DSR technique is to store the all paths to all destination nodes in a specific routing table. Since this routing table stores the address of all destination nodes then it is located in the packet header. Which will be passed from node to node among the whole network till it reaches the intended destination node.

CHAPTER III

RELATED WORKS

The wireless sensor networks are classified into static and dynamic network upon the mobility state of the network and also the encryption keys used to encrypt messages between nodes can be classified into static and dynamic based on whether these keys are able to update or not. These keys can be generated by the following algorithms:

Recent Algorithms

Many researchers like Mr. G. Ravi, Mr. M. Mohamed Surputheen and Dr. R. Srinivasan have mentioned in their research papers [25] that RSA and ECC algorithms are considered as the base for most effective algorithms for secure routing in the wireless networks, but they think that the RSA and ECC algorithms provide less security in the wireless networks than that of the RAC (Random number-Addressing Cryptography) and eRAC algorithms.

RSA- Probabilistic Signature Scheme

RSA-Probabilistic Signature Scheme (RSA-PSS) is a new improvised signature scheme that is mainly built on the RSA cryptographic algorithm and contributes towards enhance security level. This is developed to provide more security mathematically. When the RSA encryption algorithm identifier is used for a public key, the Algorithm Identifier parameters field MUST be assigned as NULL. After Bellare and Rogaway the proposal of Full Domain Hashing, they continuously kept their work by introducing two new

versions for RSA algorithm that became one of the main base of looming cryptography standards. Also they have proposed an Optimal Asymmetric Encryption Padding (OAEP) for encryption. As per the discussion between Rogaway and Bellare in 1996, no tight security affirmation could be made for both the schemes. So they came up with another scheme known as the Probabilistic Signature Scheme.

PSS and OAEP algorithms have randomization in such way that gives a protection against specific kind of implementation attacks. This randomization is a critical and significantly important as part of providing security proof.

How RSA-PSS Works:

Mr. Johannes B¨ock in his research [71] have describe how RSA-PSS works like following, RSA-Probabilistic Signature Scheme takes the input message and a random number (Salt) and runs a hash function with them. This hash result H is used as the first part of the output. Then, a mask for the H is determined that has the length of RSA modulus minus the length of H. Then XOR operation is performed with the salt and the output and this is called maskedDB. Then, maskedDB is attached to H to get the input for the RSA function RSA-PSS. Now, H and the maskedDB are swapped in their order. The input message M is hashed at the first and then hashed again with a random number.

Probabilistic Signature Scheme comes in two different variants, one with appendix and the other with message recovery. Signature scheme with appendix (referred to as SSA) means that the signature is an additional block of data added to a signed message. The message recovery means that parts of the message are concealed within the signature.

Implementation and Explanation:

In this scheme also like in digital signature scheme having Hash and Sign procedure.

For given message “MSG”, The Signature generated as follows:

- “MSGhash” generated by using the one-way method to the given message “MSG”.

$$\text{HASH (MSG)} = \text{MSGhash}$$

- Perform the encoding on the “MSGhash” then it will be “EMSG” (Eencoded message).

$$\text{TRANSFORM (MSGhash)} = \text{EMSG}$$

- Then Signature S will be generated as follows:

Applying the Signature elements to the encrypted message with private secret key:

$$S = \text{SigPrim (private secret key, EMSG)}$$

$$S = \text{Signature (private secret key, TRANSFORM (MSGhash))}$$

$$S = \text{Signature (private secret key, TRANSFORM (HASH (MSG)))}$$

We can represent the above equation in the basic form of RSA algorithm as below

$$S = (EMSG)^{D} \text{ MOD } N$$

As we know (D, N) pair is private key, S and EMSG are integers because “MSG” was encoded prior to the encryption/decryption.

The recovery of the encoded message from signature and Signature verification as follows:

- Similarly “MSGhash” generated by using the one-way method to the given message “MSG”.
- Recover the encoded message “EMSG” from Signature “S” by applying Signature Primitive with help of key.

- Then verify the “EMSG” by transforming the hash value “MSGhash”
- If both are same then signature verified.

RSA- Probabilistic Signature Scheme Advantages:

1. The main feature of newer version of RSA algorithm compare to older version 1.5 of PKCS#1 is that provides more security.
2. Older version of RSA cannot find the attacks made on the data whereas newer version can find the attacks by verifying the signature.
3. According to [29] “the proof of security for RSA-PSS is very tight. The randomization in the signature scheme plays an important role in achieving tightness”
4. According to [29] there is one more advantage of RSA-PSS is that, an attacker will not know in advance about the encrypted message “EMSG”, due to randomization.

RSA- Probabilistic Signature Scheme Disadvantages:

1. .According to RSA laboratories the time complexity of the signature will keep increasing as long as the problem gets harder and harder

Random number-Addressing Cryptography (RAC)

The RAC algorithm is an innovative way of the cryptographic technique; in the RAC algorithm there is a unique way of streaming the cryptographic data like continuous stream of encrypted and decrypted data. RAC algorithm does not have complicated operations but at the physical (hardware) level it will scramble memory access. In

addition to that RAC works in such way were it doesn't use any arithmetic logical procedures but theoretically it is high speed because it simply does memory access. RAC algorithm can be implemented to design secure routing protocol for wireless sensor networks.

1. RAC is considered as the more secure algorithm than of the RSA and ECC algorithms and RAC also consumes less power when compared to the other security algorithms in WSNs [25].
2. In order to implement the wireless security in large scale, it is becoming very vital in security protocol for data encryption in routing and to implement these secure algorithm if we want to assure of a useful cryptographic implementation in the WSN.

The RAC algorithm is explained in the following way:

RAC Algorithm:

Mr. G. Ravi , Mr. M. Mohamed Surputheen & Dr. R. Srinivasan have stated in their research [72] the RAC algorithm steps as following:

1) Main Block

Step: 1 Specify the data scanning mode store and Initialize the data in buffer

Step: 2 Go to Address Generation Block and generate the transposition addresses

Step: 3 Do Encryption or Decryption with Transposition Block

Step: 4 Do Step: 1-3 until the end of buffer and last scan

2) Address Generation Block

Step: 1 Read the initial value

Step: 2 Random Number Generator

Read the sequence

Generate a random number; assign it to the members of the sequence

Do until the end of sequence

Step: 3 Return the transposition addresses

3) Transposition Block

Step: 1 Read the [n]th content of the buffer

Step: 2 Write into the Random[n]th address of the Buffer

Step: 3 Do until the end of the content

Step: 4 Return the encrypted/decrypted content

Advantages and Disadvantages of RAC

- RAC algorithm does not have complicate operations
- RAC works in such way were it doesn't use any arithmetic logical procedures but theoretically it is high speed because it simply does memory access
- Provide more security than original ECC and RSA

Elliptic Curve Diffie-Hellman Scheme (ECDH)

According to Mr.Pritam Shah, Mr. Xu Huang, and Mr.Dharmendra Sharma as mentioned in their papers [31]. In the field of network security, Elliptic curve

cryptography (ECC) is considered as one of the good algorithm because of its high security and small key size. They also mentioned that it takes 80% of key calculation time on wireless sensor networks and in their research [31] papers they have described a solution to reduce the key calculation time to meet the potential applications. In [31] paper the authors have proposed an cryptographic algorithm built on the 1's complement subtraction to represent scalar in scalar multiplication, according to them it offers less Hamming weight and it will significantly enhance the computing efficiency performance of scalar multiplication.

In ECDH to achieve sufficient security, one must have the Diffie-Hellman algorithm with the same security level provided by RSA with a key of 1024 bits but this can be obtained in an easier and simpler way with the same security level in 160-bit key size and it can be obtained by combining Diffie-Hellman and ECC algorithms.

The authors of [31] have shown below the steps how the Elliptic Curve Diffie-Hellman scheme works:

- In the first step, sender and receiver agree on a specific curve with one base point, let's call this point P.
- In the second step, they populate the public keys of the sender and receiver by multiplying point P with their own private keys, let call the private key of the sender K_s and the private key of the receiver K_r.
- Thirdly, this phase starts with sharing public keys between the two ends then they start the process of multiplying their public keys with their private keys to generate shared secret key.
- The secret key is $R = K_s * Q_r = K_r * Q_s$.

The values of Q_s, Q_r and point P it is computationally uncompromising for an attackers to calculate the sender private key K_s and the receiver private key K_p.

R now is the shared key and it is incredibly hard for adversaries to figure it out. The whole steps of creating, Private Key Public Key, and one Shared Secret Key by Ellipitc Curve Diffie Hellman Scheme (ECDH) is explained in figure 7.

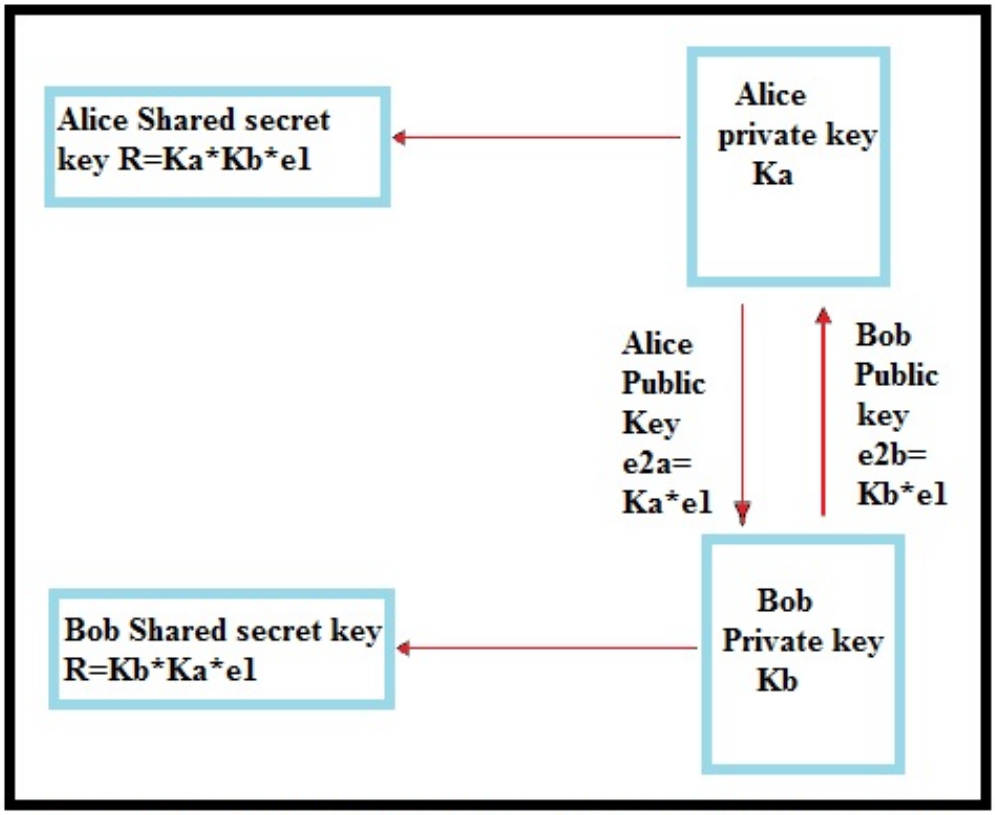


Figure 7. ECDH process schema.

ECDH Advantage and Disadvantage:

- ECDH benefits from combining the ECC algorithms high security and small key size with simplicity of DHKE algorithms.

- There is a chance for a man-in-the-middle intrusion on the ECDH since either party has the difficulty of authenticating on the public key. A PKI or a signature procedure might be able to remedy such vulnerability.

Identity-based signature (IBS) algorithm

During the data moving between two communicating nodes that should be accessible by the nodes that were authenticated in that network. So, unauthorized nodes do not have access to the confidential data in that network. In order to provide authentication between two communicating nodes a proper secure authentication schema should be needed. For that Al-Mahmud and Akhtar proposed a protocol [40] built on the identities of the sensor nodes is identity-based signature (IBS) algorithm.

IBS algorithm is a collection of four different algorithms, the first two are System setup and Key Extraction algorithms are used by Base station (BS) to generate public key parameters and secret keys of sensor nodes. Next two algorithms are Signature generation and Signature verification algorithms are used to sign the message by sender and verify the message by receiver node. The main authentication process in this schema consists of every node registered by the base station. Communicating nodes mutually authenticated each other and finally session key establishment between those nodes for their future communication secure. In addition to that, Neighborship-based detection algorithm is used to detect a compromised node. This algorithm is based on the signal power level of two neighbors whose having same certain limit. IBS algorithm uses Time stamps to avoid replay attacks.

IBS Algorithm:

IBS algorithm implemented in the following three steps

1. System initialization
2. Sensor node authentication
3. Session key establishment

System initialization:

- By using System setup algorithm, Base station (BS) produces its own private (SKPKG), public key (PKPKG) and the public system parameters P.
- Base station registers every user of sensor node then uses Key Extraction algorithm to produce the private key for the sensor node (private key DIDi for node i) and users (private key UPKi for user i). The sensor nodes and the users who registered successfully store their own id combined with their own private key. Also stores public system parameters into their physical memory, then before the deploying of all nodes and users in Wireless sensor (WS) network.
- Base station broadcasts data set (id, TS) of the each sensor node to all the sensor nodes. Then all other nodes acknowledge to the Base station based upon receiving the information from Base station. If any node does not receive the message then BS again resend the message and those nodes that do not get the message previously get the message by verifying the time stamps in order to avoid replay attacks.

Sensor node authentication

The process of sensor node authentication has been explain by Mr.Choudary Gorantla, Boyd, Manuel, and Nieto in their research paper "G ID-based One-pass Authenticated Key Establishment" [27] as following:

1. The sender node creates authentication request to authenticate sensor nodes by using message A and signs it by the signature generation algorithm used by Identity-

based signature (IBS) algorithm. The sender node sends this message authentication request A message combined with the signature B, its identity D, and a time stamp T1, this time stamp T1, time stamp will be sending to ensure it avoid reply attacks.

Sender node	Receiver node or BS
Sender sends A, D, T1	Receiver receives (A,D, T1, B)

Signature B=Signature Generation((A, D,T1S), DID,)

2. Receiver or BS will receive the message R from Sender and verify the sender node in registration list whether the sender registered or not. Then verify the replayed message or not based on the timestamp then verify signature B of the sender using signature verification method of the IBS algorithm.

- Registration verification: A,D, T, B
- Check node with identity D is already registered
- Time stamp:

  Calculate (TC-T)

  Check (TC-T) $\geq \Delta T$
- Verify the node signature:

  Accept/Reject Signatures Verify((A,D,T), D, B, P)

3. If all these verifications are successful then the receiver node or BS sends its own ID and TS to the sender node as in step 1.
4. Sender node will do the same verifications on the receiver node as in the step 2.
5. If all verifications are successful, then both nodes are mutually are authenticated otherwise authentication will be rejected.

IBS Algorithm Advantages:

1. Base station, sends only hash key of id to all other nodes instead of sending total id of sensor node. The sensor node memory necessity can be reduced by using hash value to determine the node identity.
2. The base station also keeps a corrupted nodes list. When a node attacked then the base station receives this information about the compromised node through the network, once it gets it then immediately append this sensor node address into the corrupted nodes list, after this list is updated then it broadcast it throughout the entire network, the previous procedure is necessary to make sure the network is secure against compromised nodes.
3. It has an advantage of the neighborship-based detection algorithm.
4. It also avoids Replay attack by using Tome stamp.
5. The Authentication between any pair of two nodes required only once. So communicating nodes do not need to lose their energy.

IBS Algorithm Disadvantages:

1. In this protocol attacker may capture the secret key that was sent by base station to the sensor node.
2. Base station consumes more energy because it needs to broadcast all sensor node information to all the other nodes.

Secure Topology Discovery and Network Setup Protocol.

Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, and John Pinkston [17] have presented the first version of this protocol in 2002. This protocol aims to provide a better authenticate for the sender, privacy and integrity to data and prevent the replay

attacks. This protocol expands the broadcast scale from a base station using an intermediary node, also they claim that this protocol can correct some classes of irregular node behavior.

The following are assumptions to run the protocol as specified in [17].

1. The base station is computationally robust, and the base station is part of a trusted computing environment.
2. The communication paradigm is either base station to sensor or sensor to base station.
3. The radio range of a sensor is 15 meters.
4. Given the radio range of a sensor, the single hop area of coverage with the base station at the center is: 706 square meters,
5. The sensing range of a sensor is 1 meter.

The following algorithm shows how this protocol works.

Handshaking process starts when sensor node wants to send a request to another sensor node, so a message travels among the network from base station and multiple nodes till it arrives to the intended destination. During this stage, the network datagram is sent to do handshaking then collects the addresses of the sender and receiver nodes. After initiation of the cryptographic key the sender will start sending a cryptic data using the key. Now the Receiver receives data and decrypts the data using the key that is familiar to it. The protocol has been developed using SensorSim network simulator which is based in network simulator NS-2 [24] as stated in their published research [17] next is the protocol.

C ← all sensors in Sensor Network

Route Table ← Φ

Temp Route Table ← Φ

∀ **J** □ C do

Base Station → j : <Addr 1(), E**Key** $_j$ {Addr 2(**j**), DTG, *HELLO}*, null >

if (**j** → Base Station : < Addr_1(j), E**Key** $_j$ {Addr_2(**j**), DTG, *HELLO-REPLY}* , null

>) then

Route Table ← Route Table + **j**() C ← C - **j**

∀ **K** □ C do

∀ **J** □ Route Table do

Base Station → j : <Addr_1(), E**Key** $_j$ {Addr_2(**j**), Null, *RELAY}*,

E**Key** $_k$ {Addr_2(**k**), DTG, *HELLO}*>

J → k: <Addr_1( ), Ek $_k$ {Addr_2(**k**),

DTG,*HELLO}*, ψ}>

if k → j: Addr_1( ), header, payload >

where:

Header = ψ = E**Key** $_j$ {Addr_2(j), null, *RELAY}*

Payload = Addr_1(**k**), E**Key** $_j$ {DTG, Addr_2(**k**), *HELLO-REPLY}*, null >

j → Base Station: < Addr_1(**k**), E**Key** $_k$ { DTG, Addr_2(**k**), *HELLO-REPLY}*, null >)

then

Temp Route Table ← Temp Route Table + **k**(j) Optimize(Temp Route Table)

Route Table ← Route Table + Temp Route Table

Note: The DTG is only verified by the final destination consequently it is null for intermediate nodes [17].

The experimental topologies stated in [17] *as following:*

a. 30 nodes randomly are placed in the inner circle and 70 nodes randomly are placed in the outer circle, it illustrated in Figure 8.

b. 50 nodes randomly are placed in the inner circle and 50 nodes randomly placed are in the outer circle, it illustrated in Figure 9.

c. 70 nodes randomly are placed in the inner circle and 30 nodes randomly are placed in the outer circle, it illustrated in Figure 10.

d. 100 nodes randomly are placed across the entire area, it illustrated in Figure 11.

The below figures shows all the experiments results as it appears in [17] from (a) to (d) topology:

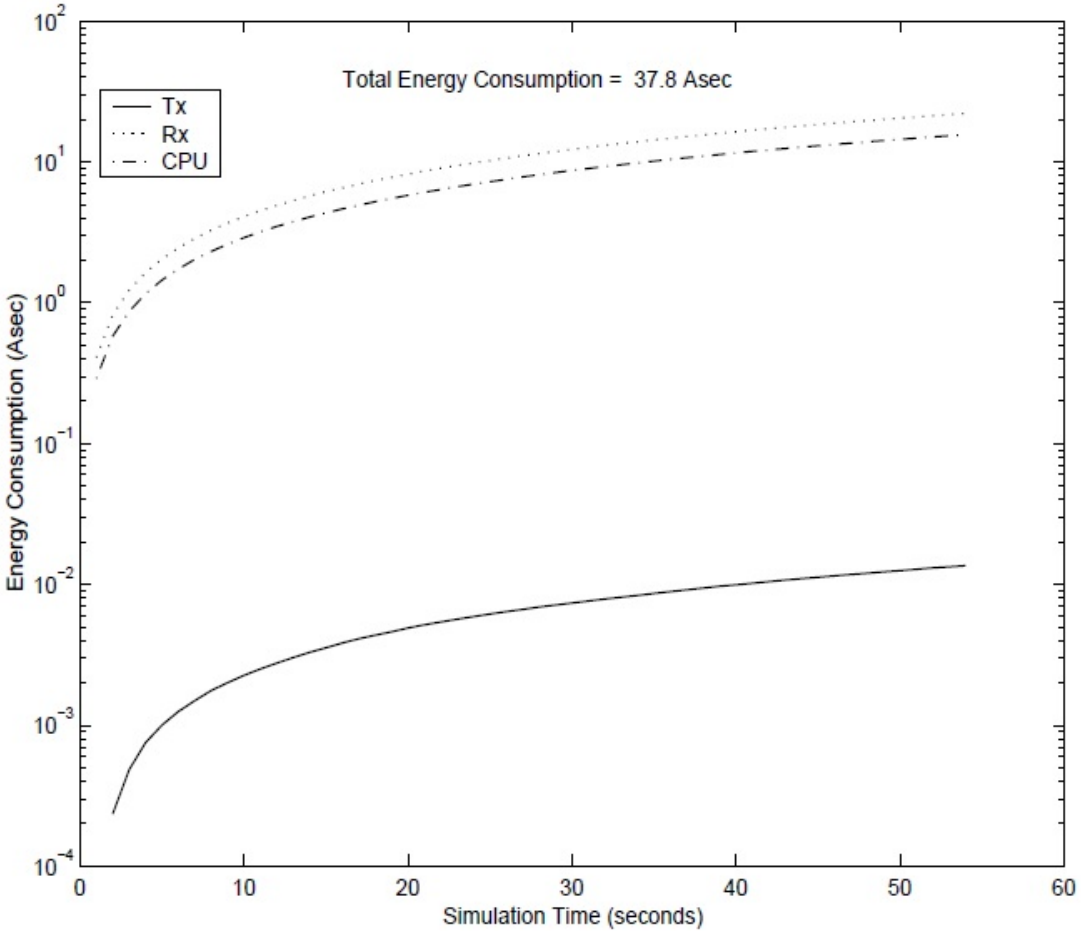


Figure 8. Topology (a) 30 Adjacent and 70 Nonadjacent Nodes.

