PERFORMANCE ANALYSIS OF SPIN PROTOCOL UNDER DIFFERENT SECURITY THREATS IN WIRELESS SENSOR NETWORKS

Dissertation submitted to the Central University of Punjab

For the award of

Master of Technology

In

Computer Science and Technology

BY

Rohit Choudhary

Supervisor

Er. Amanpreet Kaur

Centre for Computer Science and Technology

School of Engineering and Technology

Central University of Punjab, Bathinda

September, 2014

DECLARATION

I declare that the dissertation entitled “PERFORMANCE ANALYSIS OF SPIN PROTOCOL UNDER DIFFERENT SECURITY THREATS IN WIRELESS SENSOR NETWORKS” has been prepared by me under the guidance of Er. Amanpreet Kaur, Assistant Professor, Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab. No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

Name: Rohit Choudhary
Centre for Computer Science and Technology,
School of Engineering and Technology,
Central University of Punjab,
Bathinda – 151001.

Date:

CERTIFICATE

I certify that ROHIT CHOUDHARY has prepared his dissertation entitled "PERFORMANCE ANALYSIS OF SPIN PROTOCOL UNDER DIFFERENT SECURITY THREATS IN WIRELESS SENSOR NETWORKS", for the award of M.Tech degree of the Central University of Punjab, under my guidance. He has carried out this work at the Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

Er. Amanpreet Kaur
Assistant Professor
Centre for Computer Science and Technology,
School of Engineering and Technology,
Central University of Punjab,
Bathinda – 151001.

Date:

ABSTRACT

Performance Analysis of SPIN Protocol under Different Security Threats in Wireless Sensor Networks

Name of Student:	ROHIT CHOUDHARY
Registration Number:	CUPB/M.Tech/SET/CST/2012-13/16
Degree for which submitted:	M.Tech
Name of Supervisor:	Er. Amanpreet Kaur
Name of centre:	Centre for Computer Science and Technology
Name of School:	School of Engineering and Technology

Key words:	SPIN, E-SPIN, AES-SPIN, Energy, Security, Sybil Attack, Wormhole Attack.

The wireless sensor network consists of homogenous sensor nodes with limited energy and computational power which are self organisable. These nodes use radio frequency channels to communicate with each other wirelessly. Besides that wireless sensor networks are resource constrained with low energy and low bandwidth along with shorter communication range. The evolution of VLSI circuit technology has also enabled the development of wireless sensor networks. The ease of deployment and low cost availability of sensor devices has attracted much advancement in wireless sensor networks. The nodes with capabilities of sensing and computing help the administrator to observe particular environment like battle field, climatic conditions and weather forecasting in remote areas etc. This dissertation research is about the study of performance challenges in wireless sensor networks using Sensor Protocol for Information via Negotiation(SPIN) protocol under various security threats and to analyse their impact on SPIN. The empirical study has been carried to validate the issues studied in literature review by simulating the scenarios. On the basis of achieved observations the inference is drawn about the better protocol in sensor network and future recommendations are made for the analysis and enhancement.

Rohit Choudhary Er. Amanpreet Kaur

DEDICATED TO
MY LOVING PARENTS

ACKNOWLEDGEMENTS

“The successful completion of any task would be incomplete without accomplishing the people who made it all possible and whose constant guidance and encouragement secured us the success.”

On the submission of my thesis on “PERFORMANCE ANALYSIS OF SPIN PROTOCOL UNDER DIFFERENT SECURITY THREATS IN WIRELESS SENSOR NETWORKS”, I would like to extend my gratitude and sincere thanks to my respected guide Er. Amanpreet Kaur, Assistant Professor, Centre for Computer Science & Technology, Central University of Punjab, Bathinda, for her constant motivation and support during the course of my work. I truly appreciate and value her esteemed guidance and encouragement from the beginning to the end of this research work. I am indebted to her for having helped me shape the problem and providing insights towards the solution.

I would also like to thank Dr. A. K. Jain, Dean, School of Engineering & Technology, for his valuable suggestions in the course of my research work. I wish to thank all the faculty members of Central University of Punjab, Bathinda for their invaluable knowledge they have imparted to me in most exciting and enjoyable way. I am grateful for their constant support and help.