Research [17] results for topology (a) tells us that. “Discovery and network setup occurred in 54 seconds of simulation time with a total energy expenditure of 37.8 for all nodes in the sensor network”.

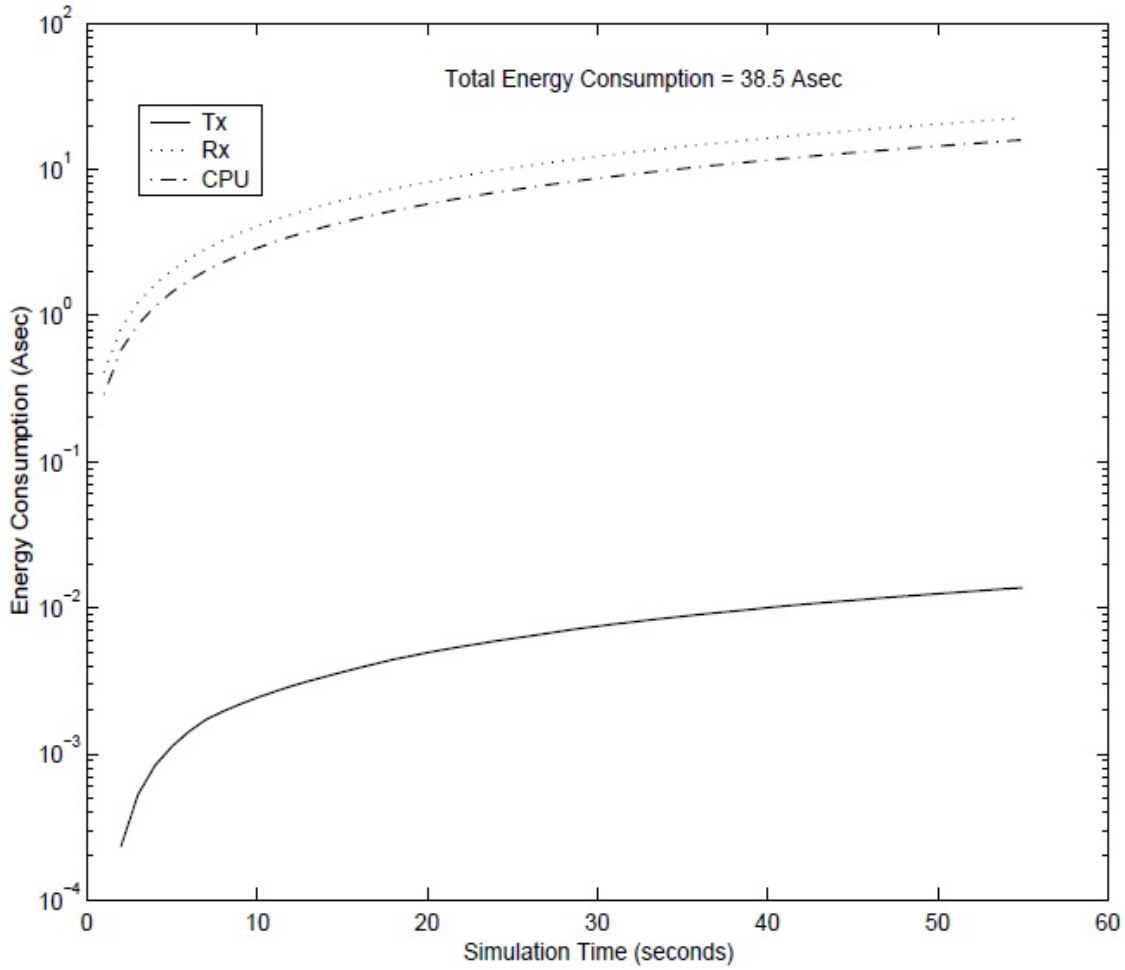


Figure 9. Topology (b) 50 Adjacent and 50 Nonadjacent Nodes.

Research [17] results for topology (b) tells us that. “It took 55 seconds of simulation time for topology discovery and network setup and the total network energy consumption was 38.5”.

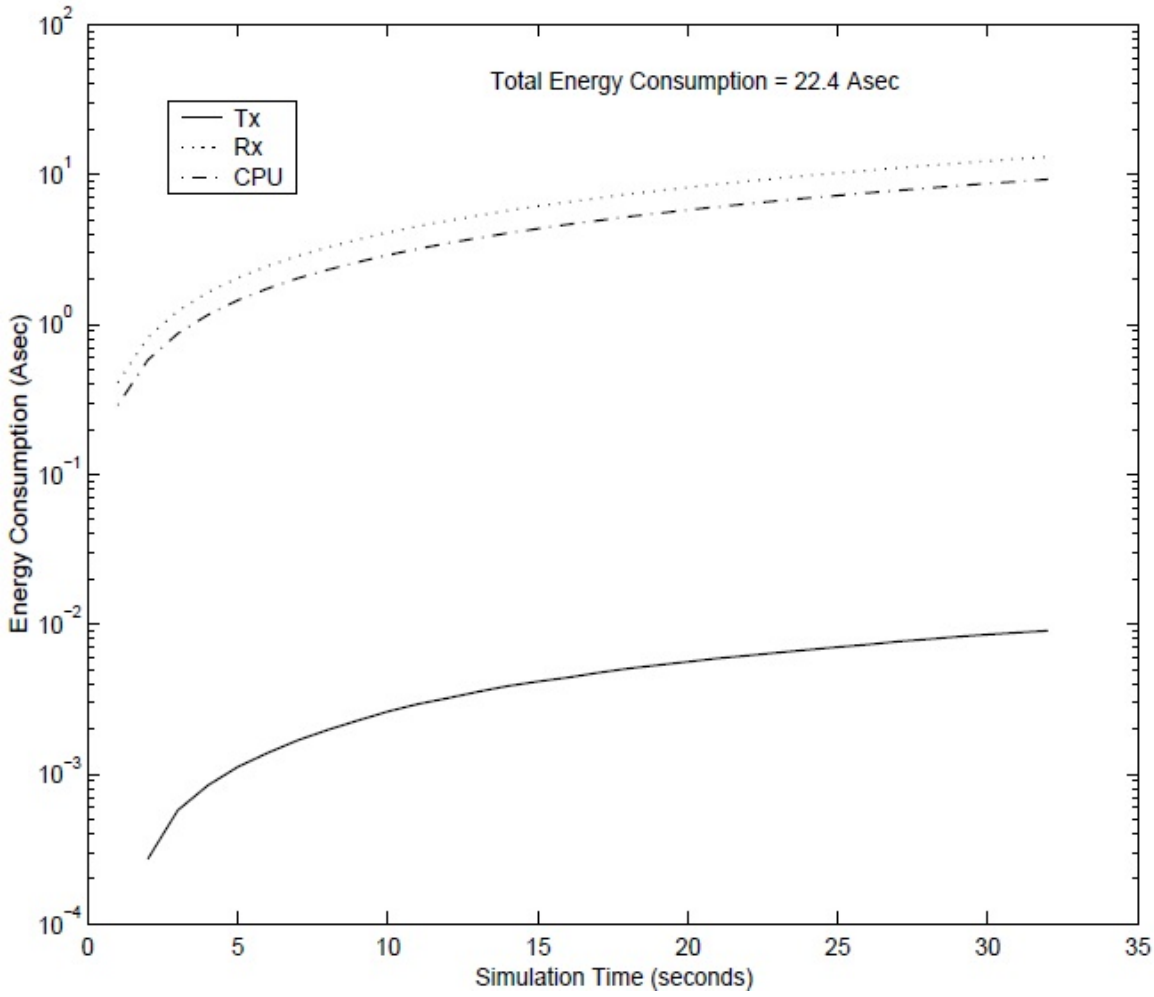


Figure 10. Topology (c) 70 Adjacent and 30 Nonadjacent Nodes.

Research [17] results for topology (c) tells us that. “It took 22.4 for energy consumption and it took 32 seconds for simulation time for topology discovery and network setup”.

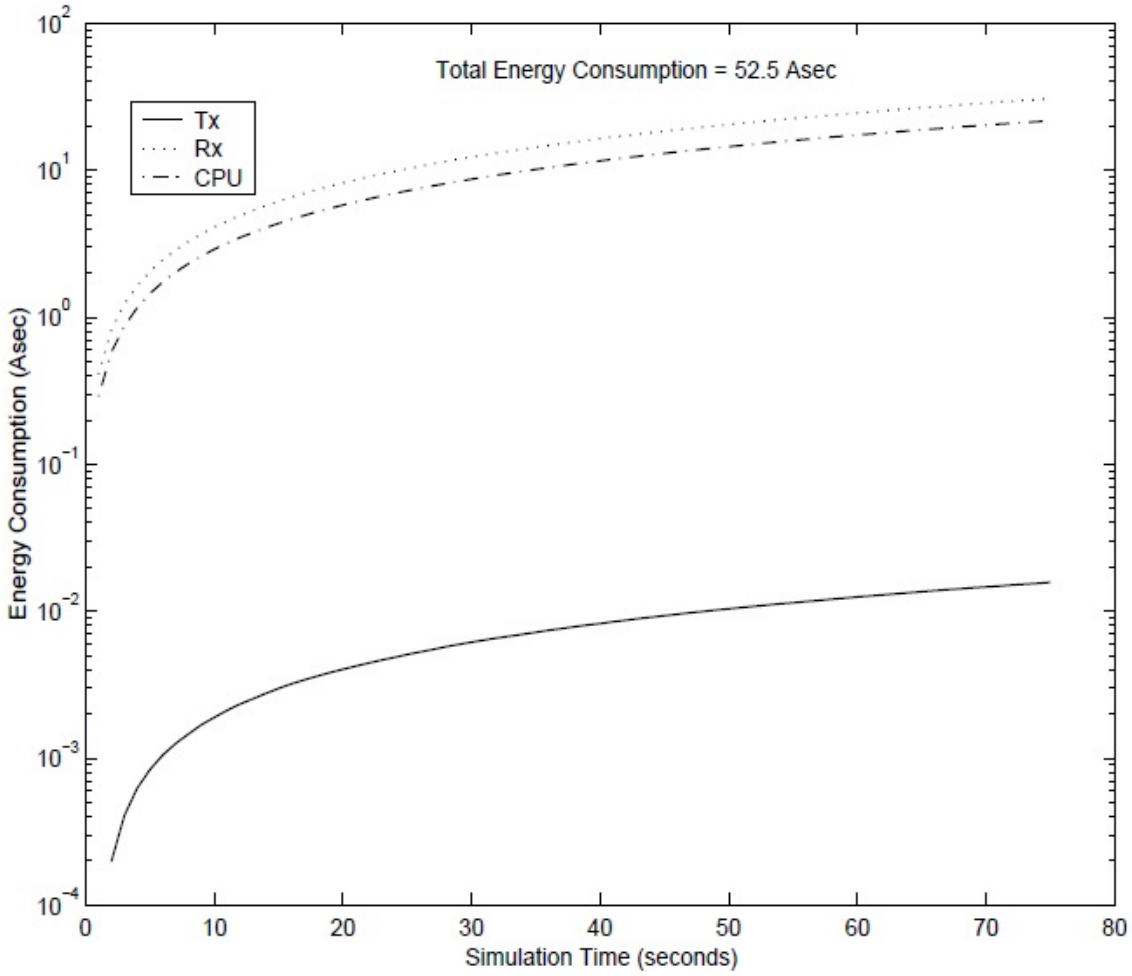


Figure 11. Topology (d) Random Distribution of Nodes.

Research [17] results for topology (d) tells us that. “It took 75 seconds of simulation time and energy consumption was 52.5”.

Research in [17] have specified “In all cases, the receiver (*Rx*) component consumed the highest amount energy, closely followed by the CPU. The transmitter (*Tx*) component consumed the least amount of energy”

Reasons for choosing the previous protocol to be my competitor (advantages and disadvantages):

Advantages of Secure Topology Discovery and Network Setup Protocol

- Not only it is more general than the previous protocols, but also it covers the authentication and the routing part.
- Solve many security problems such as:
- Wormhole Attack
- Hello attack
- Acceptable energy consumption.
- Sensor battery approximately will live for about 435 hours if it has capacity of 3,135 mAh.

Disadvantages of Secure Topology Discovery and Network Setup Protocol

- This protocol is limited to scale of two nodes distance from the base station
- Does not solve the cycle path problem

AD hoc On-Demand Distance Vector Routing

For the operation of typical ad hoc networks the Ad hoc On Demand Distance Vector Routing (AODV) has been presented as a novel algorithm. Each Sensor node operates as a separate router and all message packets routes are generated as needed is on demand. AODV was developed by Elizabeth M Belding-Royer, Charles E Perkins and Samir R. Das, in a project between Nokia Research Center and the University of California, Santa Barbara and University of Cincinnati in 2003.

The AODV algorithm primary aims to:

- To transmit message packets to discover routes between sender and receiver nodes only and only when necessary.
- To recognize the network links connectivity as following.

1. Neighbor links.
2. The rest of the network links.

- To scatter and update information if any changes happens in the links connectivity among the network to the nodes that needed to start transmission message packets.

For the message to replay back to the sender a reverse path has to be maintained for a certain time to allow the request replay to reach the original sender node. But if there is a new route then the sensor has to find the destination sequence number, once it finds it then it has to compare it with the current route destination sequence number.

AODV Routing:

According to [52], [53], [56] the combination of both Destination-Sequenced Distance Vector (DSDV) and DSR routing protocols are Ad hoc on demand distance vector routing (AODV) where sensor nodes maintain one routing table, according to [53] this routing table contains the following entries:

1. Active neighbor list: where this list contains list of all neighbors' nodes that are actively and still uses this route path. Once this link entry changes to be broken, then neighbor nodes within the same list will be informed.

Destination address

2. Next-hop address toward that destination

3. Number of hops to destination

4. Sequence number: for choosing route and prevent loop

5. Lifetime: time when that entry expires

Routing using AODV protocol consists of two phases:

- Route Discovery

- Route Maintenance.

A sensor node looks up in the routing table when it ready to start to communicate with a sensor node. When the required destination node is found the sender node will start transmitting data in the way as in DSDV otherwise it starts the route discovery mechanism phase. After it completes the route discovery phase then it keeps up to date using the Route Maintenance mechanism. The AODV can be explained as following:

AODV Explanation:

Step1:

- Assume node number 1 wants to start sending data packets to node 7.
- Let node 6 to be the only sensor node knows the route to destination node.

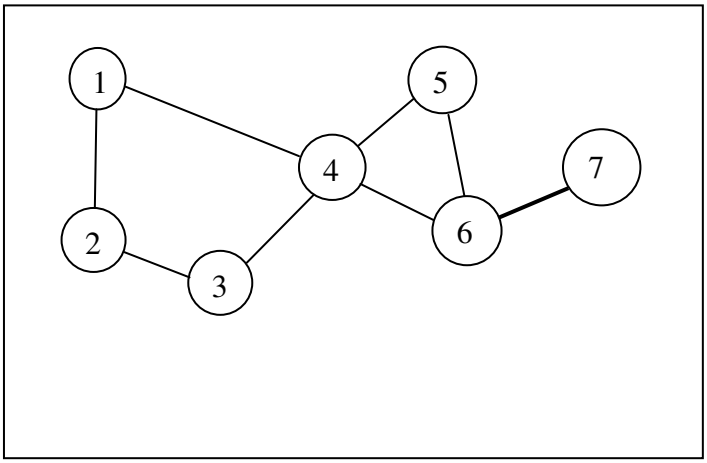


Figure 12. (AODV Step 1).

Step 2:

- Sender node number 1 start sending a RREQ packet to the nearest neighbors of its location.

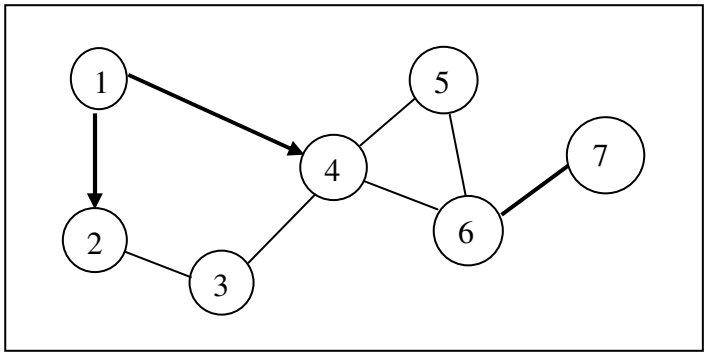


Figure 13. (AODV Step 2).

Source add_number =1,

Destination add_number =7,

broadcast_id_number = broadcast_id_ number +1,

Source seq_number = source seq_number + 1,

Destination seq_number = last Destination seq_number for node number 7.

- Then nodes number 2 and 4 shall confirm that this is a fresh RREQ.

Step 3:

- They forward the RREQ

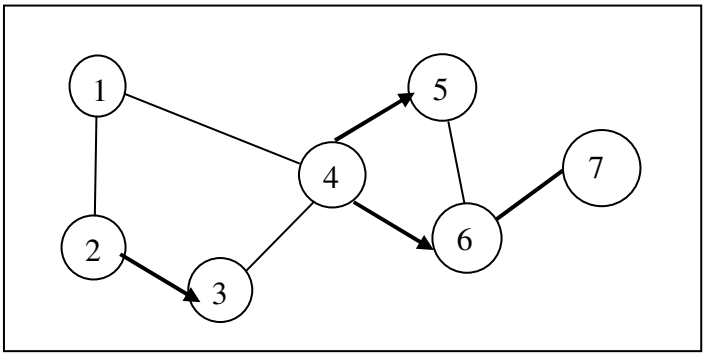


Figure 14. (AODV Step 3).

- In this step it updates the necessary information like source sequence number for the sender node number 1 and increment hop level in the RREQ packet.
- Then the RREQ message arrives at node number 6 coming from node number 4.
- When node number 6 receives the RREQ then it must verify necessary information such as destination node sequence number is lesser than or equal to the destination node sequence number it has registered for node number 7.

Step 4:

- Nodes number 5 will try to send RREQ packet to node number 6, but it observe this packet and deal with is as duplicates

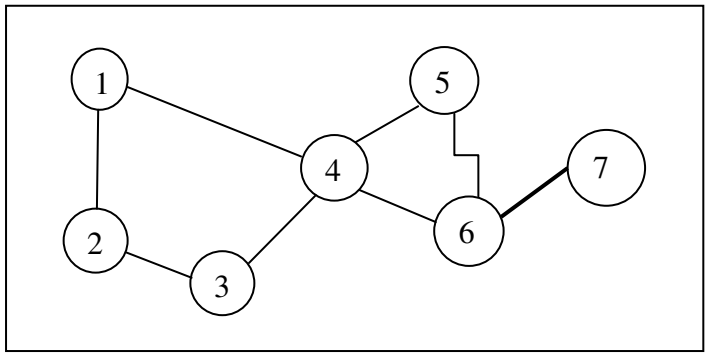


Figure 15. (AODV Step 4).

- When node number 6 receives the RREQ packet and it has the current route to the destination node number 7, then it sends a route reply packet (RREP) to node number 4 which it has sent the RREQ packet. Following is replay request packet format.