Rohit Choudhary

CUPB/M.Tech/SET/CST/2012-13/16

Centre for Computer Science & Technology

School of Engineering and Technology

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Sr. No.	Full Form	Abbreviation
1.	Abstract Window Toolkit	AWK
2.	Advanced Encryption standard	AES
3.	Advertisement	ADV
4.	Constant Bit Rate	CBR
5.	Data centric RoUtinG protocol	DRUG
6.	Energy Enhanced Modified-Sensor Protocol for Information via Negotiation	EEM-SPIN
7.	Global Positioning System	GPS
8.	Hyper Text Transfer Protocol	HTTP
9.	Kilo Bytes Per Second	KBPS
10.	Link Layer	LL
11.	Local Area Network	LAN
12.	Long Term Support	LTS
13.	Message Authentication Code	MAC
14.	Modified- Sensor Protocol for Information via Negotiation	M-SPIN
15.	Network Simulator version 2	NS2
16.	Object Oriented Toolkit Command Language	OTcl
17.	Packet delivery ratio	Pdr
18.	Quality of Service	QoS
19.	Request	REQ
20.	Secure- Sensor Protocol for Information via Negotiation	S-SPIN
21.	Sensor Protocol for Information via Negotiation	SPIN
22.	Sensor Protocol for Information via Negotiation- Image Transfer	SPIN-IT
23.	Sensor Protocol for Information via Negotiation version- 1	SPIN-1
24.	Sensor Protocol for Information via Negotiation version- 2	SPIN-2

25.	Sensor Protocol for Information via Negotiation-Broadcast	SPIN-BC
26.	Sensor Protocol for Information via Negotiation-Energy conserving	SPIN-EC
27.	Sensor Protocol for Information via Negotiation-Gossiping	SPIN-G
28.	Sensor Protocol for Information via Negotiation-Improved	SPIN-I
29.	Sensor Protocol for Information via Negotiation-Point to point	SPIN-PP
30.	Sensor Protocol for Information via Negotiation-Reliable version	SPIN-RL
31.	Shortest Path minded- Sensor Protocol for Information via Negotiation	SPMSPIN
32.	Shortest Path minded- Sensor Protocol for Information via Negotiation- Reduced energy consumption	SPMS-Rec
33.	Toolkit Command Language	TCL
34.	Transmission Control Protocol	TCP
35.	User Datagram Protocol	UDP
36.	Variable Bit rate	VBR
37.	Wireless Sensor Networks	WSN
38.	Exclusive OR	XOR

CHAPTER 1

INTRODUCTION

Wireless Sensor Network (WSN) consists of hundreds or thousands of self organizing, low-power, low cost wireless device called nodes which can be used in a variety of applications such as military sensing and tracking, environmental monitoring, disaster management, etc (Li et.al., 2010). The characteristics of wireless sensor networks are that they have low data rate and have wireless medium. The other characteristics includes that they are self configurable, self-organised and are infrastructure less. But the main issues arise when these sensor nodes are deployed in open, un-monitored, hostile environment, sensor nodes will be exposed to the risk of being captured by an active adversary. So with the demanding constraint of nodes with limited energy and computational power, the key issue for Wireless Sensor Networks (WSN) is designing a feasible security mechanism that can ensure at least authenticity, integrity or confidentiality (application specific) to prevent the malicious attacks on the sensor networks.

Wireless sensor network are expected to be widely deployed in the near future because of their ability to monitor the physical environment from remote locations. Wireless sensor network increases the accuracy of the gathered information by providing the distributed processing of information collected by the sensor nodes (Kulik et.al., 2002).

1.1 Wireless Sensor Network Model

The major difference between WSN and ad-hoc networks lies in the fact that WSNs are resource limited, their deployment is dense, they may subject to failures, the number of nodes in WSNs is much higher than that of ad hoc networks, the network topology is constantly changing (dynamic), WSNs use broadcast communication mediums and finally sensor nodes don’t have a global identification tags (Das et.al., 2012). The major components of a typical sensor network are shown in figure 1.1.

- **Sensing Field**: A sensor field can be considered as the area in which the nodes are placed or deployed.
- **Sensor Nodes**: Sensors nodes are responsible for sensing and collecting data and routing this information back to the sink.
- **Sink**: A sink is responsible for receiving, processing and storing data from the other sensor nodes from sensing field. They have to reduce the total number of packets that need to be sent, hence reduces the overall energy requirements of the network. The network usually assigns such points dynamically (Das et.al., 2012).Regular nodes can also be treated as sinks if they delay outgoing messages until they have aggregated the required sensed information. Sinks are also known as data aggregation points.

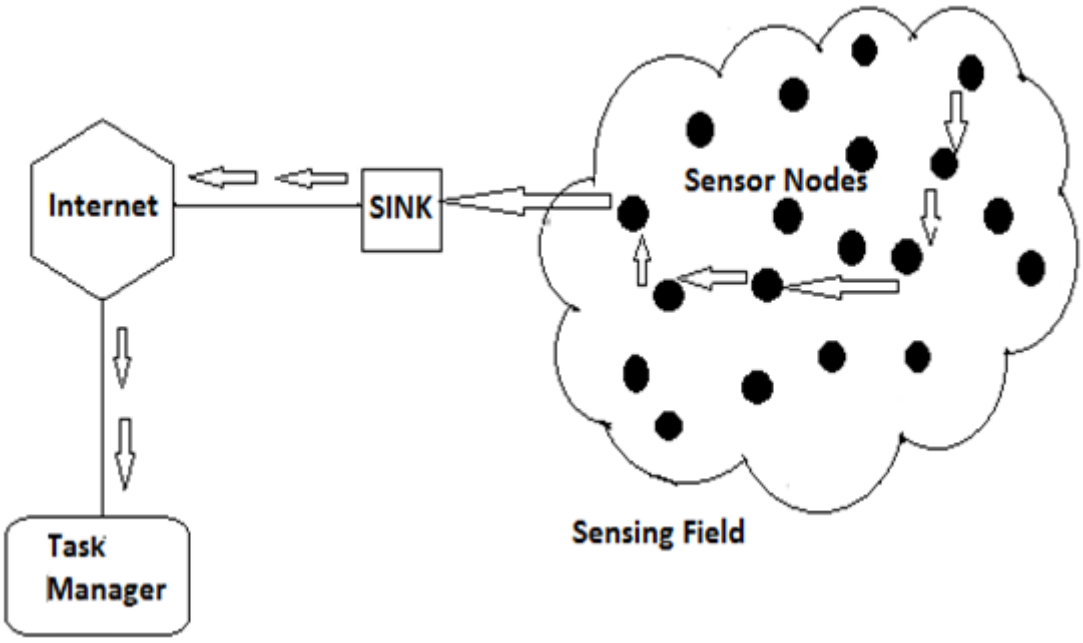

Figure1.1 .Components of Wireless Sensor Networks

- **Task Manager**: The task manager (generally base station) is a centralized point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface (Das et.al., 2012).The base station could be a laptop or a workstation having sufficient energy source. Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So several

hundred nodes are deployed throughout a sensor field to create a wireless multi-hop network with infrared, radio, optical media or bluetooth as their medium of communications.

1.2 Classification of Routing Protocols in WSN

Routing is a process of efficiently determining a path between source and destination upon request of data transmission. In WSNs the network layer is mostly used to implement the routing of the incoming data. It is common in multi-hop networks that the source node cannot reach the sink directly, so intermediate sensor nodes have to relay their packets (Al-Karaki & Kamal, 2004). In order to pass on (or relay) the packets correctly and efficiently the routing algorithm uses routing tables. Routing table contains the list of node option for any given packet's destination. Moreover the routing algorithm is responsible for constructing and maintaining routing table with the help of routing protocol.

Routing protocols in WSNs can be classified depending on the application (Protocol-Operation-based) and network architecture (Network-Structure-based) as shown in Figure 1.2. Based on the underlying network there are three protocol categories (Al-Karaki & Kamal, 2004):

- **Flat-Based Routing**: In Flat-based routing every node plays the same role as sensor nodes. The numbers of sensor nodes are relatively very large, so this leads to the data-centric approach in which the base station sends a query to nodes in its proximity and waits for their response.
- **Hierarchical-Based (Cluster-based) Routing**: This type of routing is used in energy efficient communication and scalable networks. It is also known as cluster-based routing. In this routing the nodes with high energy are assigned the task of processing and sending the data while the low energy nodes are given the task of sensing the region and information to their respective cluster heads (Al-Karaki & Kamal, 2004). This feature has significant effect on scalability, lifetime of network and energy minimization of the network.
- **Location-Based**: In this the sensor nodes are scattered in their area of interest and they are located by means of their geographic locations by means of Global Positioning System (GPS). The distance between any two neighbouring nodes is estimated on the basis of incoming signal strengths received from them and

relative locations of neighbouring nodes can be obtained by exchanging such information between neighbours or by communicating with a satellite using GPS. To save energy, some location-based schemes put the nodes to sleep state if there is no activity.