Table 4

Route Replay Packet of AODV

Type	Flag	Hopcnt
• Destination address • Destination seq_number • Source address • Lifetime		

Step 5:

- Node number 6 recognize a route to node number 7 and sends the RREP to node number 4 and update the necessary information at the routing table.
    - Source address =1,
    - Destination address=7,
    - Destination seq_number = maximum (sequence number, destination seq_number in the RREQ),
    - Hop level =1.

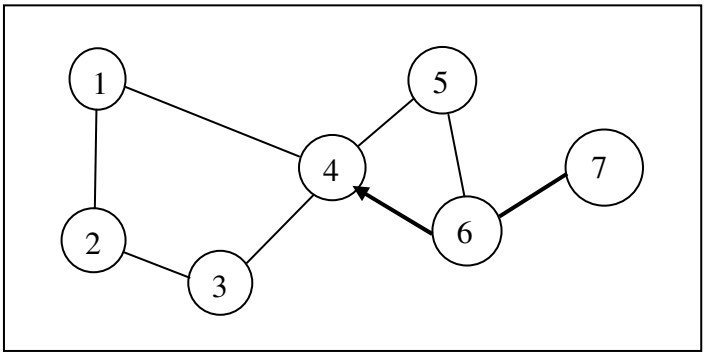


Figure 16. (AODV Step 5).

Step 6:

- Node number 4 makes sure that this routing packet is a fresh route reply, once it receives it then it sends the RREP packet to node number 1.
- Increase the hop level in RREP packet.

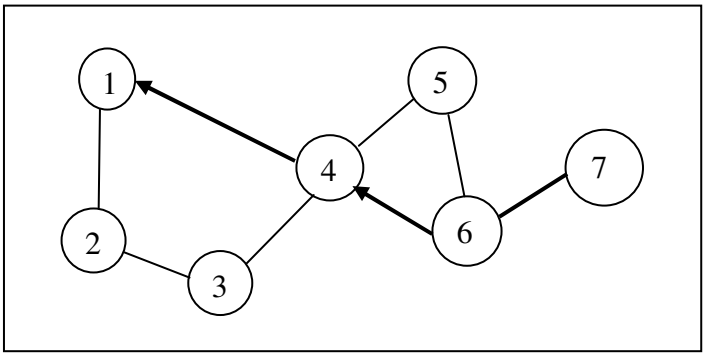


Figure 17. (AODV Step 6).

Step 7,

- Update route table.
- Node number 1 now it is ready to use this routing path to send and receive data packets from and to node number 7.

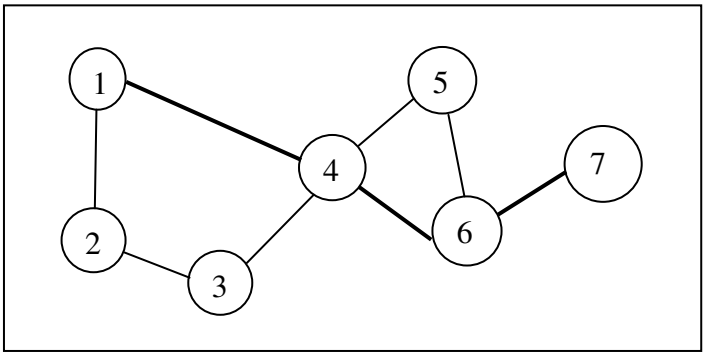


Figure 18. (AODV Step 7).

The advantages of AODV are

- Minimize the amount of broadcast data packets by create routes on needing basis.
- Processing time is low.
- Fast adapting to network topology changes.
- It is very scalable for mobile nodes.

The Disadvantage of AODV protocol is that

- Sometimes a network inconsistent can happens, when sequence number gets old and the middle sensor nodes do not have most updated sequence number for the destination node.
- If multiple Route Reply packets responded to one single RREQ packet this can issue a control overhead.
- Control overhead leads to longer delay, packet loss and unsuccessful bandwidth consumption.

Anu Arya1, Jagtar Singh2 in their research [52] have a comparative study of AODV, DSDV and DSR routing algorithms, using the network simulator NS 2 with this parameters:

- Simulation Time: 150ms
- Number of Nodes: 20, 40, 60
- Packet Type: TCP Packet
- Queue Type: Priority Queue
- Traffic Type: Constant Bit Rate
- Platform: Ubuntu
- Simulator: NS2

Results like following:

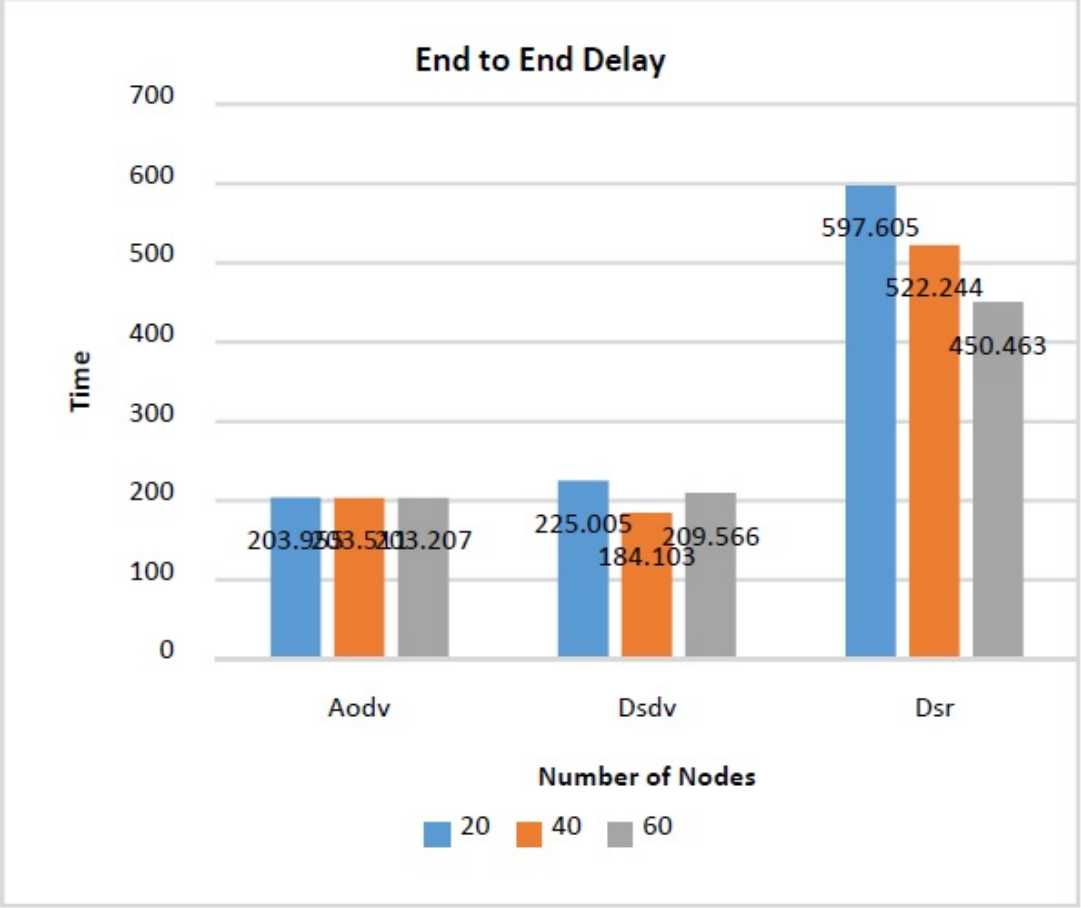


Figure 19. Delay for three topologies 20 nodes, 40 nodes and 60 nodes [52].

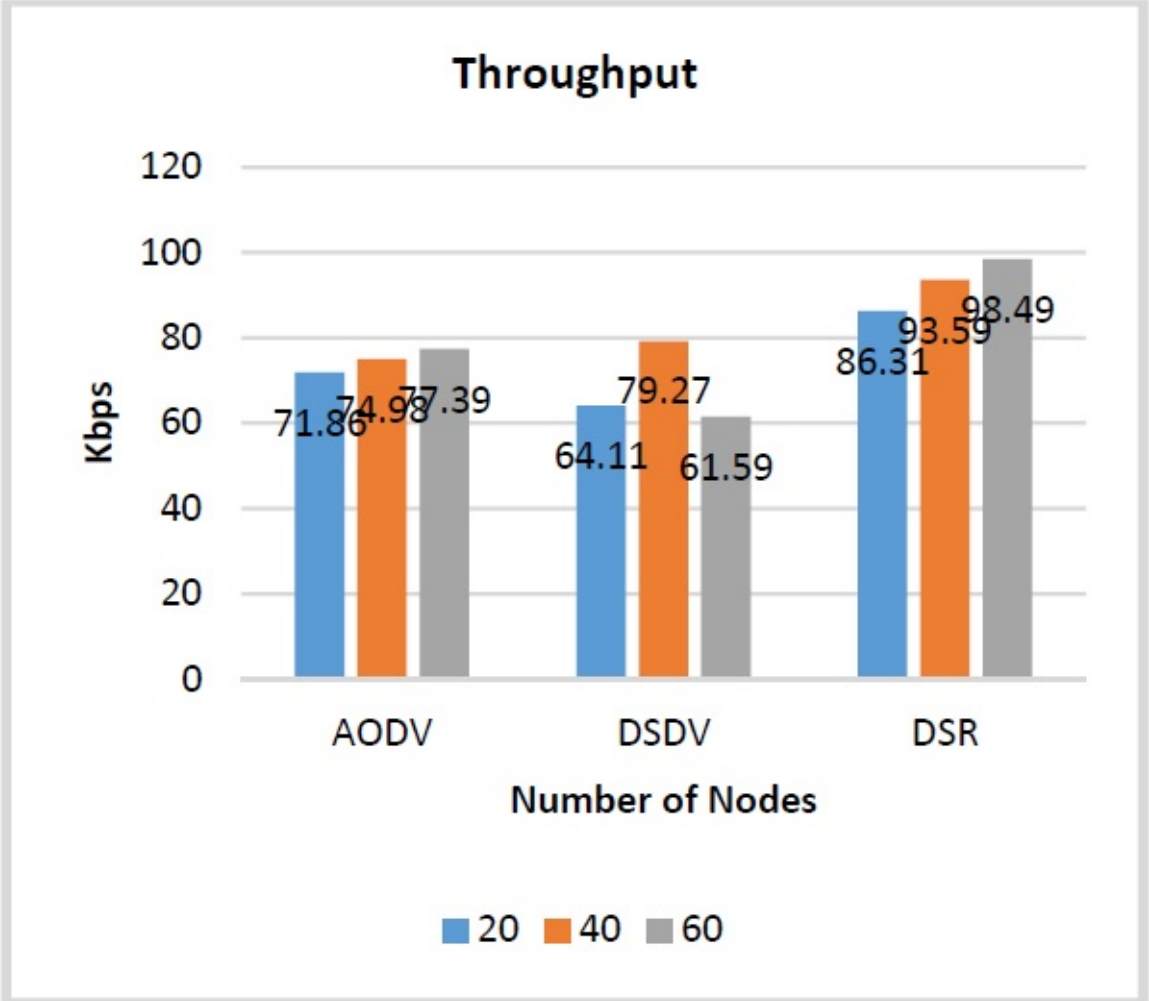


Figure 20. Throughput for three topologies 20 nodes, 40 nodes and 60 nodes [52].

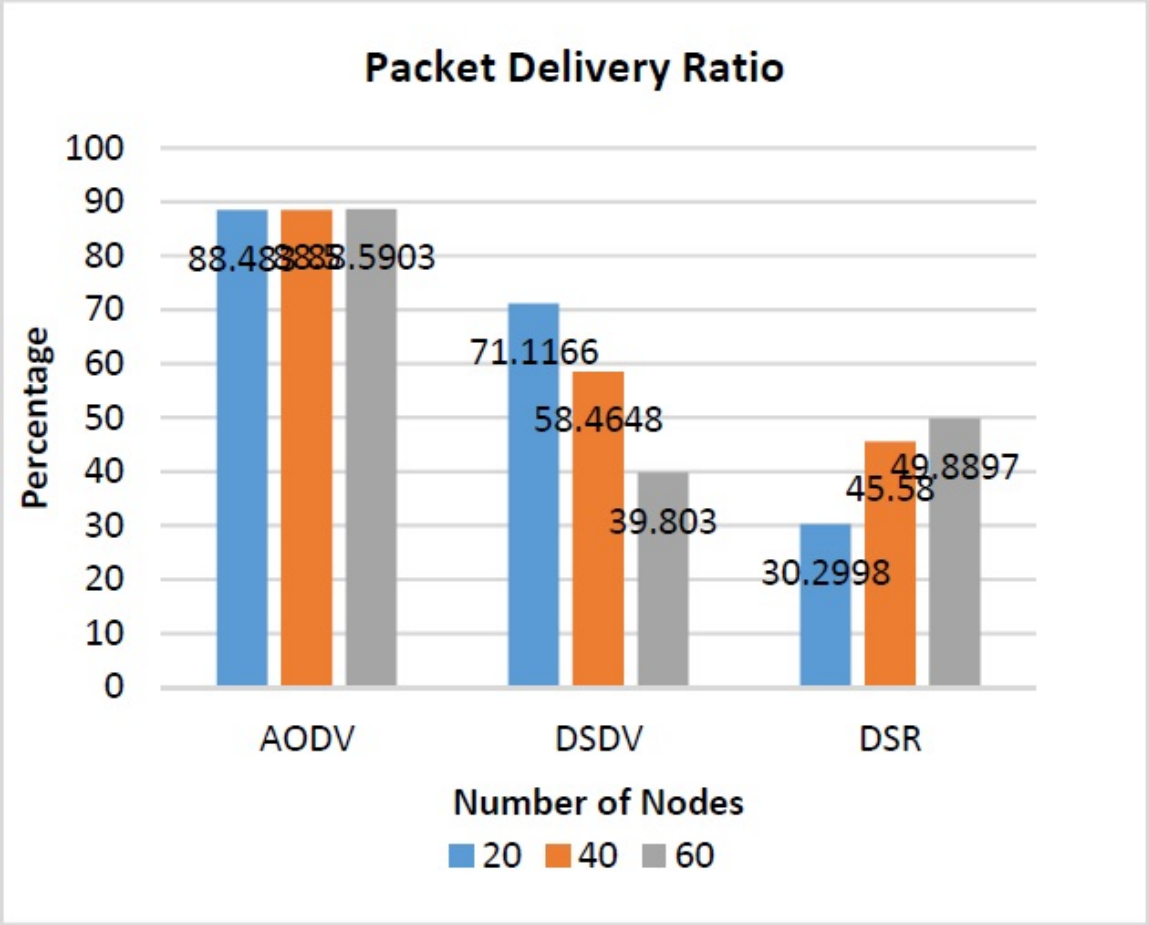


Figure 21. Packet Delivery Ratio for three topologies 20 nodes, 40 nodes and 60 nodes [52].

As we can conclude from Anu Arya1, Jagtar Singh2 [52] comparative study is the whole overall performance of AODV is perform better than both protocols. Also AODV has the ability to send more packets.

CHAPTER IV

ADEL ROUTING PROTOCOL

This dissertation presents Adel routing protocol to enhance security level during data transmission between sender party and receiver party in wireless network environment. Whenever these sensor nodes are placed in the network, they need to inform their location and their data related to the security for the further communication in the network. For that an efficient mechanism needs to be implemented in order to perform better communication among sensor nodes. Adel routing protocol generates dynamic routing table using Ant Colony Optimization (ACO) algorithm with all the necessary information from the network nodes after they being deployed.

Adel routing protocol aims to achieve the following

1. To ensure it achieves the authentication and authorization requirement,

   It generate nodes table that has all the necessary information from all nodes in the network right after deploying it, such as:

   - Sensor Nodes location.
   - Surrounding sensor nodes.

2. To ensure it achieves the integrity and freshness requirement

   - The intended destination sensor node will receive the expected time for the encrypted message arrival, this received packet will be encrypted with its own key inside the message.
   - The intended destination, also will receive the expected time to decrypt the message before tearing it down.

3. Base station generates dynamic routing table that grantees the travel of messages that will be on the shortest path between sensor nodes without having cycle path problems.

    - It uses one of the shortest path algorithms to find the most suitable path between the sender and the receiver party, this path should be the shortest path or the most nearest path to the optimal path between the sender and the receiver nodes among the whole WS network.
    - Before the transmission starts the routing table will be generated and fixed. Then it will transfer within messages among all nodes on the shortest path till it reaches the destination. Once it reaches the destination, it will reverse the order of the table back to the sender.

4. The communication paradigm is from base station to any sensor within the network and vise versa.

5. To avoid cycle paths problem

    - Researchers like Chiang Tzu-Chiang, Chang Jia-Lin, Tsai Yue-Fu, and Li Sha-Pai have presented in their research “Greedy Geographical Void Routing for Wireless Sensor Networks, ” algorithm to solve cycle paths problem. (2013 at World Academy of Science, Engineering and Technology [35]).

      Figure 22. Illustrates a case where cycle path routing could happen.

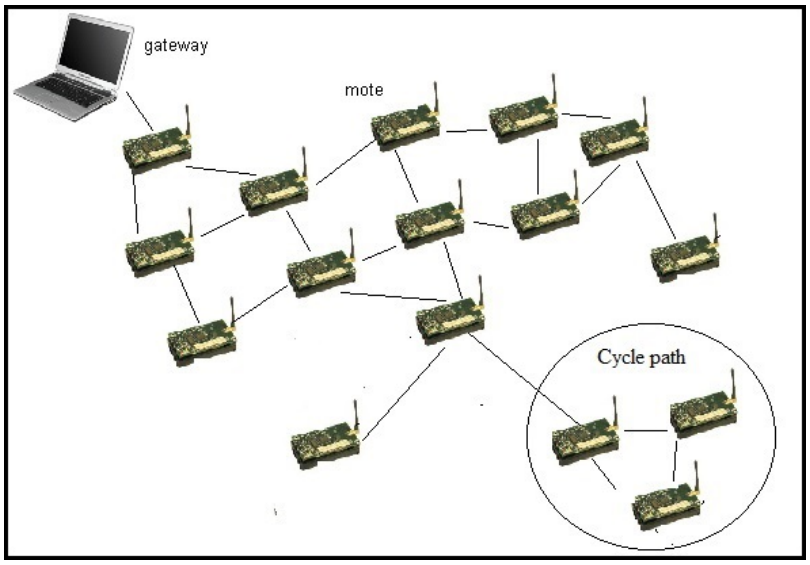


Figure 22. Example of Cycle path in WSN.

- Secure Topology Discovery and Network Setup Protocol could not solve this problem because its WSN contains only inner and outer cycles like Figure 23 below.

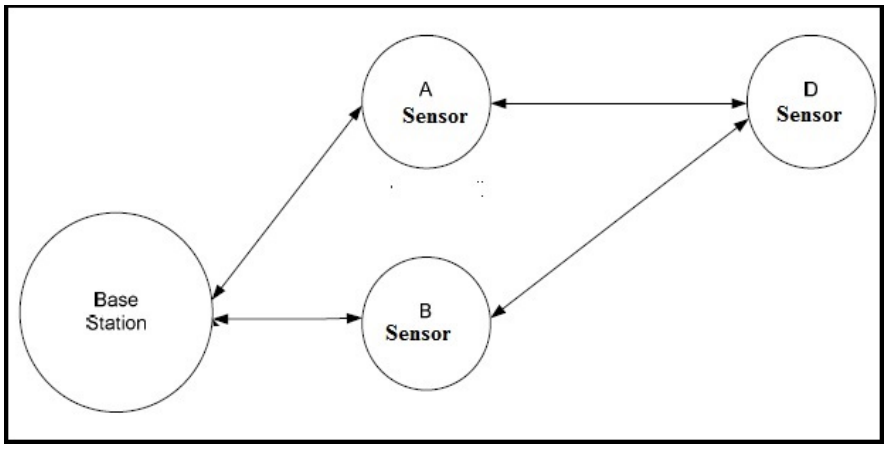


Figure 23. Secure topology discovery and network setup only Inner and outer cycles.

Assumptions

The following are assumptions to run the protocol

- Static WSN.
- Sensor nodes have GPS features.

- Homogeneous WSN.
- The base station is computationally robust.
- The radio range of the sensor node is 15 meters.
- The sensing range of the sensor node is 1 meter.
- All sensor nodes within the network must be time synchronized with the robust base station.

Handshake Protocol Packet Design

- Preamble: contains the sender address (if the sender is the base it will be empty).
- Header: contains the receiver address ,time needed by the message to travel from source to destination and its clock is synchronized with the robust base station Time To Travel (TTT) .The TTT is only used to verify the time needed by a message to travel from the sender party to the receiver party, This TTT can be only calculated at the final destination node, while for the intermediate nodes among the whole network from sender to receiver nodes it is null and Command, the header encrypted by receiver key.
- The payload: contains specific data to be stored in a table. This data is encrypted by the receiver key and contains the location and address of the current sensor node.