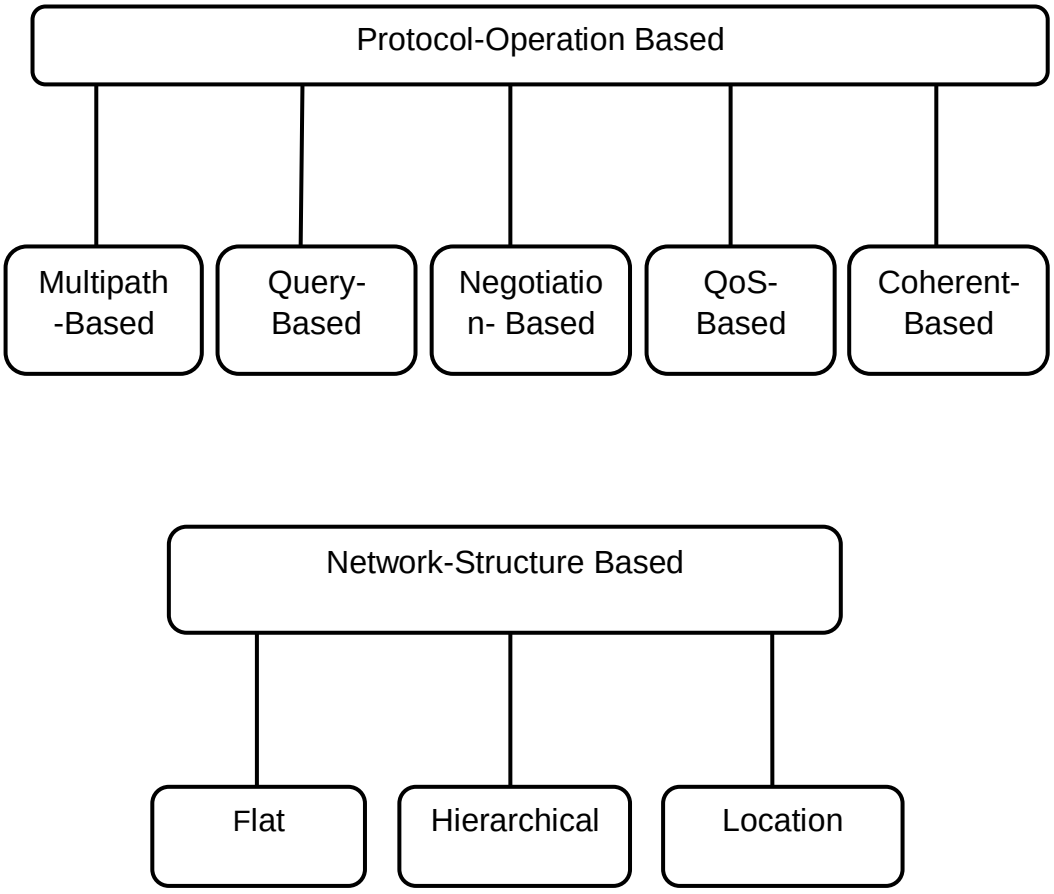

Figure 1.2 Classifications of Protocols

Depending on the protocol operation we can divide routing protocols in categories shown in fig 1.2 (Al-Karaki & Kamal, 2004):

- **Multipath-Based**: In this approach the multiple paths are used rather than a single path in order to decrease delay and increase network performance. For example the multiple paths are created between source and destination to increase fault tolerance at the expense of increase energy consumption.
- **Query-Based**: The destination nodes propagate a query for data from a node through the network, a node with this data sends the data that matches the query back to the node that initiated it.

- **Negotiation-Based**: Use negotiation in order to eliminate redundant data transmissions. Communication decisions are also made based on the resources available.
- **QoS-Based**: In this the network uses the balanced approach to achieve QoS. The data is delivered in such a way that network balances between energy consumption and data quality through certain QoS metrics as delay, energy or bandwidth.
- **Coherent-Based**: In this the Node performs low data processing (suppression, time-stamping) on the nodes in coherent-based (minimum processing) and non-coherent (full processing) routing protocols.

1.3 Applications of Wireless Sensor Networks

As discussed in (Mangla & Arora, 2013) and (Bhuniya et.al., 2014) wireless sensor networks have a variety of applications as follows:

1.3.1 Area monitoring

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. For example military use of sensors is to detect enemy intrusion.

1.3.2 Earth Monitoring

The term Environmental Sensor Networks, has evolved to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests, etc.

1.3.3 Air Pollution Monitoring

Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take benefit of the ad-hoc wireless links rather than the wired installations, which also make them more dynamic for testing readings in different areas.

1.3.4 Forest Fire Detection

A network of Sensor Nodes can be installed in a forest to detect fire. The sensor nodes can be used to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection of fire is crucial for a successful action of the fire-fighters.

1.3.5 Natural Disaster Prevention

Wireless sensor networks can act effectively to prevent the consequences of natural disasters, like floods. Wireless sensor nodes can be deployed in rivers where changes of the water levels have to be monitored in real time.

1.3.6 Health Care Applications

Wireless sensor network also has its application in health care systems. A wireless sensor can be used to monitor cognitive disorders in a controlled manner at different stages. Sensor can also be implanted in to human beings to support a function that requires human to communicate wirelessly with computers which uses advanced processing.

1.3.7 Military Application

Wireless sensor networks can also be used in military applications to detect the enemy tanks in battle field. A sensor can be deployed in a battle field which sends information about the enemy tanks positions at regular intervals.

1.4 Sensor Protocol for Information via Negotiation (SPIN) Protocol

SPIN is a negotiation based protocol used to efficiently disseminate information in a wireless sensor network. Earlier data dissemination approaches like flooding and gossiping wastes the communication and energy resources by sending duplicate information throughout the network. Moreover, these protocols were not resource-adaptive. SPIN solved these shortcomings of conventional approaches using meta data negotiation and resource-adaptive algorithms. Nodes deploying SPIN algorithm assigns a high-level descriptor to their data, called meta-data, and performs meta-data negotiations before any data transmission is done. This ensures that there is no redundant data is sent in the network. In addition,

SPIN has access to the current energy level of the node and adapts the protocol it is running based on how much energy is available with the node. SPIN is more energy-efficient than flooding or gossiping algorithms and disseminate data at the same rate or faster than either of these protocols (Heinzelman et.al.,2000).

SPIN is among the early work to pursue a data-centric routing approach. The philosophy behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement. Each node upon receiving new data, advertises it to its neighbours, i.e. those who do not have the data, retrieve the data by sending a request message. SPINs meta-data negotiation solved the classic problems of flooding such as transmission of redundant data, overlapping of sensing areas and resource blindness and provides a lot of energy efficiency. There is no standard meta-data format and it is believed to be application specific, e.g. using an application level framing. There are three messages in SPIN to exchange data between nodes. These includes : ADV message to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual data. One of the advantages of SPIN is that topological changes are localized since each node needs to know only its single-hop neighbours (Heinzelman et.al., 1999).

The SPIN family of protocols are based on two basic assumptions (Heinzelman et.al., 1999):

- First, before sending the actual data the nodes exchange the meta-data to negotiate with neighbours and hence conserve the energy by operating more efficiently.
- Secondly in conventional flooding and gossiping-based routing protocols the energy and bandwidth of the network is wasted by sending unnecessary copies of data in overlapping areas.

In the figure1.3 node A starts advertising its packets to B by its ADV packets. Node B responds to node A by sending REQ packet. After that A sends the requested data to B by its DATA packet. Afterwards node B sends out the ADV packets to its neighbours which in turns gets the REQ packets from them and

sends the requested DATA. In this way the data is disseminated in the network using the explained approach.