Adel Routing Protocol phases

- Phase 1: Start handshaking protocol to generate nodes table
- Phase 2: Use routing function with nodes table to generate dynamic routing table
- Phase 3: Start transmission protocol for exchanging data over WSN

Phase 1

In this phase, the base station collets information from all reachable nodes in the wireless sensor mesh network. This phase explained in the following steps:

- Create a node table has the same size of the network nodes number.
- Set the routing command to hello in the packet header as long as there is empty slots in the node table.
- Handshake protocol starts to authenticate sensor node by collecting all the necessary information, such as location and address of the current nodes.
- Add the current node information to the node table.
- If the node table not full then skip the base station and go to the next node.
- If the node table if full change command to go to base station.

Phase 2

In this phase: Utilize Ant Colony algorithm with nodes table to generate dynamic routing table, it computes the shortest path from each sensor node to the mother node (base station).

Phase 3

In this phase, it starts exchanging encrypted messages among the network nodes, transmission process starts when a node starts to send a request to another sensor node, so a message travels between the node and multiple nodes till it arrives to the intended destination. During this stage, the network datagram is already has been sent to do handshaking then collects the addresses of the sender and the receiver and each node it goes through, these addresses and datagram TTT (time to travel) encrypted with public cryptographic keys .After initiation of the cryptographic key the sender will start sending a cryptic data using the key. Now the Receiver receives data then decrypts the data using

the key that is familiar to it. Also the data in packet payload has limited time to decrypt before it turns down TTDP(Time To Decrypt Packet).

The following is a pseudo code for routing technique during exchange data among the sensor nodes. The handshake protocol to generate routing table during the first phase It creates a table to store important information, this contains static network link information.

```
int nodes[i][j]
Create visited list int nodes_list[k];
Create single array for neighbors int next_to_baseStation[a];
int current_node;
From the base station to neighbor nodes
for(int j=1;j<=n;j++)
{
if link exists between base station '0' and node 'j'
   if(nodes[0][j]==1)        {
    from base station to the node 'j'
        Then send packet to the nodes[0][j];
        then add the node to 'j' to the visited list
         nodes_list[k++]=j;
            this is base station neighbors list
                next_to_base[a++]=i;
        }
  }
```

from the next node of base station to the other nodes

```
for(int a=1;a<=n;a++)
{
    current_node=next_to_base[a];
     then from neighbor node to the remaining nodes
    hand_shake(current_node);
}
```

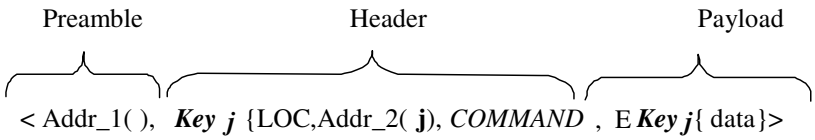
Create function used for how to send packets to other nodes until the all nodes visited

```
void hand_shake(int d)
{
    for(int j=1;j<=n;j++)
      {
        int flag=0;
          if(nodes[d][j]==1)
            {
              check the already visited nodes
              while(k<=n)                    {
                if node not previously visited then execute
                  if(nodes_list[k] =! j)                    {
                    send packet to other nodes[d][j];
                     nodes_list[k++]=j;
                      flag++;
```

```
                    make function shake that is a recursively called by other nodes
                        hand_shake(j);
                    }
                }
            }
        }
        if(flag==0) // used to backtrack to the initial stage
        {
          then back track the network;
        }
}
```

The following is the handshake protocol to generate routing table during the first phase of the proposed protocol:

HANDSHAKING PROTOCOL TO GENERATE ROUTE TABLE



C ← all sensors in Sensor Network

Nodes Table ← Φ

∀ J □ C do

For j=1 to C

IF Nodes Table not full

Then

skip Base Station

Node j → Next Node j : <Addr_1(j), **EKey** $_j$ {Addr_2(Next Node j), *HELLO}*,

EKey $_j$ {Node Table[LOC_j][$Addr_j$]} >

Nodes Table ← Nodes Table + j()

Node j ← Next Node j

IF j equals to C Then

Nodes Table ← Nodes Table + Next Node j()

j = 1

Else

Node j → Next Node j : <Addr_1(j), **EKey** $_j$ {Addr_2(Next Node j), $SEND_{bs}$*}*,

EKey $_j$ {Node Table[LOC_j][$Addr_j$]} >

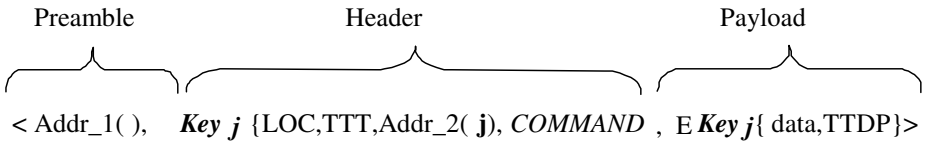
Node j ← Next Node j

IF Next Node j equals to Base Station

END For Loop

Route Table ← Nodes Table + Route Function

TRANSMISSION PROTOCOL FOR WSN



C ← all sensors in Sensor Network

If R_Cost =1

then

Temp Route Table ← j

J □ C do

Base Station → j : <Addr_1(), E**Key** $_j$ {LOC_{bs}, TTT_j, Addr_2(**j**), *COMMAND}*,

EKeyj{data,TTDP} >

j → Base Station : < Addr_1(j), E**Key** $_j$ {LOC_j, TTT_{bs}, Addr_2(), *COMMAND-REPLY}* , EKeyj{data,TTDP} >

Else

K □ C do

Generate K Route Table

K □ Nodes Table do

Base Station → j : <Addr_1(), E**Key** $_j$ { LOC_{bs}, TTT_j, Addr_2(**j**), $SEND_K$*}*,

E**Key** $_k$ {(R_Table[], *COMMAND),TTDP}*>

J → k: <Addr_1(**j**), EKey

$_k${LOC_j,TTT_k,Addr_2(**k**),*COMMAND}*,

E**Key** $_k$ {(R_Table[], DATA), *TTDP* }>

k → j: Addr_1(k), header,

payload > where:

header = E**Key** $_j$ { LOC_k, TTT_j, Addr_2(j), $SEND_{bs}$*}*

payload = E**Key** $_j$ {(R_Table[], DATA), *TTDP* } >

j → Base Station: Addr_1(j), header, payload >

where:

header = E**Key** $_j$ {LOCj, TTT_{bs}, Addr_2(),*COMMAND-REPLY }*

payload = E**Key** $_k$ {(Addr_3(**k**), DATA*)*, TTDP} > End IF

Shortest Path Algorithm

Ant Colony Optimization

The ant colony optimization algorithm (ACO) is a technique based on probabilistic algorithm for finding shortest optimal path, which can be reduced based on the behavior of ants to finding good shortest paths between ants nest and food location. At the beginning an ant go looking for food and once it finds a source of food, it start gathering food and produce a pheromones during her walking back to nest. Now when other ants come across the pheromones, most likely they will follow the same path with a certain probability. Also, these ants will mark their paths to the food source with their pheromones to assure to other ants about the food source path to other ants in the colony. This ACO algorithm is one of the members of ant colony algorithms family, it uses swarm intelligence process, the first version of ACO algorithms goals was to search for an best path in a graph; the basic concept has was to solve a lager scale of numerical problems, as consequence, some problems have emerged or drawing on numerous aspects from the ants behavior. The ants interact in such way as freelance agents which interact and communicate via indirect intercourse known as stigmergy.

T.Nishitha and P.Chenna Reddy [47] have defined it as “Stigmergy is an indirect form of communication where individual agents leave signals in the environment and other agents sense them to drive their own behavior. This form of communication is local wherein simple agents interact locally without having any global information.”

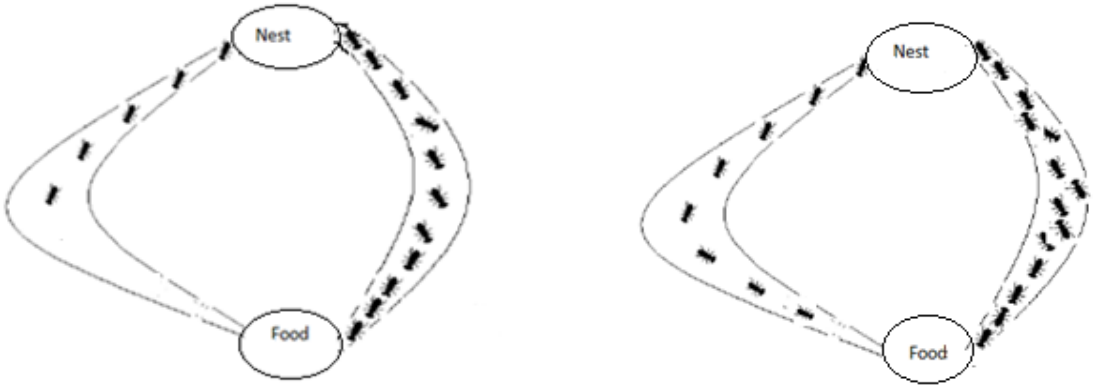


Figure 24. Ant colony optimization.

Figure 24 shows how research paper [48] explains ACO. Ant colony optimization: (a) Ants using two ways to reach the food source takes less time. (b) Ants using shorter path will get to their nest faster, while the ants on the other path will take more time.

Flowchart of ACO routing algorithm illustrated in Figure 25.

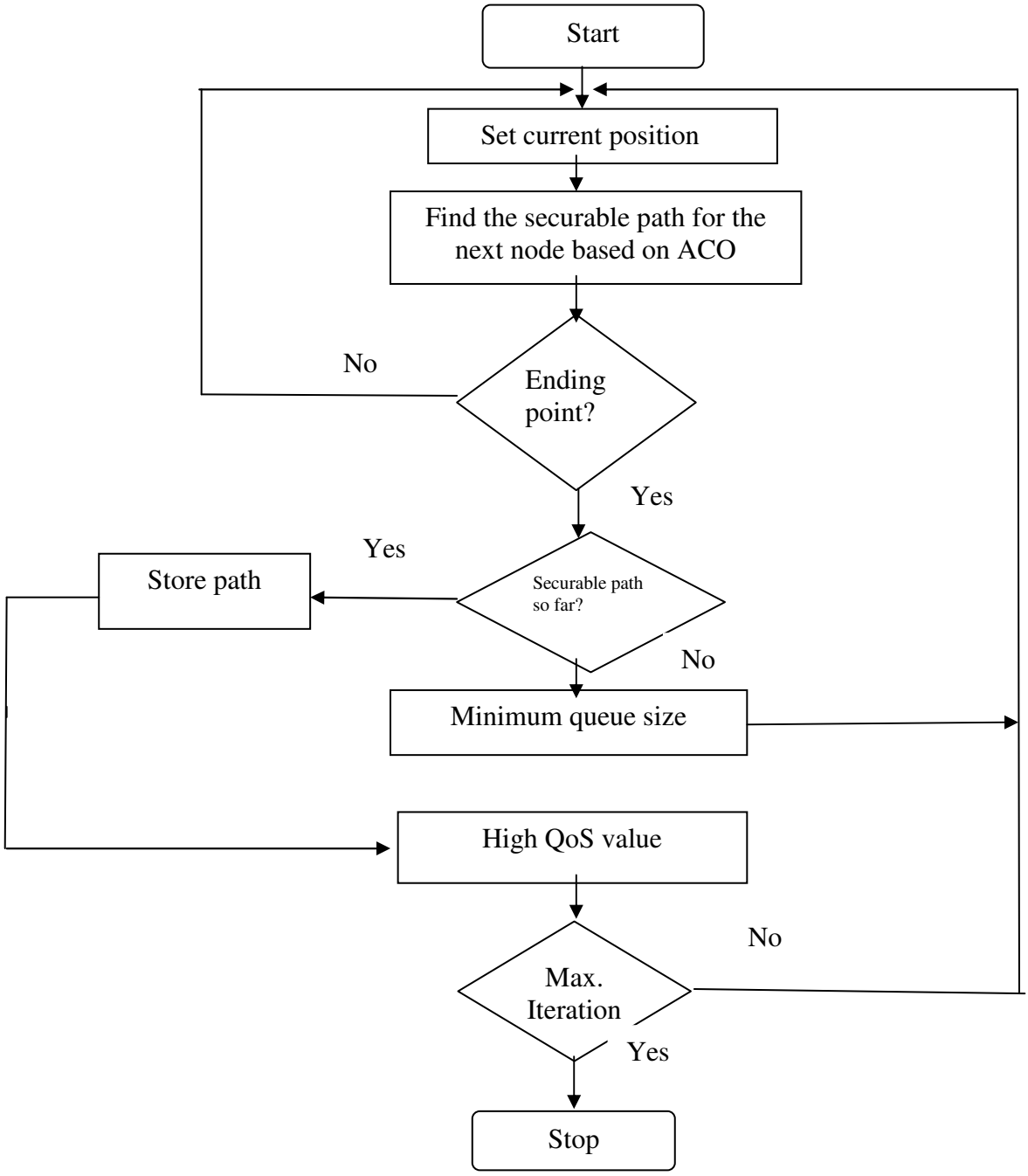


Figure 25. ACO routing algorithm.

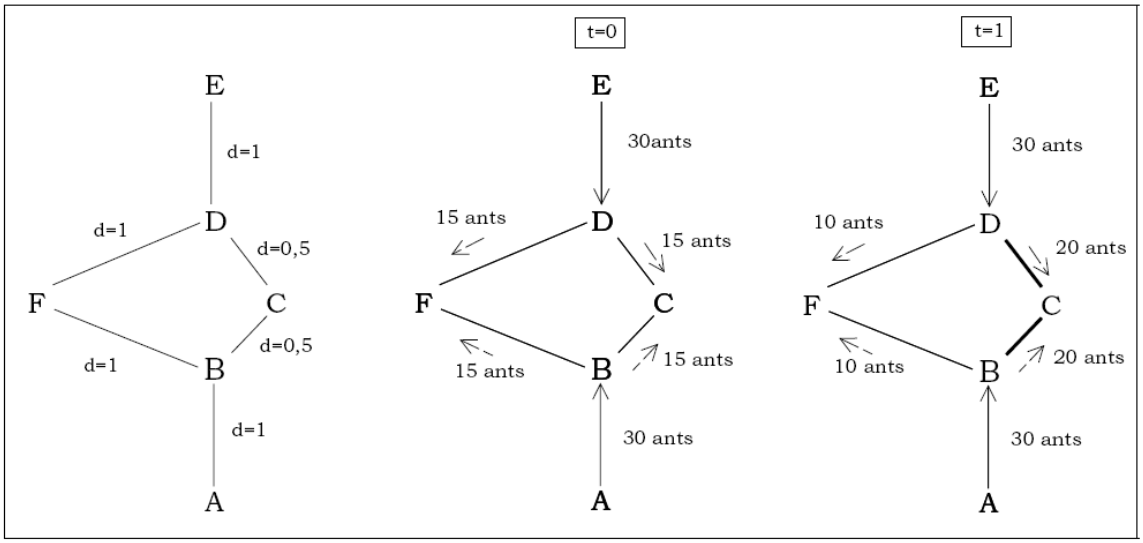


Figure 26. Successive AS tour progression over a simple graph. Note how the pheromone values change between time t = 0 … 1 (preferring BCD) [48].

Advantages of Ant Colony Algorithm:

- Collateral parallelism.
- Positive feedbacks for brisk discovery of optimal solution.
- Efficient in finding short path such as Traveling Salesman Problem (TSP) and other analogous problems.
- The fact it adjust to new modifications such as a distances increases makes it useful for dynamic applications.
- Convergence is guaranteed.

Disadvantages of ACO

- Theoretical analyses are complicated.
- Series of indiscriminate decisions.
- Probabilities distribution variation by refinement.

- Time to interchange ambiguous

Proposed System Block Diagram

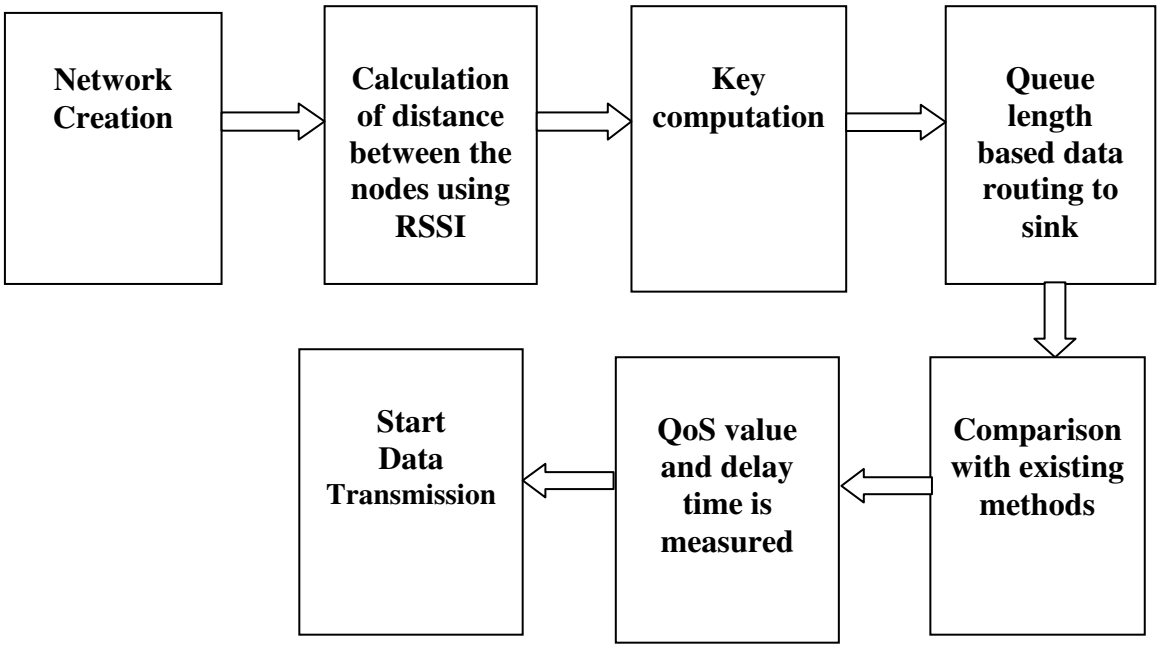


Figure 27. Block Diagram of proposed system.

Researchers also consider important aspects in their researches [50], [52], [54], [56], [59], [64] such as:

Validity time:

Validity time indicates a time limit, which states and specifies the time for packet to be transferred and delivered at the destination end. The destination node always specified with the certain time limit for receiving data.

VT = C * (1 + a/16) * 2^b

Where C is a scaling factor for the "validity time" calculation

A is the higher order bit

B is the lower order bit

Vtime = 0.0625 * (1 + 2/16) * 2^2

= 0.281 sec

As validity time decreases, we need to process the packet very quickly with the help of priority, so that we can increase the performance.

Packet Delivery Fraction (PDF)

The PDF states number of message packets to deliver at the receiver side successfully, which is transmitted, from the sender.

$$PDF = \frac{\text{Number of received packets}}{\text{Number of sent packets}}$$

This estimation gives us an overview of how effective is this protocol when it comes to delivering messages packets. When doing the performance analysis on a new routing protocol, the higher packet delivery ratio the more it indicate the successfulness and the better it is.

Average End-to-End Delay (AED)

In the world of routing protocols the average time used by the data packets to reach the intended destinations node can be defined as Average End to End Delay (AED). Many reasons can cause delay throughout the WS networks such as queuing delay, broadcasting delay, computing delay, packets preparing time etc. It can be represented as next:

$$AED = \frac{\Sigma\ (\text{time received} - \text{time sent})}{\text{Total data packets received}}$$

Challenges

Although of the huge diversity of applications, wireless sensor networks face a number of uneasy technical problems due to the following factors:

Firstly WSN deployment: Most wireless sensor nodes are placed in an unfriendly environment, which might have no good infrastructure. A normal way of deployment sensor nodes in a forest for example, would be throwing out the sensor nodes from a plane. In such a case, it is entirely up to the sensor nodes to determine the connectivity and allocations.

Unattended processes: In many situations, Wireless sensor nodes are deployed in an unstructured environments, once sensor node has been deployed, the wireless network has no human interference. Therefore the sensor nodes themselves are in charge of reconfiguration in situation of any mobility.

Untethered: In general, the wireless sensor nodes are not linked to energy source. This means these nodes have limited source of energy, which must be used in the best way for operating, remains active as much as WS needed and communication during data transmission among the WN. Energy consumption in WSN is a growing research filed in order to have the optimal use of energy in WN, in some cases the processing and transmission energy between in active nodes should be reduced as much as possible (stand by mood).

Adel-Handshake Protocol Cost Calculation

Let A_d is the size of the preamble in the message packet

Let H is the size of the Header in the message packet

Let P_y is the size of the payload in the message packet

Let L be the total size of the message packet

L = (Preamble + Header + Payload)

Then total size of the message packet will be

$L = A_d + H + P_y$ in terms of bits ---------- (1)

For example,

Let ‘t’ is the time to prepare a one bit of data at source node.

So, the time to prepare a ‘L’ bits of data is L*t

From (1)

Total time to prepare a packet = L * t

$$= (A_d + H + P_y) * t$$

Let C_p be the total cost for preparing a packet,

Here we assume that the time to prepare a packet is also the cost for preparing a packet,

So,

Total time to prepare a packet = total cost for preparing a packet,

Therefore from the above equations,

Total cost for preparing a packet $C_p = (A_d + H + P_y)t$ ---------- (2)

For handshake between nodes initially a sample packet with “HELLO” command will be sent to every node and the handshaking is done successfully

Firstly the Base station sends the “HELLO” packet to one of the neighbor nodes.

Base station -> 1^{st} node

t_p is time to send ‘1’ bit of data

So the total time to send a packet is $L * t_p$

$$= (A_d + H + P_y) * t_p$$

$T_{BS \text{ -> } 1st}$ is the Total cost to transmit a packet from Base station to neighbor node in terms of time

$T_{BS \text{ -> } 1st} = (A_d + H + P_y) * t_p$

T_{cost} be the total transmission cost

(total transmission cost is = Cost to prepare a packet at Base station +cost for sending the packet)

$T_{cost} = C_p + T_{BS \rightarrow 1st}$ ---------- (3)

Then from neighbor node (1) to remaining nodes {2,3,…..,n-1,n}

$\sum_{i=1}^{n} (C_p + D_i + T_{i \rightarrow i+1})$---------- (4)

When, D_i is delay at every i^{th} node

Ti -> i+1 is time to send the message packet from i^{th} node to $(i+1)^{th}$ node

C_p be the cost to prepare a packet at every i^{th} node

From (3) and (4)

For one time hand shaking between all the nodes will be

$C = C_p + T_{BS \rightarrow 1st} + \sum_{i=1}^{n} (C_p + D_i + T_{i \rightarrow i+1})$ ---------- (5)

Adel-Transmission Protocol Cost Calculation

If neighbor node is the destination node:

Let A_d is the size of the preamble in the message packet

Let H is the size of the Header in the message packet

Let P_y is the size of the payload in the message packet

Let L be the total size of the message packet

L = (Preamble + Header + Payload)

Then total size of the message packet will be

$L = A_d + H + P_y$ in terms of bits ---------- (1)

For example,

Let ‘t’ is the time to prepare a one bit of data at source node.

So, the time to prepare a 'L' bits of data is L*t

From (1)

Total time to prepare a packet = L * t

$$= (A_d + H + P_y) * t$$

Let C_p be the total cost for preparing a packet,

Here we assume that the time to prepare a packet is also the cost for preparing a packet,

So,

Total time to prepare a packet = total cost for preparing a packet,

Therefore from the above equations,

Total cost for preparing a packet $C_p = (A_d + H + P_y)t$ ---------- (2)

For transmitting data from Base station to the neighbor node,

We have so many possibilities for transmitting messages from the robust mother node (base station) because we do not know how many nodes are directly connected to the base station.

Let 'm' be the number of neighbor nodes around base station

Let 'n' be the number of all nodes exits in the whole WN

So probability of selecting one node from out of m nodes for sending a packet,

P_r (If neighbor is destination) = $({}^mC_1)/({}^nC_1) = m/n$

With (m/n) probability then BS can transmit data of size 'L' to one of the m nodes

1,2,…….,m-1,m nodes

So time to send the packet with (m/n) probability is = $C_p + T_{BS \rightarrow j}$ ---------- (1)

Where

$T_{BS \rightarrow j}$ = from base station to j^{th} node out of m nodes

Then again destination node ‘j’ replies to the base station

with “ACKNOWLEDGEMENT”

Transmission time = $C_p + T_{j \rightarrow BS} + D_j$ ---------- (2)

Where ‘D_j’ is delay at node ‘j’

From (1) and (2)

With probability of (m/n)

Total time = $2\ C_p + T_{BS \rightarrow j} + T_{j \rightarrow BS} + D_j$

Here $T_{BS \rightarrow j} = T_{j \rightarrow BS}$

So $T_{BS <-> j} = T_{BS \rightarrow j} + T_{j \rightarrow BS}$

Because the transmission time for sending a packet will be equal to the transmission time for receiving the packet.

$= 2\ C_p + T_{BS <-> j} + D_j$

The trust of packet sending and receiving depends on the probability (m/n).

For any sensor node in the network: -

To send message packet from Base station to any node ‘k’ in the network

We have to generate a route table for ‘k’ and the probability of generating the shortest path to K depends on routing table

Suppose total ‘L’ number of links among the whole WN

And ‘S’ is the exact number of links connected to the ‘k’ node.

Probability of choosing best path out of S links will be

$= ({}^{S}C_1)/({}^{L}C_1)$

$= S/L$

With this probability (S/L)

Route table will be generated for k^{th} node from base station, which describes its path to travel in the network

BS -> j -> j +1 -------- -> K

Where j, j+1 and so on are the intermediate nodes between Base station and K

After establishing the route table then every node should select the correct node with (m/n) probability

Where,

m is a number of the neighbor sensor nodes at every j^{th} node

n is the overall number of sensor nodes

So probability of sending packet from Base station to any 'K' node is

$$(S/L) * (m/n) = (Sm/Ln)$$

With this probability, every node sends the data efficiently to the following nodes as given in the route table

Time to transmit from Base station to j^{th} node is

$$C_p + T_{BS \rightarrow j} \text{ ---------- (1)}$$

Suppose 'I' be the total number of Intermediate nodes between Base station and 'K'

Then time to transmit from one sensor node to another sensor node is same

i.e., $= C_p + T_{j->j+1} + D_j$

Where,

$T_{j->j+1}$ is the time to travel from j to $(j+1)^{th}$ node

D_j -> delay at every j^{th} node

So the total time to send packet from j^{th} node to 'k' node

= Sum of time to transmit between two intermediate nodes

i.e.,

$\sum_{j=1}^{i-1} (C_p + T_{j->j+1} + D_j)$ ---------- (2)

From (1) and (2)

The total time to transmit data from Base station to 'k' node is

$= C_p + T_{BS\ ->\ j} + \sum_{j=1}^{i-1} (C_p + T_{j->j+1} + D_j)$

With the probability (S/L) it will pick the shortest path from base station to the intended destination with intermediate nodes j, j+1 and so on.

After choosing the shortest path with the probability (S/L) it will select the best intermediate node with the probability (m/n)

So finally the packet is transferred from Base station to the Destination node with (Sm/Ln)

Network Simulator to Develop Adel Routing Protocol

The network simulator NS2 software has been used to validate my work to develop wireless sensor network to run Adel routing protocol. There are various types of network simulators are obtainable like NS2, TOSSIM, SensorSim, OPNET etc. From that, we selected the network simulator 2 (NS-2) to develop our proposed protocol, also to evaluate the security and efficiency of proposed routing protocol, NS-2 it is the one of the most acceptable simulator for wired and wireless networks in academic research fields, also it is open source. The first version was developed in 1995 and the second version was released in 1996. NS-2 uses animator to visualize the simulation of networks Figure 28.

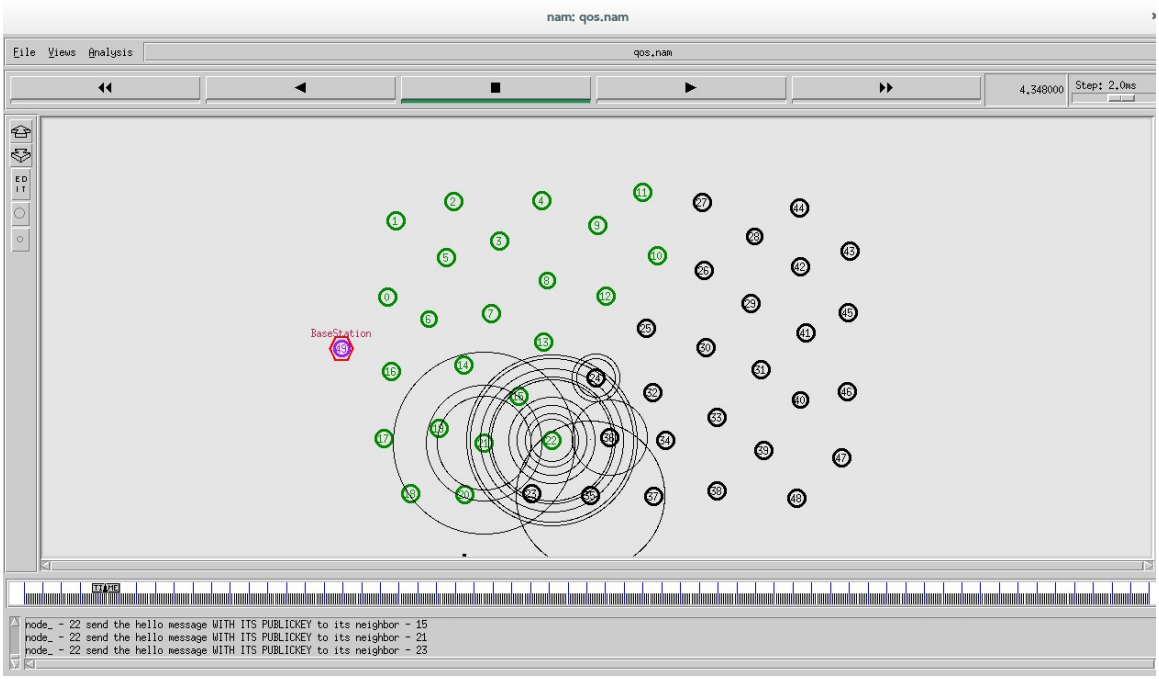


Figure 28. NS-2 animator.

NS-2 was the result of a cooperation of institutes like UC Berkeley, XEROX PARC, AT&T and ETH [56]. According to [42], [43], [55] basically NS-2 is an object-based development tool, which encapsulate individual objects that is linked one to each other's within a system hierarchy. NS-2 uses C++ as a front end and OTCL as an interpreter. It realizes the basic structure of the NS-2 network simulator [43].

Network simulator 2 uses two of the basic languages for developing and accomplishment their missions and meet their needs. First, the study of routing protocols needs a systems of strong programming languages, which can helps to involve bytes, bits, message packets header, and develop algorithms that can execute over large sets of data. Second, the execution time speed and change time is lesser important than real time simulation time. Routing protocols evaluation performance on NS2 simulator. Three main parameters are considered for evaluation: throughput of WN, packet delivery ratio and end to end delay.

1) Throughput: It is the overall number of received packets from the sender party to the intended destination node out of the overall packets that have been transmitted during the transmission session.
2) End to End Delivery Ratio: is the average time used by the data packets to reach the intended destinations node can be defined as Average End to End Delay (AED). Many reasons can cause delay throughout the WS networks such as route finding process, queuing delay, broadcasting delay, computing delay, packets preparing time etc. Only the successful message packets to reach the destination sensor node are counted.

3) Packet Delivery Ratio: It is the ratio of number of messages packets to deliver at the receiver side successfully, which is transmitted, from the sender. This estimation gives us an overview of how effective is this protocol when it comes to delivering messages packets. When doing the performance analysis on a new routing protocol, the higher packet delivery ratio the more it indicate the successfulness and the better it is. [66], [67].

The command and configuration interface in Network Simulator is developed in C++ programming language with an OTcl interpreter. C++ is used for detailed protocol implementation. The C++ part, which is quick to execute but slower adopt to changes, is utilized for itemized convention execution and on the other hand the OTcl part, then again, which runs slower however it can be modified exceptionally quickly, is utilized for real time animation configuration using animator NAM. One of the most advantages of using these two languages in this program process is that it considers quick era of huge situations. To just utilize the NS-2, then we will need to have suitable knowledge of OTcl

language. At the other side there is one disadvantage is that modifying, changing, expanding and enlarging the NS-2 simulator can obliges the programming at both dialects.

The following are the various kinds of simulations that can be done by using the Network Simulator NS-2 as described in [42], [43].

1. Routing: dynamic and Static routing
2. Topology: Wireless and Wired Networks.
3. Application: HTTP, FTP, Telnet etc.
4. Transport: TCP, UDP etc.

USER'S VIEW OF NS-2

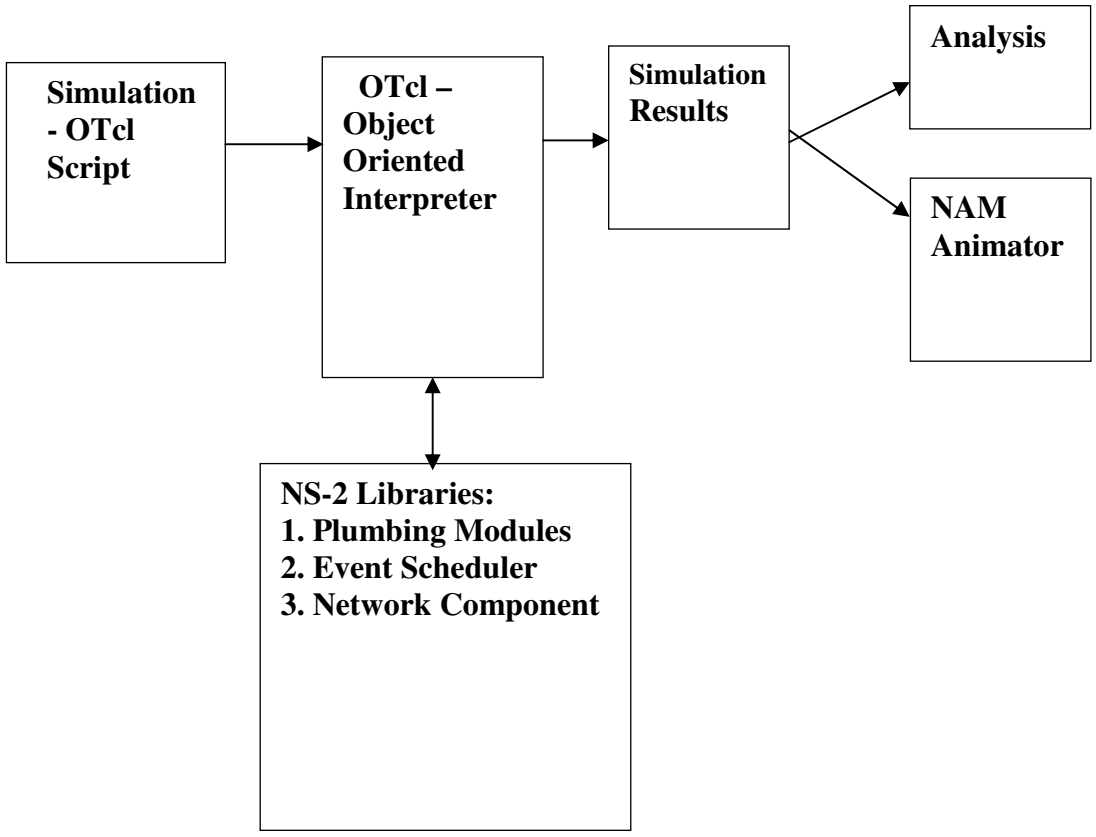


Figure 29. Block diagram of Architecture of NS-2.

Network Components

In this section a description about the NS-2 components inside, in general it compound all the network entities.

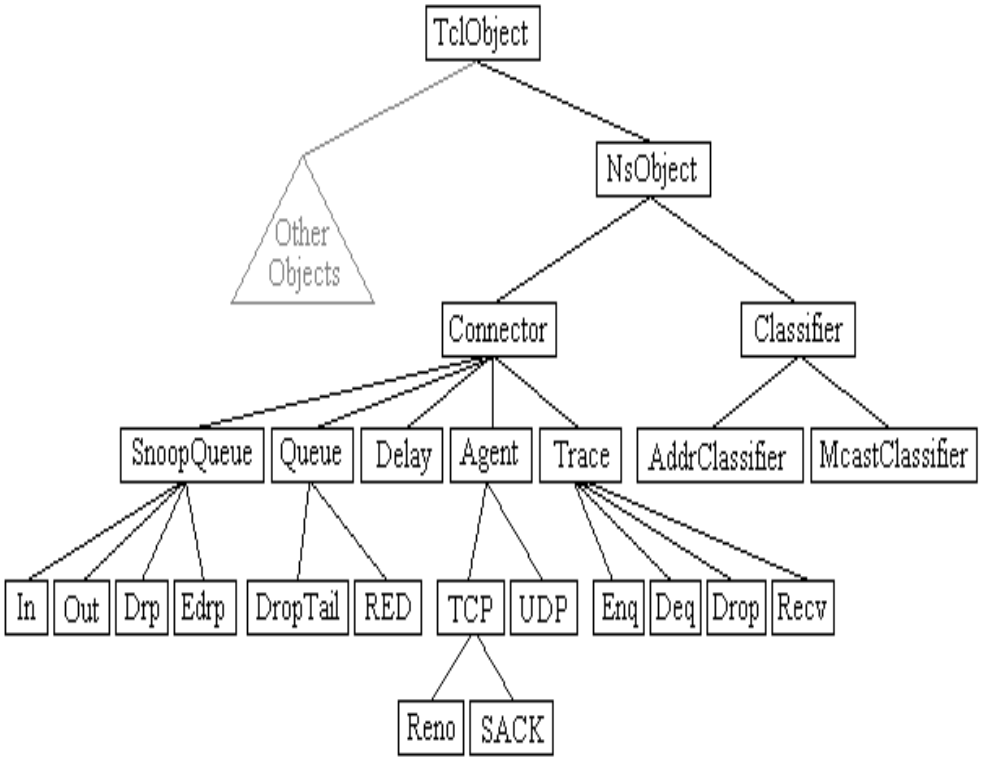


Figure 30. OTcl class hierarchy as stated in [55].

TCL Class

The population Tcl elements are the real occurrence of OTcl interpreter, furthermore gives the procedures to communicate within this interpreter, code. Those classes give methods for the following operations as stated in [43].

1. Obtain a reference to the Tcl instance
2. Invoke OTcl procedures through the interpreter
3. Retrieve, or pass back results to the interpreter
4. Report error situations and exit in a uniform manner

5. Store and lookup "TclObjects"

6. Acquire direct access to the interpreter.

Common Simulation Parameters to evaluate Adel Routing protocol

To evaluate and test out proposed routing protocol for transmission date in wireless sensor network, the following parameters were considered:

1. *Packet Delivery Fraction:* It is the ratio of number of messages packets to deliver at the receiver side successfully, which is transmitted, from the sender. This estimation gives us an overview of how effective is this protocol when it comes to delivering messages packets. When doing the performance analysis on a new routing protocol, the higher packet delivery ratio the more it indicate the successfulness and the better it is [42], [66], [67].

2. *Average Throughput:* It is the overall number of received packets from the sender party to the intended destination node out of the overall packets that have been transmitted during the transmission session [42].

3. *Packet delay:* Is also known as end to end delay average time, which is used by the data packets to reach the intended destinations node can be defined as Average End to End Delay (AED). Many reasons can cause delay throughout the WS networks such as route finding process, queuing delay, broadcasting delay, computing delay, packets preparing time etc. Only the successful message packets to reach the destination sensor node are counted. By packet to reach the final destination from initial source. It will give the network transmission speed [44]. These three parameters will give the result about performance of routing protocol. In addition to these there are other parameters less considered like Latency, Network Life Time, and Packet generation rate.

Performance Evaluation of Adel Routing Protocol

Routing protocol is significantly leading matter when it comes to performance evaluations in Wireless sensor networks [42]. Firstly, we have to overcome the initial factors which degrade the performance before we focus on the proficient communication can be accomplished in wireless sensor networks. Sensor node distribution is depends on the application and distresses the performance of the routing protocol in wireless sensor network. So, our protocol as shown in Figure 31. Has handshaking sub protocol, it can overcome this sensor deployment problem by initially sending Hello message to every node in the whole network.