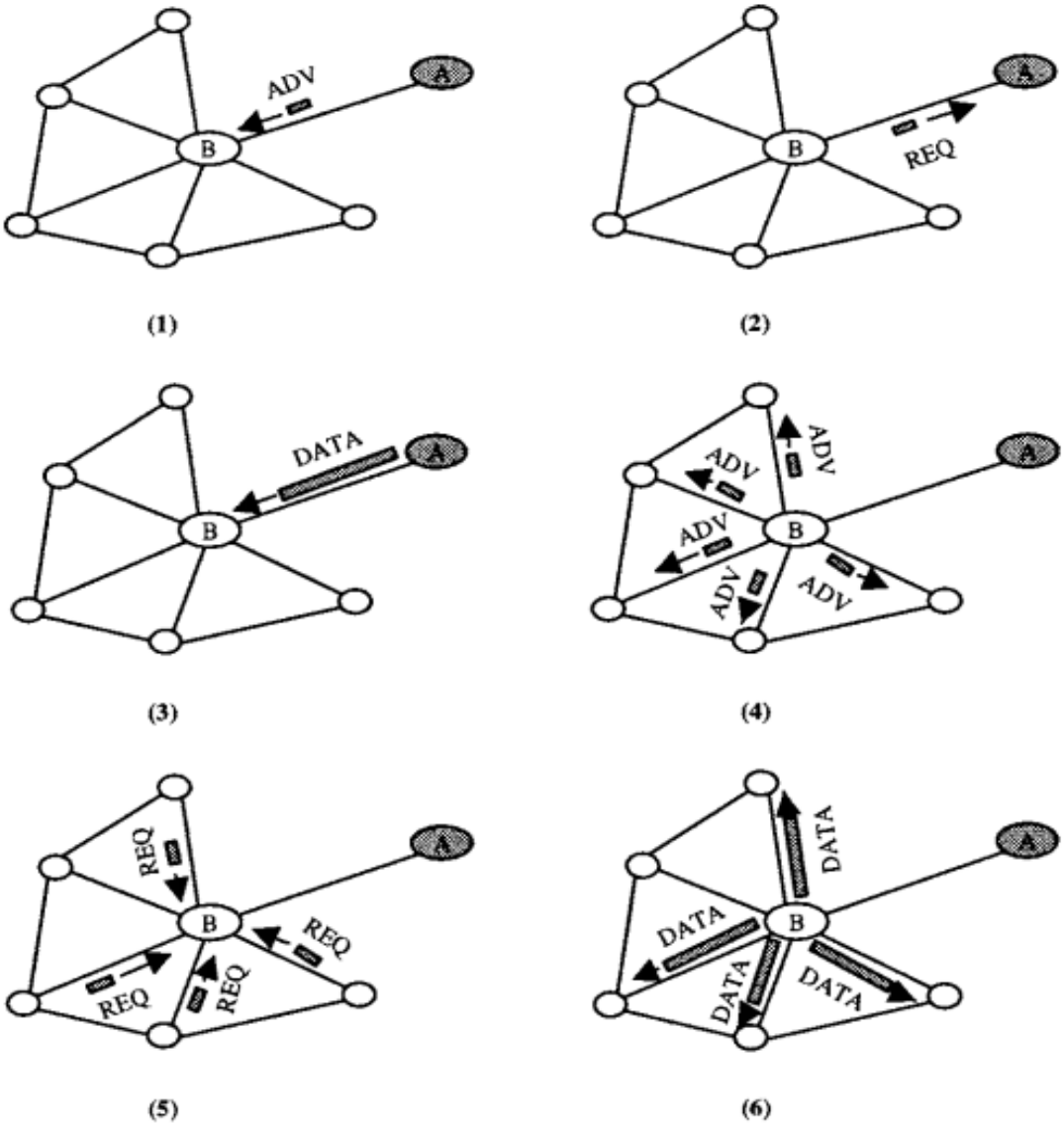

Figure 1.3 Concept of SPIN Protocol (Heinzelman et.al.,2000)

1.5 Routing Attacks on Wireless Sensor Networks

The protocols for wireless sensor networks are susceptible to attacks due to their broadcast nature of the transmission. Moreover, wireless sensor networks have an additional vulnerability because nodes are more often placed in the hostile and open environment where they can get physically tampered. Basically the routing attacks in wireless sensor networks can be categorised in to two categories namely active attacks and passive attacks (Padmavathi & Shanmugapriya, 2009).

1.5.1 Active Attacks

In these types of attacks, the attacker monitors, listens and modifies the data stream in the communication channel. The following attacks are active in nature.

- **Routing Attacks:** These are the attacks which exploits the loop holes in the existing routing protocol in the networks. They can either tamper the data packets being communicated, exploits the bandwidth of the network, (Padmavathi & Shanmugapriya, 2009) tunnels the data in to other networks by using illegitimate nodes within the network or may drop the packets. The attacks which come under this category are given below:
  - Sybil attack
  - Sinkhole attack
  - HELLO flood attack
  - Worm hole attack
- **Packet Dropping Attacks:** In these types of attacks the attackers somehow tend to behave maliciously and start dropping packets. Their main objective is just to affect the communication in the network.

1.5.2 Passive Attacks

If the unauthorised node or the user monitors and listens the communication channel then it is termed as passive attacks. (Padmavathi & Shanmugapriya, 2009). In general term the attack against privacy is called passive attack. It includes:

- Eavesdropping
- Traffic analysis
- Location disclosure

1.6 Selection of Routing Attack

Since the wireless sensor networks are resource limited these networks are exposed to variety of attacks. The attacks are either related to routing or to packet dropping attack. This research work will be focussing on simulating routing attacks namely Sybil attack and Wormhole attack on SPIN protocol as these are assumed to be more prevalent attacks in wireless sensor networks.