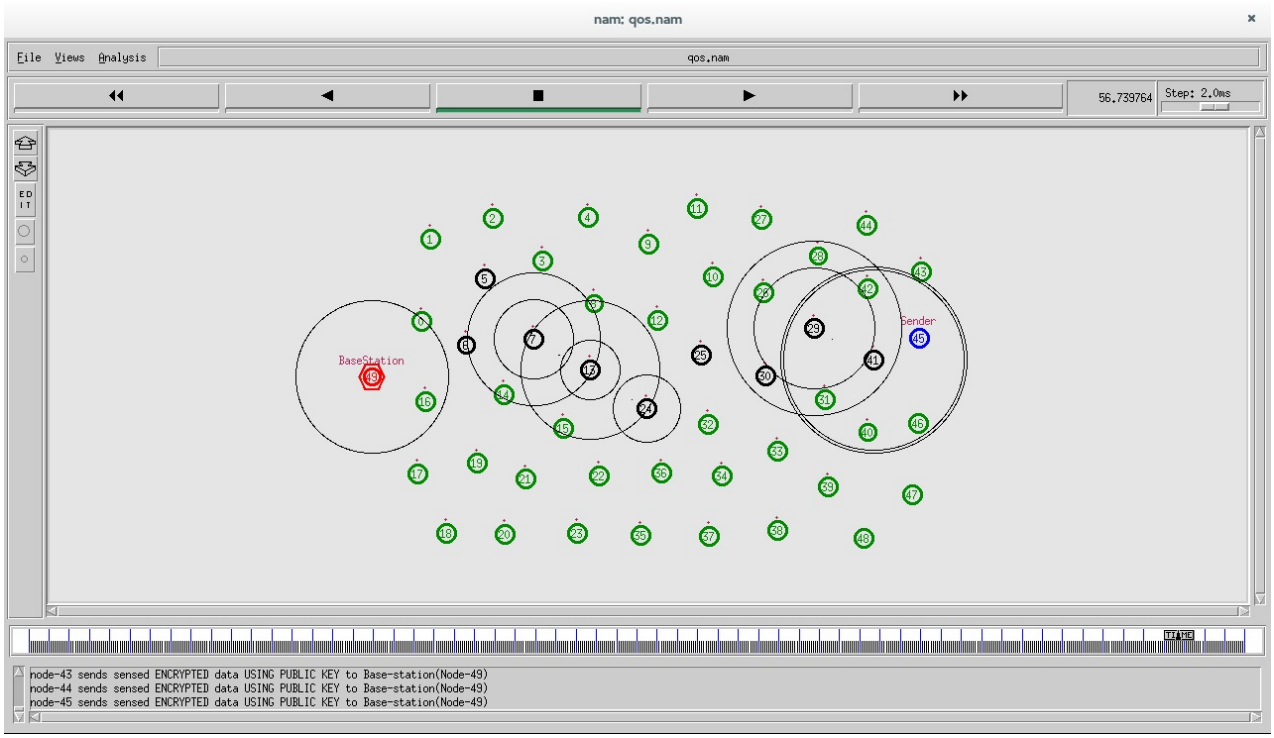


Figure 31. Simulation of 50 nodes WSN running Adel routing protocol.

Secondly, Sensors can execute and run their computations and data communications transmission of data in a physical links free environments by using some of their energy supply [45]. Our protocol can prepare routing table for every node at base

station then base station transmit the routing table to every node. So, sensor nodes no need to compute the routing information every time then they can effectively use their energy for data transmission and receiving only. So, with the new protocol sensor nodes can optimize their power resources.

There are other main concerns, which influence the performance of wireless sensor networks location as error tolerance, communication media, coverage, data collection, network connectivity and quality of services. In Wireless sensor networks, the node concentration, network size and topology are influenced by scalability factor. This factor comes out form the fact that the range of sensing is less in network communication and needs of nodes are bigger for area covering [42]. So, we have to evaluate the scalability of the wireless sensor network against the routing protocol.

The evaluation of the performance and network scalability problem in WSN is a big experiment because different types of routing protocols, the bigger number of sensor nodes, and the variety of network sensor nodes applications. The evaluation of the SN scalability is not eventually achievable on the real network, and with help of network simulator, it can provide a meaningful perspective into the study of the sensor networks scalability [44], [46]. For that we use the ns2 network simulator to evaluate different parameters in order to know the protocol performance and evaluation.

Evaluating the new protocol

In our new protocol we prepared the packet with the Permeable, header and payload. Here we sent the Address of source node in permeable, address of the destination in the header node and data packet in the payload. We provided the

encryption at header and payload in order to avoid the attacks. From that we can achieve the security at transmission level by using this new protocol.

In the new routing protocol we prepared the special module to generate routing table at every node. So, any sensor node can easily transmit the data easily to the intended destination node by using the routing data. By using route tables at every node this protocol can get the good results in Success rate, good throughput and packet delivery ratio. It can also achieve the better performance. Here our assumption in the new protocol is static and well-connected mesh network. So, there is no packet-dropping problem between source and destination. From all the above our new protocol can give the good performance in wireless sensor network.

Simulation parameters of 50 nodes network

Table 5

Simulation parameters

Simulation Parameter	
1. Network Size	~702 M2
2. Number of Sensors	50

Table 5 (continued).

Simulation Parameter	
3. Node Placement	Uniform
4. Radio Range	15
5. MAC Layer	IEEE 802.11
6. Size of Data Packet	64 byte
7. Number of Actuators	1
8. Antena model	Antenna/OmniAntenna
9. Initialenergy	100 Joules

Results

The following graphs in figures 30, 31,32,33,34 and 35 shows the performance evaluation of Adel routing protocol in subject of security, connectivity and energy consumption also a comparison with other routing protocols. Our proposed protocol have shown good enhancement level in security and connectivity but as we have expected didn't do so well in energy consumption, our main goal was to enhance security and connectivity level.

Simulation Analysis of 50 Nodes Network - Security Analysis

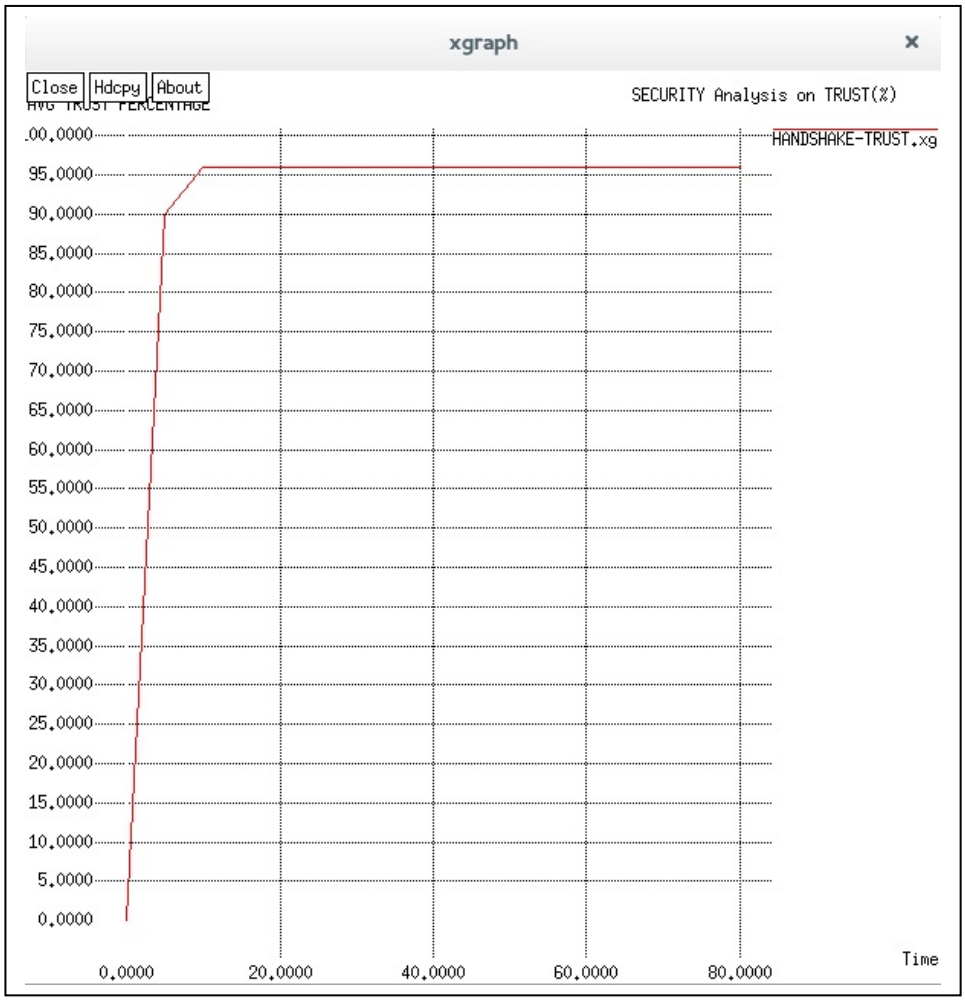


Figure 32, Average trust percentage of 50 nodes.

Figure 30 shows a security analysis of WSNs running Adel routing protocol using NS-2 network simulator, it runs average trust test which shows that a percentage of 96% of security trust during the simulation running time. This high level of security was expected since we have focused on authenticating all the network nodes from the beginning, using the elements of time and distance between sensor nodes.

Simulation Analysis of 50 Nodes Network - Packet Drop

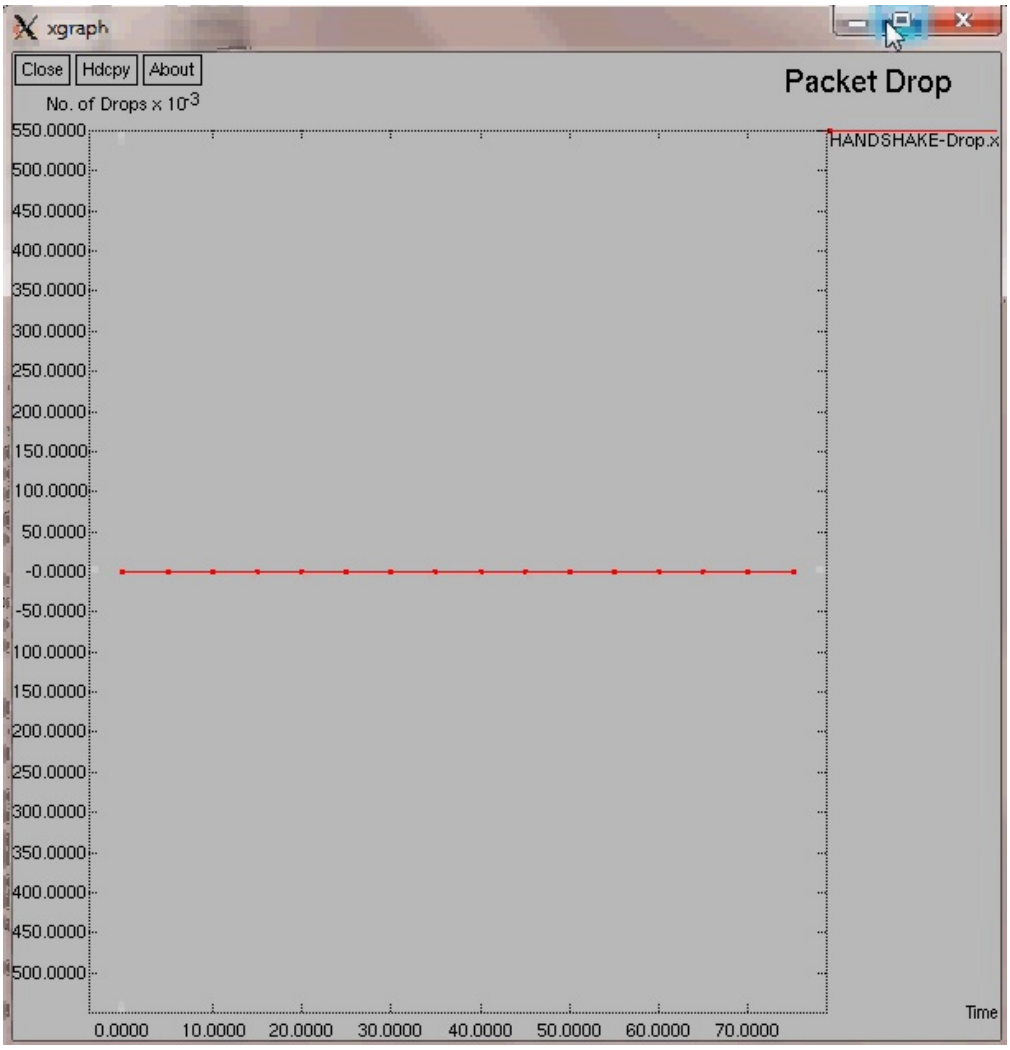


Figure 33. Packet drop test on 50 nodes.

This packet drop test shows in Firgue 33 and 34 that Adel routing protocol has dropped 0 packets comparing to Quality of service particle swarm (QoS-Pso) protocol and to Ad hoc On-Demand Distance Vector during the running time of this simulation.

Simulation Analysis of 50 Nodes Network - Packet Drop comparison

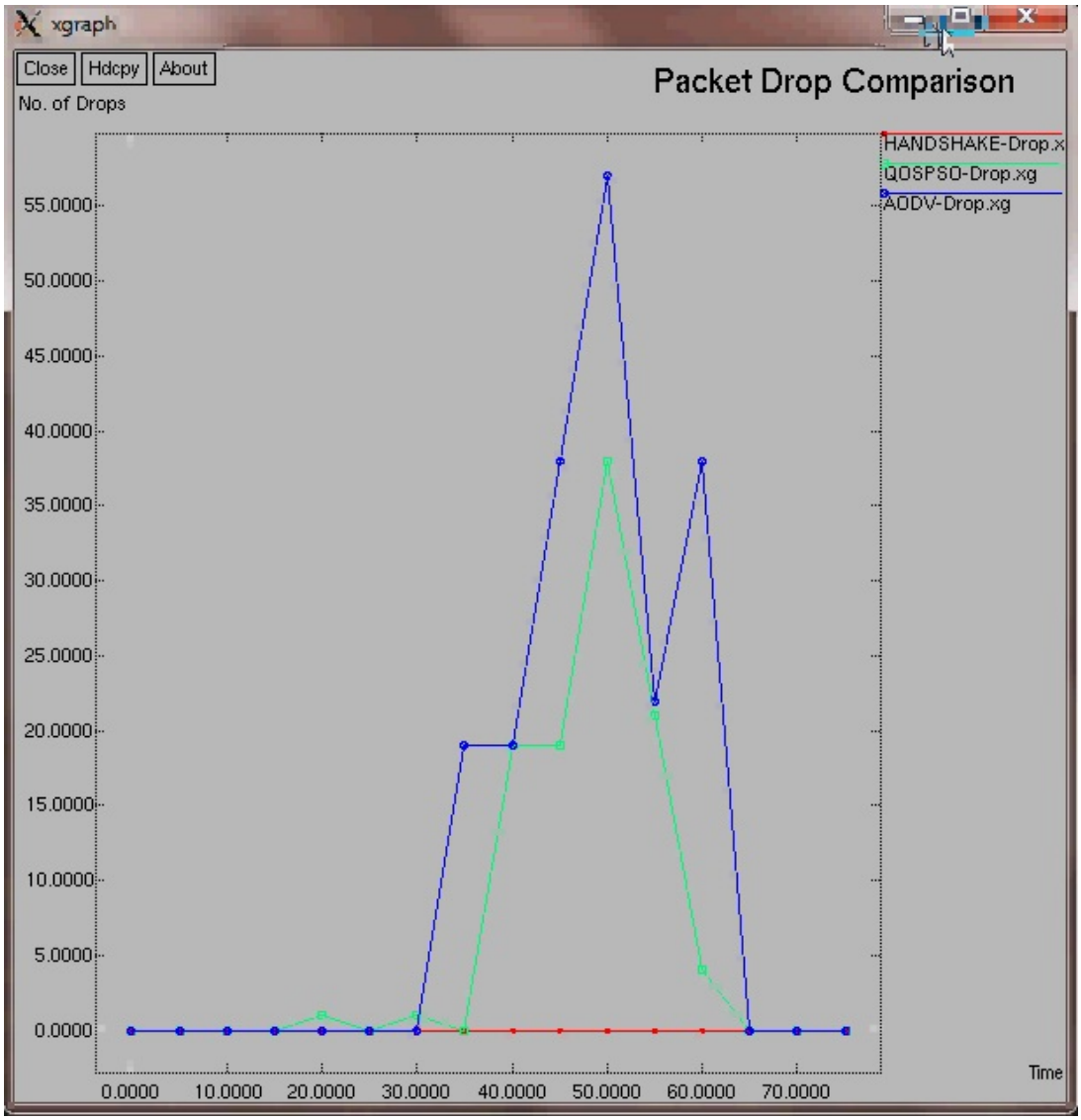


Figure 34. Packet drop comparison between Adel, AODV and QoS-Pso routing protocols.

Simulation Analysis of 50 Nodes Network - Average Delay

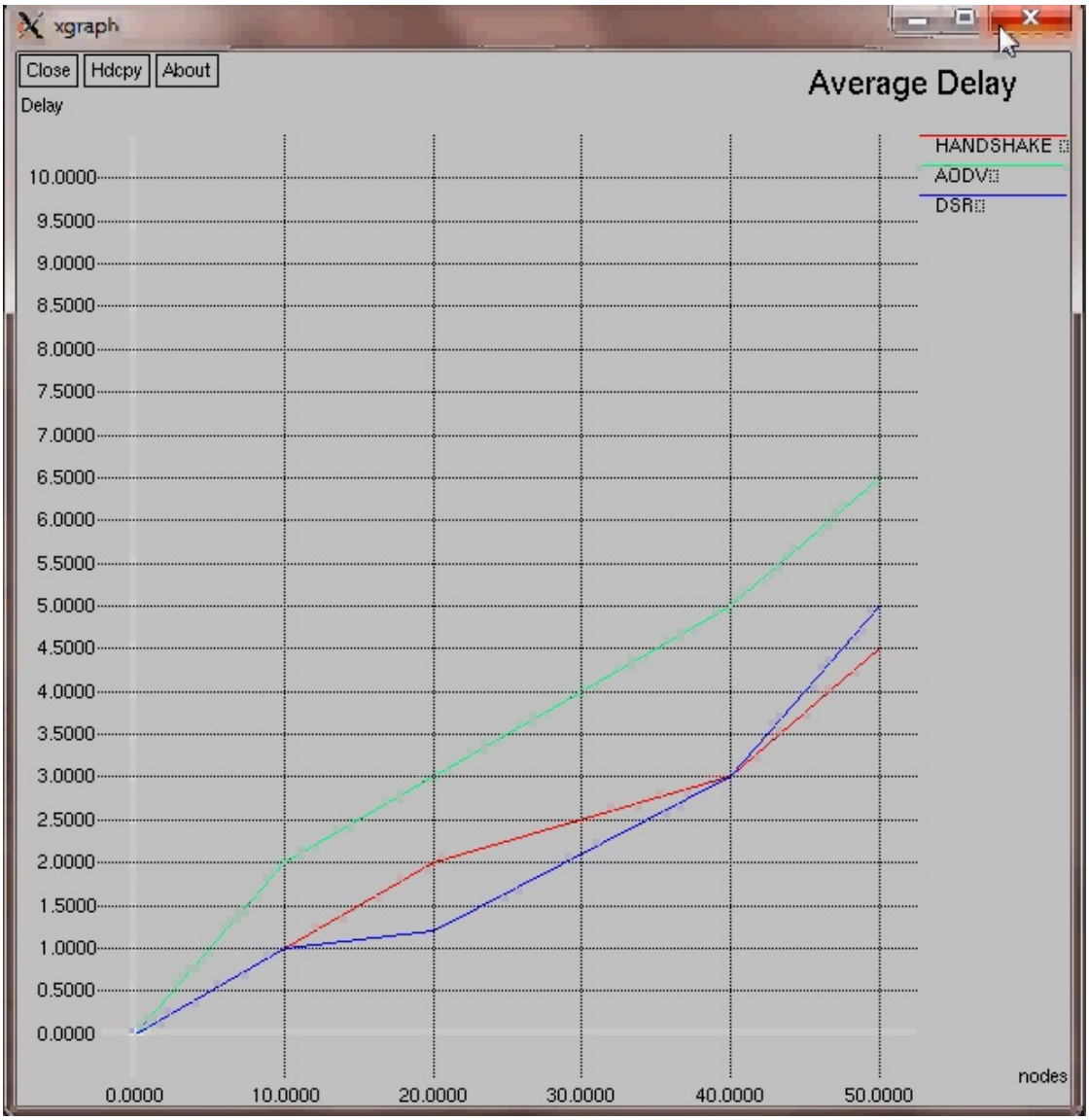


Figure 35. Average delay of 50 nodes.

Figure 32 shows a comparison between AODV, DSR and Adel routing protocol in subject of average delay, this analysis of WSN running Adel routing protocol using NS-2 network simulator, it runs average delay test which shows that Adel routing protocol has the least average delay among the other routing protocols.

Simulation Analysis of 50 Nodes Network - Energy Comparison

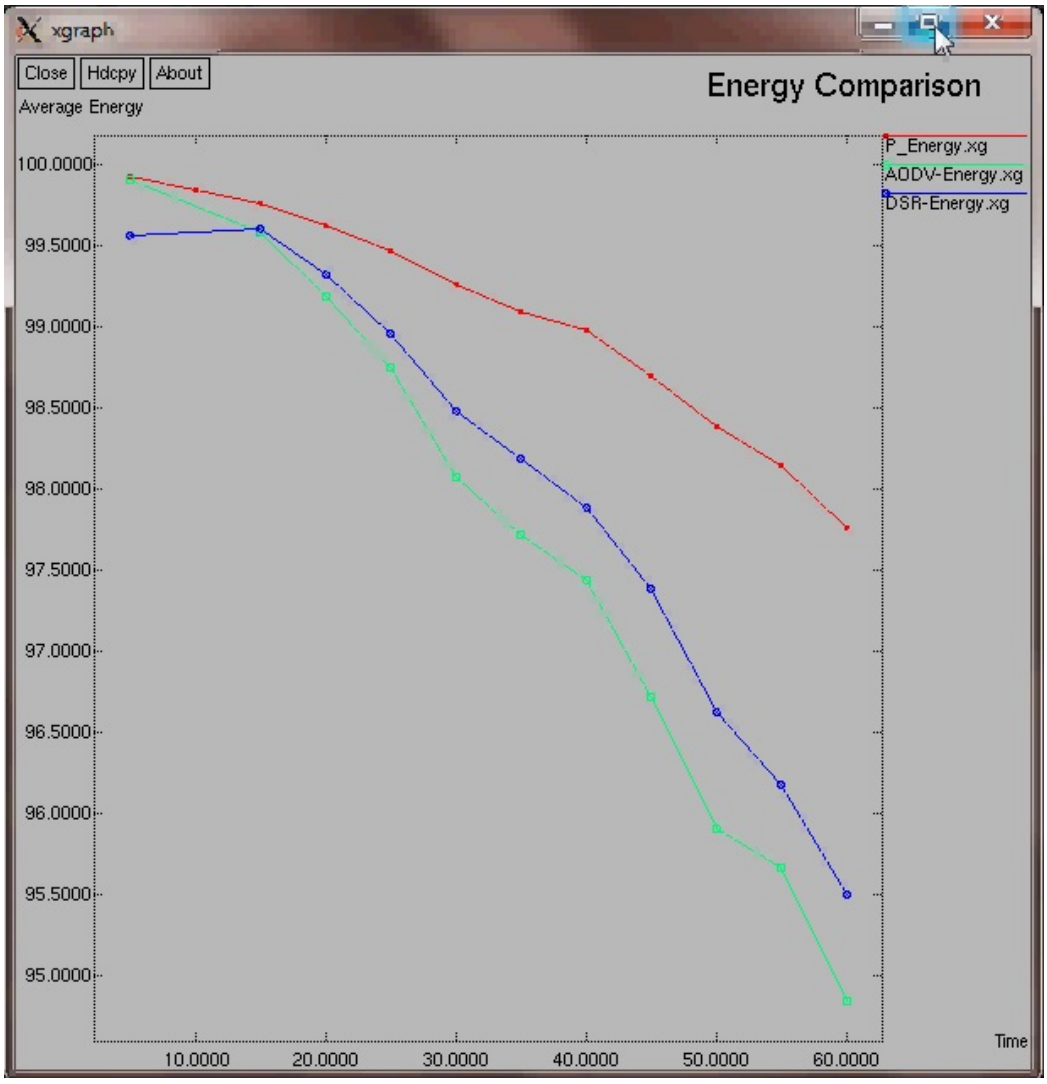


Figure 36. Result of Energy comparison on 50 nodes.

Figure 32 shows a comparison between AODV, DSR and Adel routing protocol in subject of energy consumption, this analysis of WSN running Adel routing protocol using NS-2 network simulator, as we have expected Adel routing protocol uses the highest amount of energy among the compared protocols during running time. Our main goal is to enhance security and connectivity level.

Simulation Analysis of 50 Nodes Network - Packet Delivery Ratio

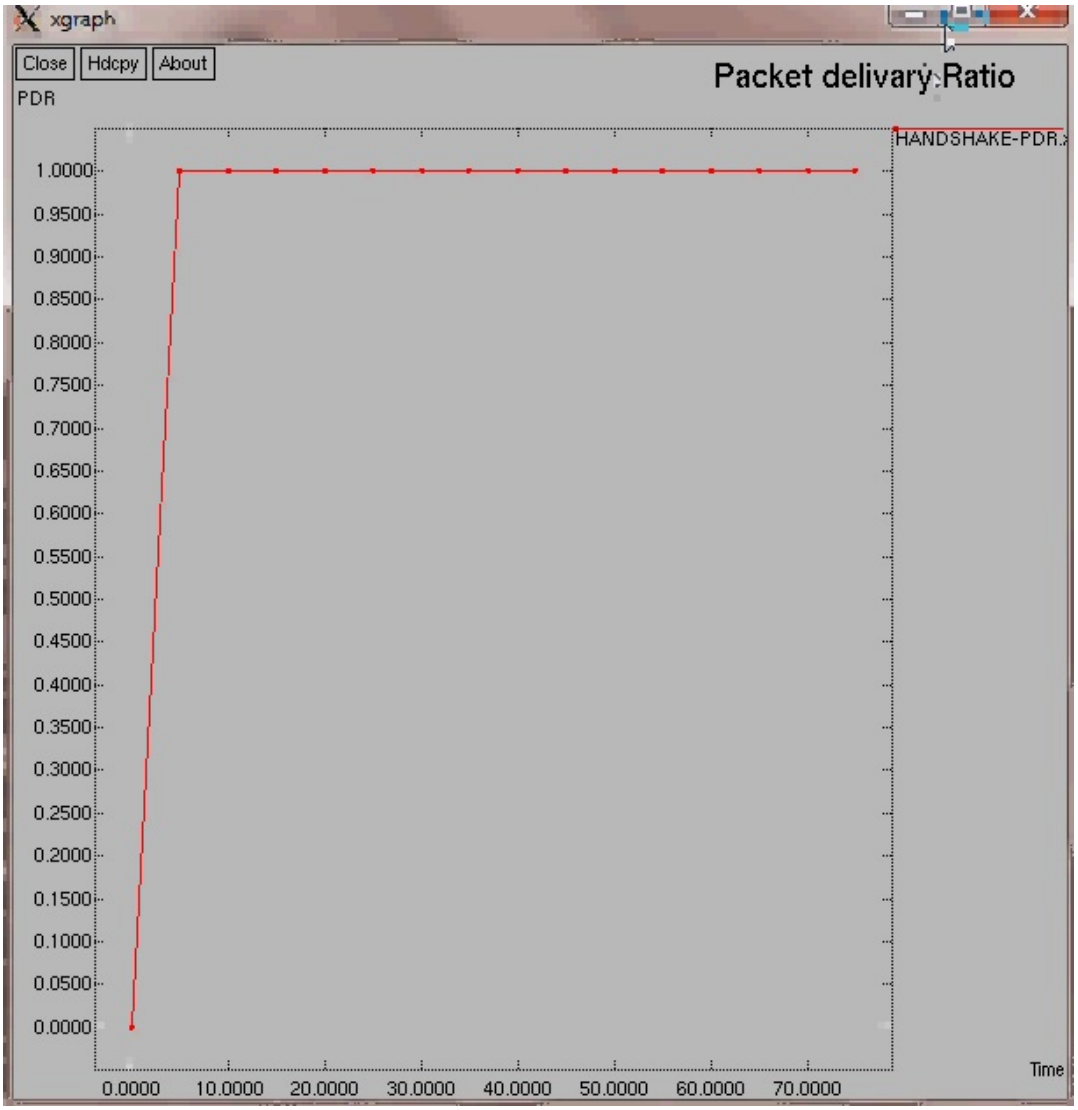


Figure 37. Result of Packet delivery ratio test on 50 nodes.

This packet drop test shows in Figure 37 and 38 that Adel routing protocol grantees packets delivery during running time while Quality of service particle swarm (QoS-Pso) protocol and to Ad hoc On-Demand Distance Vector does not always grantee packet delivery during the running time of this simulation.

Simulation Analysis of 50 Nodes Network - Packet Delivery Ratio Comparison

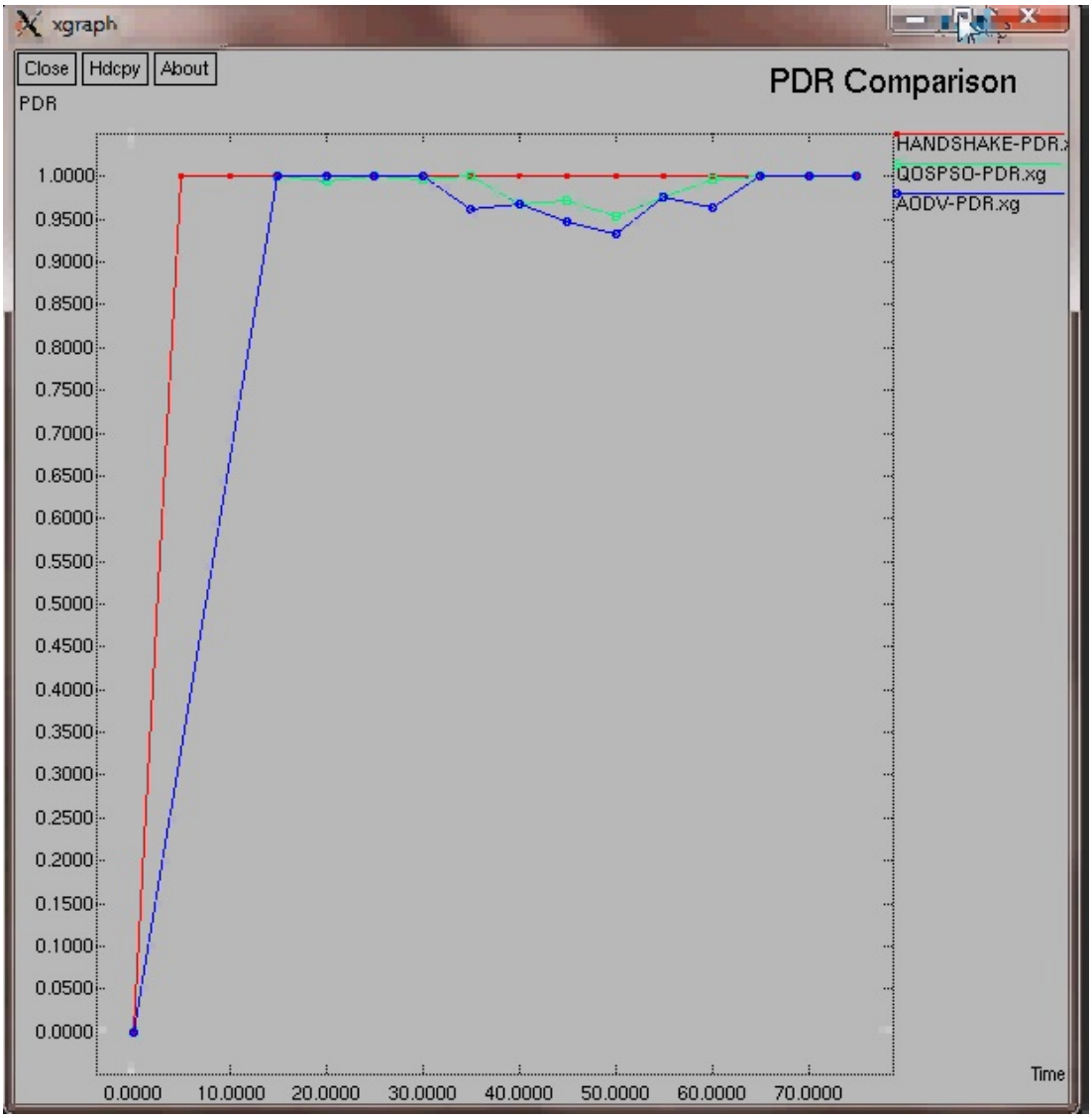


Figure 38. Packet delivery ratio comparison between Adel, AODV and QoS-Pso routing protocols.

Simulation Analysis of 50 Nodes Network - Throughput

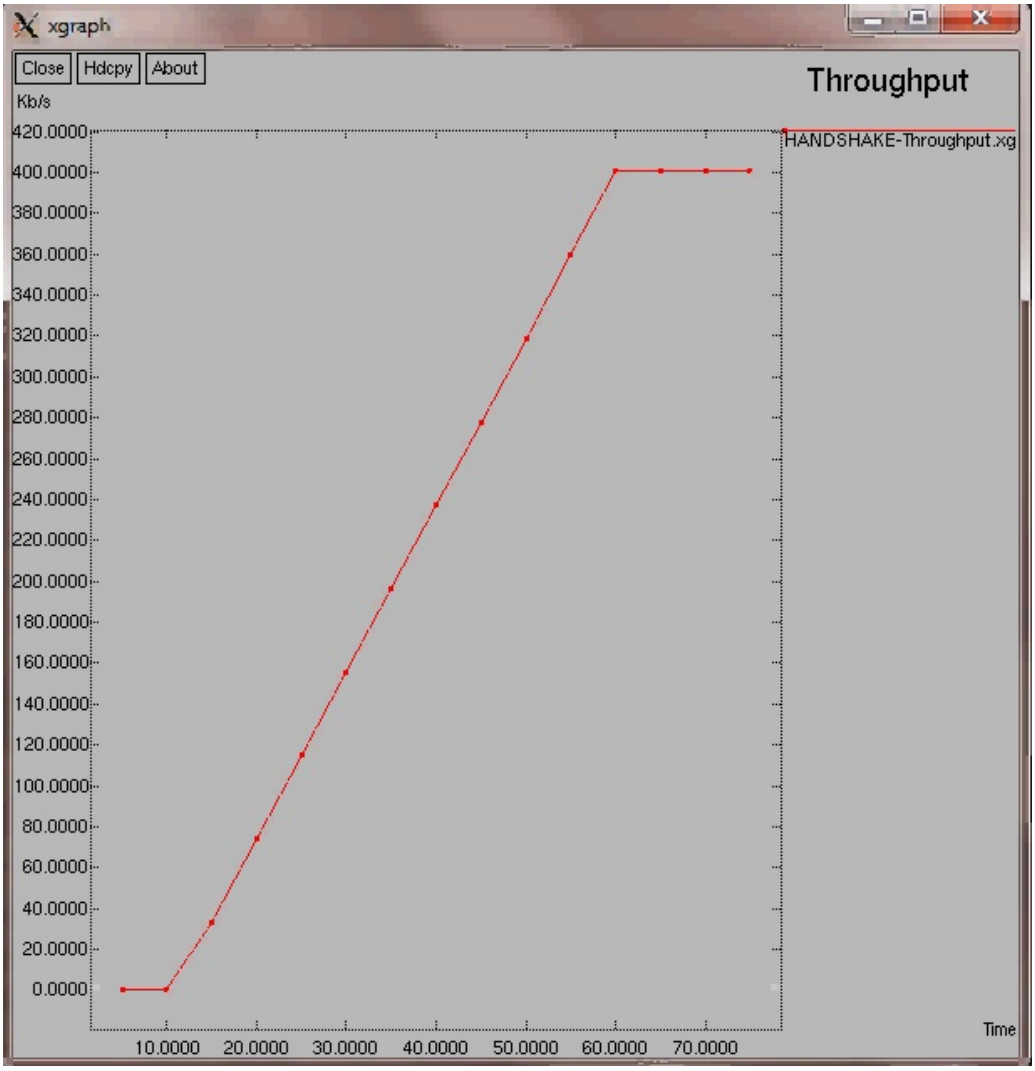


Figure 39. Result of Throughput test on 50 Nodes.

This Throughput test shows in Figure 39 and 40 that Adel routing protocol provides the highest amount of packets Kb/s during running time comparing to Quality of service particle swarm (QoS-Pso) protocol and to AODV protocol.

Simulation Analysis of 50 Nodes Network – Throughput Comparison

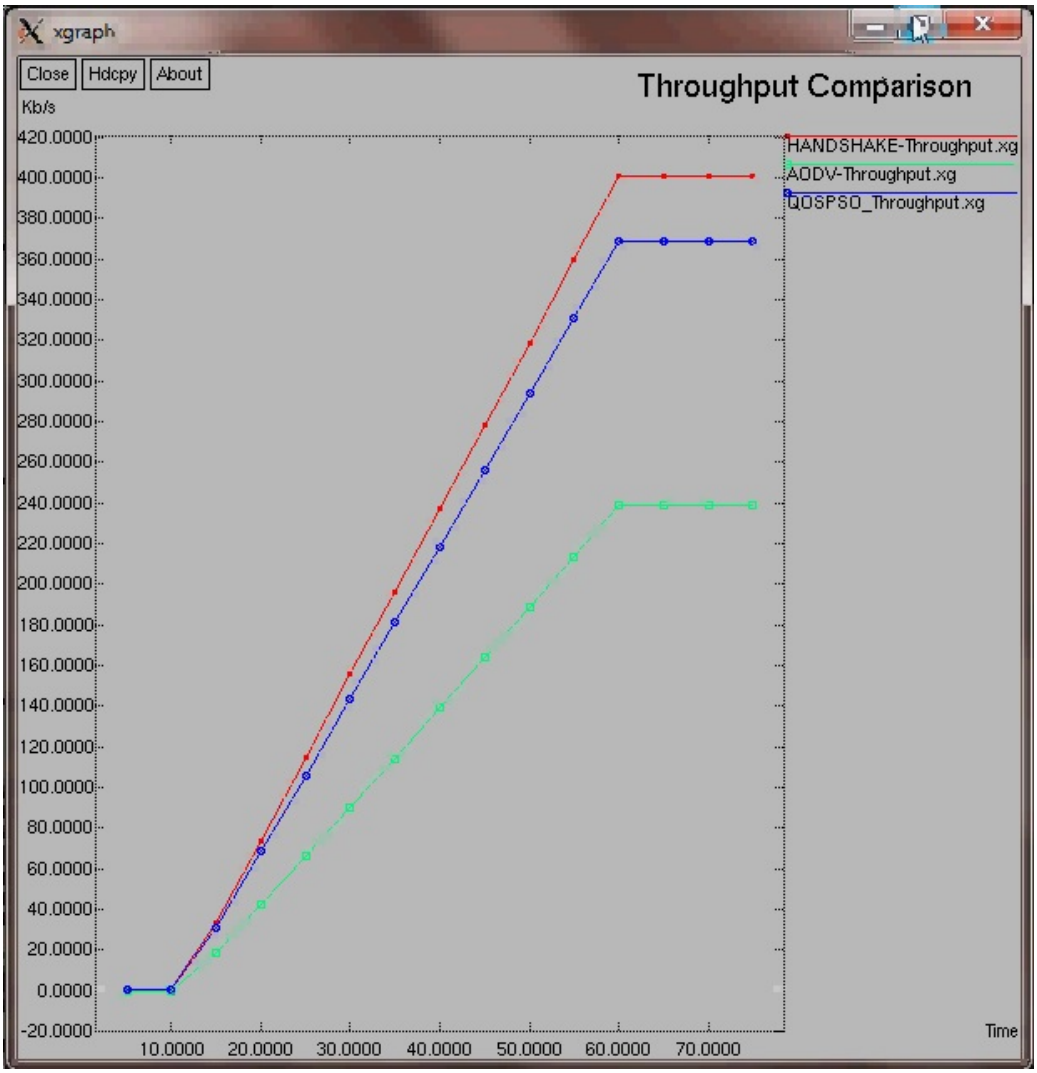


Figure 40. Throughput comparison between Adel, AODV and QoS-Pso routing protocols.

CHAPTER V

SUMMARY AND FUTURE WORK

This chapter summarizes the research of this dissertation and introduces some suggestions for future research.

Summary of Dissertation

The primary research objective was to study the security properties emerging from wireless sensor networks and routing protocols to develop simple mechanisms to enhance security for mesh topology WSNs, and to study secure routing techniques for communication in wireless sensor networks with respect to three important aspects: broadcast/multicast security, transmission connectivity, and public key distribution.

The wireless network model that has been considered during this research is based on the homogenous sensor networks model and on the mesh based topology. The network consists of at least two different types of nodes in terms of computational power: storage memory and lifetime. The more powerful nodes of the network act as base station in the network while less powerful nodes act as network members.