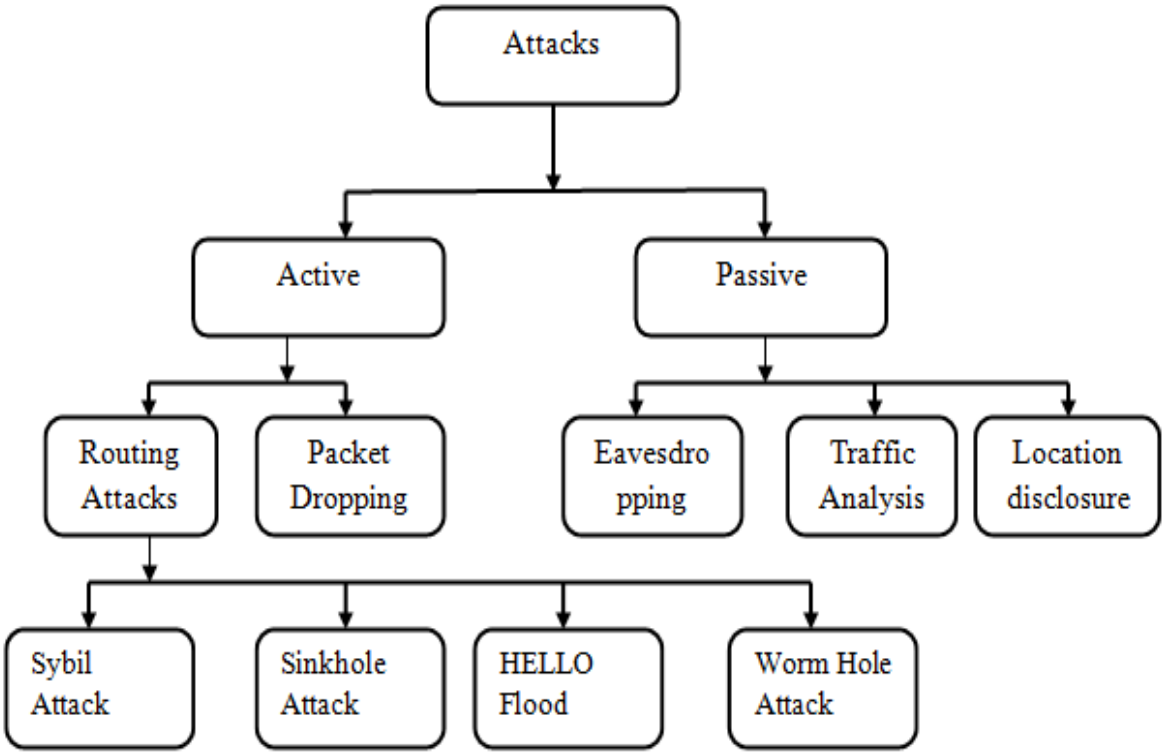

Figure 1.4 Types of attacks in WSN

The objective of simulating attack on SPIN is to calculate the performance of network under these attacks and overcome their shortcomings by proposing a protocol which ensures the better network performance along with the security.

1.6.1 Sybil Attack

In Sybil attack a single node presents multiple identities to other nodes in the network by pretending to be legitimate node or by claiming false multiple identities as shown in figure1.5. The Sybil attack can effectively reduce the effectiveness of fault-tolerant schemes such as multipath routing and topology maintenance in SPIN protocol (Karlof & Wagner, 2003).In the worst case, an attacker may generate an arbitrary number of additional node identities, using only one physical device.

Sybil attack can also be termed as multiple-identity attack. This attack normally uses a single malicious node to confuse neighbouring nodes, causing chaos among (by increasing REQ for DATA messages as a result delay increases

for the network) them and there by degrading the entire network performance (Karlof & Wagner, 2003).

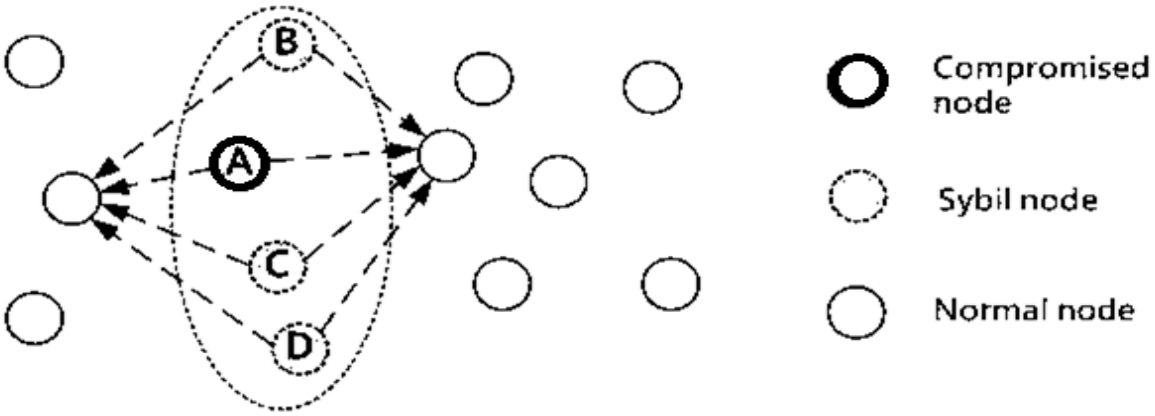

Figure 1.5 Sybil attack

1.6.2 Wormhole Attack

The wormhole attack is also called the tunnelling attack. In this attack, two or more malicious nodes collude to set up a short lower latency link or a virtual tunnel between them, through which they forward the packets to each other and replays them within the network (Sharif & Ahmed, 2010).The tunnel can be created in the following ways: packet encapsulation, creation of out of band link using specialised hardware channel, packet relay approach and usage of high power transmission.