Chapter II provided overviews of WSNs and their classifications, requirements, security threats, and attacks. Also, it included an overview on few multicast routing protocols for WSNs and three of the basic cryptographic key algorithms:

- RSA public-key cryptosystem [29].
- Diffe-Hellman Key exchange [7].
- Elliptic curve cryptography algorithm [31].

Chapter III discussed related security protocols for exchanging data through WSNs and Chapter IV discussed the ANT colony algorithm which whose techniques I have adopted

in order to design the proposed protocol and the quality of service protocols in WSNs [58],[59],[60].

Chapter V discussed a secure routing protocol for transmission data in mesh wireless sensor networks, and Adel, the presented protocol, is a novel routing protocol for exchanging data through wireless sensor, the routing protocol which is a cycle path problem free in spite of the concave multipath in mesh networks. Adel enhances security level during data transmission between sender party and receiver party in wireless network environment. In a way such that, once the sensor nodes are placed in a network, they need to inform their location and their data related to the security for the further communication in the network. For that purpose, an efficient mechanism is implemented in order to perform better communication among sensor nodes.

Adel generates dynamic routing table using ACO algorithm with all the necessary information from network nodes after being deployed. Adel works with minimum routing restrictions and exploits the advantages of the three multicast routing styles, unicast, path, and mesh based. Since it takes a routing decision with a minimum number of nodes using the shortest path between the sender and the receiver nodes, Adel is applicable in static networks. Four essential performance metrics in mesh networks, network security analysis, network latency time, network packets drop, network delivery ratio, and network throughput are evaluated. Adel routing protocol has met the most important security requirements such as authorization, authentication, confidentiality, and integrity. It also guarantees the absence of the cycle path problem in the network. The presented routing algorithm works with minimum routing restrictions and exploits the advantages of the three multicast routing styles, unicast, path, and mesh based. Since it takes a routing decision with a minimum number of nodes using the shortest path between the

sender and the receiver nodes (benefiting of ANT colony algorithm), the presented routing algorithm is applicable in static networks. Four essential performance metrics in mesh networks, network security analysis, network latency time, network packets drop, network delivery ratio, and network throughput are evaluated.

This research reports the implementation and the evaluation of performance of Adel routing protocol using network simulator NS-2. The seven main parameters are considered for evaluation all experiments are security trust, packets drop, end to end delay, packet delivery ratio, energy consumption, and throughput. The results show that the proposed system can significantly enhance the network security and connectivity level compared to other routing protocols. Yet, as expected, it did not do so well in energy consumption since our main goal was to provide higher level of security and connectivity.

Future Work

Several issues related to the study of security of routing protocols in WSNs have been covered in this dissertation. Conversely, they are worthy of further study. They include:

- Extending this secure routing technique to heterogeneous mesh wireless sensor networks.
- Extending this routing technique to other network such as dynamic mesh wireless sensor networks.
- Applying this secure routing technique to mobile networks.
- Using another shortest path routing functions to determine the next node to which the message will be forwarded, (the proposed routing protocol

used ANT colony algorithm).

- Improving the proposed routing protocol to provide better energy consumption with the same level of network security and connectivity.

APPENDIX

NS-2 HELLO PACKET

This is a hello message routing technique during the handshake routing protocol stage written using AWK which is an interpreter programming language used under Linux operating system fedora.

```
begin {
i1=0
k1=0
c1=-1
fflg1=0
}
{
if(FILENAME1=="ntemp") {
stnd1=$1
ednd1=$2
tm1=$3
itval1=$4
mnd1=$5
}
if(FILENAME1=="Neighbor") {
if($1>=0&&$1<=100) {
n[i1,1]=$1
n[i1,2]=$2
```

```
i1++
}
}
}
END {
for(j1=0;j1<i1;j1++) {
if(c1!=n[j1,1]) {
src=n[j1,1]
c=n[j1,1]
t1=tm1
tm1=tm1+itval
}
print "set cbr"src"_"n[j1,2]" [attachs-CBR-traffics $node_("src") $sink("n[j1,2]") 64
0.05]" > "hello1.tcl"
print"$ns_ at "t" \"$cbr"src"_"n[j1,2]" start\"" > "hello.tcl"
print"$ns_ at "t+itval" \"$cbr"src"_"n[j1,2]" stop\"" > "hello1.tcl"
if(src!=49) {
print"$ns_ at "t" \"$node_("src") color green4\"" > "hello1.tcl"
print"$ns_ at "t1+itval" \"$node_("src") color green4\"" > "hello1.tcl" }
print ("$ns_ at "t+0.025" \"$ns_ trace-annotate
\\\"node_ - "src" send the hello messages WITH ITS PUBLICKEY to its neighbor -
"n[j1,2]"
\\\"\"") > "hello1.tcl"
```

```
t=t+0.001
}
}
BEGIN {
st=0
et=0
i=1
f=0
avg=0
d=0
drp=0
}
{
if(FILENAME=="tdly.tr") {
start=$1
end=$2
sender=$3
rec=$4
}
if(FILENAME=="qos.tr") {
if($3>=start && $3 <=end) {
if($1=="s" || $1=="r" || $1=="f" || $1=="d") {
if($31~sender && $33~rec) {
```

```
if($1=="d") { drp++ }
if($7>=0) {
sta=$41
}
else {
en=$41
}
val[i,1]=$3
val[i,2]=$41
print $3" "$41
i++
}
}
}
}
}
END {
for(j=1;j<i;j++) {
for(l=2;l<i-1;l++) {
if(val[j,2]==val[l,2]) {
d=val[j,1]
}
else {
```

```
break
}
}
}
avg=d-val[1,1]
print "\t"sender" \t"rec" \t\t"avg > "tmpdelay"
print "\t"sender" \t"rec" \t\t"drp > "tmpdrop"
}
```

REFERENCES

[1] "wireless sensor networks Research Group." http://www.sensor-networks.org/ , October 1 2015.

[2] M.Saraogi. Security in Wireless Sensor Networks: ACM SenSys, 2004.

[3] S. Sastry, Ahazia Sulthana and S Vagdevi. "Security Threats in Wireless Sensor Networks in Each Layer." *Int. J. Advanced Networking and Applications*,vol. 04, pp. 1657-1661, 2013.

[4] S. Patil, B P Kumar, S.Singha, and R. Jamil. "A Survey on Authentication Techniques for Wireless Sensor Networks." *International Journal of Applied Engineering Research*,Vol. 07, 2012.

[5] S.Ji, L. Huang and J. Wang. (2013). "A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network." *International Journal of Grid and Distributed Computing*, Vol. 6, No. 1, February. 2013.

[6] Sarhana Idrees. "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey." *International Journal of Current Engineering and Technology*, Vol. 03, 2013.

[7] Jean-Francois Raymond and Anton Stiglic. (November, 2014). Zeroknowledge Systems Inc, [online]. Avilabe: http://crypto.cs.mcgill.ca/~stiglic/Papers/dhfull.pdf

[8] P. Maidamwar and N. Chavhan. "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network*." International Journal on AdHoc Networking Systems (IJANS)*, vol. 02, 2012.

[9] J. Shukla and B. Kumari. "Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview." *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol. 02, 2013.

[10] M. Stehlik. "Intrusion detection and optimization in wireless sensor networks." Ph.D. thesis, Masaryk University, Faculty of Informatics, Czech Republic, 2013.

[11] C K. Marigowda1and M. Shingadi ."Security Vulnerability Issues in Wireless Sensor Networks: A Short Survey." *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 0, July 2013.

[12] Alazemi Rashid. "Defending WSNs against jamming attacks*," American Journal of Networks and Communications*, vol. 02, April, 2013.

[13] G. Gaubatz, J-P. Kaps and B Sunar. *Public key cryptography in sensor networks* – Revisited Book. Berlin, Publisher Springer Berlin Heidelberg, 2004.

[14] "Software and Hardware Solutions". Internet: www.certicom.com/index.php/the-basics-of-ecc, Certicom, a wholly owned subsidiary of BlackBerry Limited (NASDAQ: BBRY; TSX: BB), Founded in 1985.

[15]. Khan Ullah. "Key Management in Wireless Sensor Networks, IP-Based Sensor Networks, Content Centric Networks." Ph.D. Thesis, Polytechnic University of Turin Torino, Italy, 2013.

[16] R. Gupta and H Dhadhal. "Secure Multipath routing in Wireless Sensor Networks." *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, vol.02, March, 2013.

[17] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J. "*Security for Sensor Networks*." 2002 CA-DIP Research Symposium.

[18] C.H. Bhatt, H.H. Patel and B., Rathod3 Dushyantsinh. "A Survey on Cryptography and Key Distribution in Wireless Sensor Network with Security Attack and Challenges." *International Journal of Engineering Development and Research*,Vol. 01, 2009.

[19] L. Sichitiu, and, C. Veerarittiphan "*Simple, Accurate Time Synchronization for Wireless Sensor Networks*." Wireless Communicating and Networking, 2003.

[20] J. Walters, Z. Liang, W. Shi, and V. Chaudhary. "Wireless Sensor Network Security: A|Survey." In *Security in Distributed*, 2006.

[21] B. K Alese., E. D. Philemon and and S. Falaki "Comparative Analysis of Public-Key Encryption Schemes" *International Journal of Engineering and Technology*, vol. 02 2012.

[22] B. K. Alese, E. D. Philemon and S. O Falaki. "Comparative Analysis of Public-Key Encryption Schemes" *International Journal of Engineering and Technology*, vol. 02, 2012.
Available. http://ietjournals.org/archive/2012/sep_vol_2_no_9/1298141336454596.pdf

23. Dr.T.P.Saravanabava., Gandhi, M. Security in Wireless Sensor Networks Using Elliptic Curve Cryptography in Arm 9, vol. 02, 2013.

24. Netowrk Simulator. (1996), Internet: http://www-mash.berkeley.edu/ns, [Oct 25 2013]

[25] Mr. G. Ravi1, Mr. M. Mohamed Surputheen2 & Dr. R. Srinivasan. "Fast Energy Efficient Secure Dynamic Address Routing For Scalable WSNs." *International Journal of Computer Science*, vol. 09, March, 2012.

[26] Xiaobing He, Niedermeier, M., and De Meer, H. Dynamic Key Management in Wireless Sensor Networks: A Survey. *Journal of Network and Computer Applications*, 2013.
Avilabe. http://www.sciencedirect.com/science/article/pii/S1084804512002573

[27] Choudary Gorantla, M., Boyd, B., Manuel, J., and Nieto, G. "ID-based One-pass Authenticated Key Establishment" Proceeding AISC '08 Proceedings of the Sixth Australasian Conference on Information Security, 2008, Vol 81, PP. 39-46.

[28] R. Tahmasbi, H. Javadi, M. Shiri and A Allahyari. "Key Management in Heterogeneous Wireless Sensor Networks Using Voronoi Diagrams." *Advances in Computer Science: An International Journal*, vol. 02, 2013.
Available. http://acsij.org/publications/acsij-2013-volume-2-issue-1/key-management-in-heterogeneous-wireless-sensor-networks-using-voronoi-diagrams

[29] RSA in RSA laboratories website (September 2014).
Available. http://www.emc.com/emc-plus/rsa-labs/historical/rsa-algorithm.htm

[30] BBN Technologies. "Review on Security Issues and Attacks in Wireless Sensor Networks." *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 03, April, 2013.
Available. http://www.ijarcsse.com/

[31] X. Huang, P. Shah and D Sharma. "Fast Algorithm in ECC for Wireless Sensor Network." *Proceeding of the International Multiconfernce and Computer Scientist*, vol. II, March 2010.

[32] Gomathi K,M.C.A1, Senthilkumar T.P, A M.C. Phil M.. "A Study on Security Challenges in Wireless Sensor Networks: Key Management Approaches." *Proceeding International Journal of Computer Trends and Technology (IJCTT)*, 2013.
Available. http://ijcttjournal.org/archives/ijctt-v4i9p132

[33] M. Anand, E. Cronin, M. Sherr, Blaze, M, Z. Ives, and I Lee. "Sensor Network Security: More Interesting Than You Think. HotSec 06: 1st USENIX Workshop on Hot Topics in Security, 2006. Available.
http://libra.msra.cn/Publication/3730681/sensor-network- security-more-interesting-than-you-think

[34] M. Bhardwaj, M. Soni, and Kotary Kumar. (2012, Jan)"Comparative Analysis of Energy Efficient Routing Protocol for Wireless Sensor Network." *Special Issue of*

International Journal of Computer Applications (0975 – 8887) on Wireless Communication and Mobile Networks. [online]. No.14, Available. http://research.ijcaonline.org/wcmn/number1/wcmn1014.pdf1 [Oct 2013].

[35] C. Tzu-Chiang, C. Jia-Lin, T. Yue-Fu, and L. Sha-Pai. "Greedy Geographical Void Routing for Wireless Sensor Networks." *World Academy of Science, Engineering and Technology*. vol. 07, 2013.

[36] RSA in RSA laboratories website (Jan 2013). Available. http://www.emc.com/emc-plus/rsa-labs/historical/rsa-algorithm.htm

[37] Dr. A. Senthilkumar. "Energy Efficient Secure Multipath Routing Protocol for Wireless Sensor Networks." *International Journal of Engineering Research & Technology (IJERT)*, vol. 02, April. 2013.

[38] Kupwade Patil, H., J. Camp, and S. Szygenda. (2011). "Identity Based Authentication using a Cross Layer Design approach in Wireless Sensor Networks." *World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2011).* [online]. Available. http://lyle.smu.edu/~camp/pubs/WMSCI_2011.pdf

[39 Y. Zhang, W. Lou†, and Y. Fang. "Securing Sensor Networks with Location-Based Keys." *In Porc of IEEE Wireless Communications and Networking Conference (WCNC).* 2005, pp. 1909-1914.

[40] A. Al-Mahmud. "Secure Sensor Node Authentication in Wireless Sensor Networks." *International Journal of Computer Applications*, vol. 46, pp. 0975-8887, May, 2012.

[41] K.Fall and K.Varadhan. (May, 2010). The ns Manual, the VINT Project.

[42] Sandeep. Kumar and Trilok. Shrimal. "Performance Evaluation of Different Routing Protocols in Wireless Sensor Network Using Different Network Parameters for Small Terrain Area." *International Journal of Modern Electronics and Communication Engineering (IJMECE),* vo1.1, March. 2013.

[43] Teerawat. Issariyakul and Ekram. Hossain. (2009). *Introduction to Network Simulator NS2.* (Kindle edition). [Online]. Avalible. file:///C:/Users/nooh/Downloads/Introduction%20to%20Network%20Simulator%20NS2.pdf [September 22, 2012].

[44] L.Alazzawi and A. Elkateeb. "Performance Evaluation of the WSN Routing Protocols Scalability." *Journal of Computer Systems, Networks, and Communications,* vol. 2008, December.2008.

[45] W. Heinzelman, J. Kulik, and H. Balakrishnan. "AdaptiveProtocols for Information Dissemination in WirelessSensor Networks." *Proceeding MobiCom '99 Proceedings*

of the 5th annual ACM/IEEE international conference on Mobile computing and networking, 1999, pp. 174-185.

[46] X. Renyi and W. Guozheng. "A survey on routing in wireless sensor networks." *Progress in Natural Science*, vol. 17, 2007, pp. 261–269.

[47] T. Nishitha and Reddy Chenna. "Bio-Inspired Routing In Ad Hoc Networks." *Journal of Engineering, Computers & Applied Sciences (JEC&AS)*, vol. 01, No.1, October, 2012.

[48] C. Eyckelhof and M. Snoek. Ant Systems for a Dynamic TSP --- Ants Caught in Traffic Jam. In Lecture Notes in Computer Science. (Vol. 2463/2002, PP 88-99).

[49] C.Jin, and Van Dijk, (March, 2015). *Secure and Efficient Initialization and Authentication Protocols for SHIELD*. (Electronic edition). [On-line]. Available. https://eprint.iacr.org/2015/210 [May, 2013].

[50] P. Chahal, P. Tak, and A. Tomar. "Comparative Analysis of Various Attacks on MANET" *International Journal of Computer Applications*. vol 111, February. 2015.

[51] RSA in RSA laboratories website (May 2014). Available. http://www.emc.com/emc-plus/rsa-labs/historical/rsa-algorithm.htm

[52] A. Arya1, J. Singh. "Comparative Study of AODV, DSDV and DSR Routing Protocols in Wireless Sensor Network Using NS-2 Simulator." *International Journal of Computer Science and Information Technologies*. vol. 05, 2014.

[53] T. Farid and A. Prahladachar. "Secure Routing With AODV Protocol For Mobile Ad Hoc Networks." Department of Computer Science, University Of Windsor, Technical Report. 2006.

[54] Y. Pan. "Design Routing Protocol Performance Comparison in NS2: AODV Comparing to DSR as Example." Department of Computer Science, State University of New York at Binghamton, New York. 2007.

[55] S. Shah, et al (2008). "Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation," Proceeding of the National Conference on Mobile and pervasive Computing (CoMPC). Chennai, India.

[56] A. Tuteja. "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET Using NS2." *M. M. Univ, Mullana, India. Advances in Computer Engineering (ACE), International Conference, IEEE*, 2010.

[57] T. Basavaraju, S. Sarkar, and C. Puttamadappa, "Impact of MAC Layer on the Performance of Routing Protocols in Mobile Ad hoc Networks." *World Academy of*

Science, Engineering and Technology International Journal of Electrical, Computer, Electronics andCommunication Engineering. vol. 01, 2007.

[58] P. Trakadas, H. Leligou, T. Zahariadis, P. Karkazis, and L. Sarakis. "Managing QoS for Future Internet Applications over Virtual Sensor Networks," *The Future Internet, Lecture Notes in Computer Science*. vol. 7858, pp. 52-63, 2013.

[59] Ehsan, S., and Hamdaoui, B. "A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks." *Communications Surveys & Tutorials, IEEE.* vol. 14, 2012.

[60] E. Tong, W. Niu, G. Li, D. Tang, L. Chang, Z. Shi, and S. Ci. "Bloom filter-based Workflow Management to Enable Qos Guarantee in Wireless Sensor Networks." *Journal of Network and Computer Applications*. pp. 39 is between 38–51, 2014.

[61] B. Othman, L. Mokdad, and B. Yahya. "An Energy Efficient Priority Based QoS MAC Protocol for Wireless Sensor Networks." *IEEE International Conference on Communications (ICC)*. 2011.

[62] R, Sumathi. M.G. Srinivas "A Survey of QoS Based Routing Protocols for Wireless Sensor Networks." *In Journal of Information Processing Systems. vol.* 08, December. 2012.

[63] S.R. Heikalabad, H.Rasouli, F.Nematy, and N.Rahman. "QEMPAR: Qos and Energy Aware Multi-Path Routing Algorithm for the Real-Time Applications in Wireless Sensor Networks." *In International Journal of Computer Science Issues*. vol. 08, January. 2011.

[64] Nandgave Sunita. "A Survey on QOS and Energy Efficient Routing Protocols in WSN." *In International Journal of Application or Innovation in Engineering and Management (IJAIEM).* vol. 01, October. 2012.

[65] D. Verma, A. Kaur. "Performance Comparison of QoS Based Routing Protocols MBRR, REAR and SPEED for Wireless Sensor Networks." *in International Journal of Research in Engineering and Technology.* vol. 07, September. 2013.

[66] P. Lambrou and G. Pamayiotou. "Collaborative Area Monitoring Using Wireless Sensor Networks with Stationary and Mobile Nodes." *Department of Electrical and Computer Engineering, University of Cyprus*. vol. 2009, March. 2009.

[67] V. Ramesh, Dr. P. Subbaiah, N. Koteswar Rao and M. Janardhana Raju, "Performance comparison and analysis of DSDV and AODV for MANET," *International Journal on Computer Science and Engineering*. vol. 02, 2010.

[68] K. Jogendra. “Performance Analysis and Simulation of OLSR Routing Protocol in MANET.” International journal of Computer Networking and Communication. vol. 1, August. 2013.

[69] Harald H.-J. Bongartz, Tobias Ginzler, Thomas Bachran, *SEAMAN: A Security-Enabled Anonymous MANET Protocol*, NATO Consultation, 2008.

[70] Mohammad Matin. *Wireless Sensor Networks-Technology and Protocols*. INTECH. September. 2012.

[71] Johannes B¨ock. “RSA-PSS – Provable secure RSA Signatures and their Implementation.” http://rsapss.hboeck.de/, May 4 2011 [July 2014].

[72] Mr. G. Ravi , Mr. M. Mohamed Surputheen & Dr. R. Srinivasan. (2012, march). “Fast Energy-Efficient Secure Dynamic Address Routing For Scalable WSNs.” IJCSI International Journal of Computer Science Issues. [online]. Vol. 9, Issue 2, No 1. Avalibale at http://ijcsi.org/papers/IJCSI-9-2-1-383-387.pdf [March 2012].