An adversary by placing a wormhole at appropriate position in the network or may be near the base station be able to disrupt the routing in the network. An adversary can convince the nodes which are at multiple hops from the base station, they are at only few or one or two hops via the wormhole node (Karlof & Wagner, 2003). A systematic diagram showing the wormhole attack is shown in figure 1.6.

No harm can be done if the attacker performs this tunnelling in a reliable way. Instead it provides the advantage of connecting the network more efficiently. However the wormhole attack puts the attacker in a powerful situation than other existing network nodes, it can exploit its position in variety of ways. Wormhole attack can be performed even if the network is assumed to provide the security

aspect likes authenticity and confidentiality, (Hu et.al., 2006) with attacker having no knowledge of cryptographic keys being used to secure the network

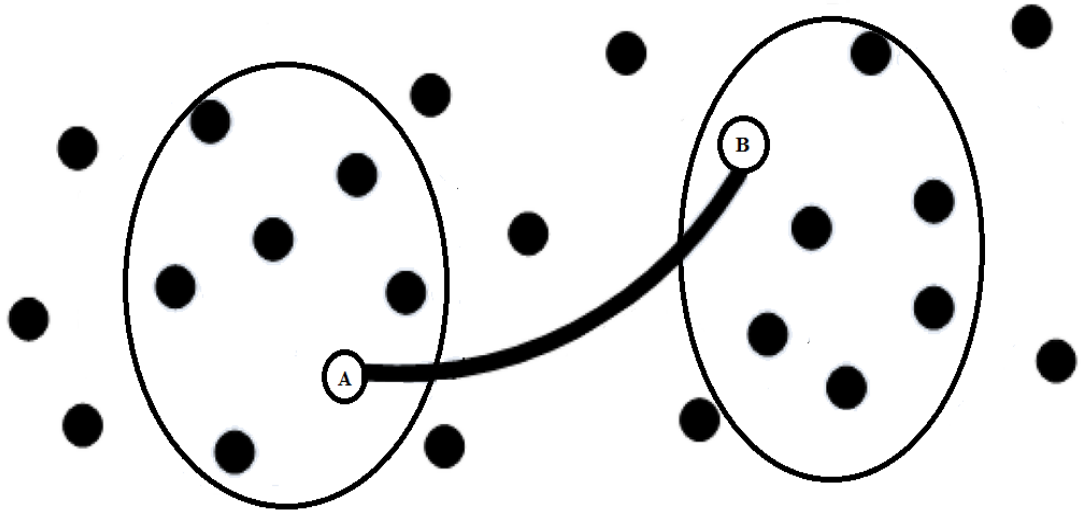

Figure 1.6 Wormhole attack

1.7 Security Requirements in Wireless Sensor Networks

As discussed by (Modirkhazeni et.al., 2010), to have secure communication over wireless sensor network there are security requirements which must be achieved. Although security requirements are application specific but following four basic requirements are considered.

1.7.1 Confidentiality

It is the ability of hiding the message to an illegitimate user. These parameters ensure that if the message is somehow intercepted by the illegitimate user, it should not be able to understand it.

1.7.2 Integrity

This parameter ensures that the message sent by the sender has not been altered or tempered i.e. it should be received as it is sent by the sender to the receiver.

1.7.3 Authentication

Authenticity ensures that message has been sent by the reliable user and not by any illegitimate user.

1.7.4 Availability

It guarantees that the network services are available whenever they are needed to transfer or forward the information i.e. if any node can use its resources to forward the packet in the network.

1.8 Advanced Encryption Standard (AES) Algorithm

AES is a 128 bit block cipher (Kak, 2014) which means it can process 128 bit data block using different keys. It allows three different key sizes 128, 192, 256 bit keys for encryption and decryption. A brief description of the algorithm is given below along with the systematic diagram shown in figure 1.7.

1.8.1 Encryption Process

Before any round for encryption begins, the first four words of the key schedule are XORed with input state array. In encryption process each round of algorithm consists of following steps(Kak, 2014):

- Substitute bytes
- Shift rows
- Mix columns
- Add round key

In the final step, output from last three steps is XORed with four words from key schedule. The last step does not include the “Mix column” operation.

1.8.2 Decryption Process

The decryption process is done in reverse manner as that of encryption process. The decryption process consists of following steps (KaK,2014):

- Inverse shift rows
- Inverse substitute bytes
- Add round key

- Inverse mix column

In the third step the output of two steps is XORed with four words from key schedule. The Last round of decryption does not include “Inverse mix column” operation as the decryption process is followed in reverse manner as that of encryption process.

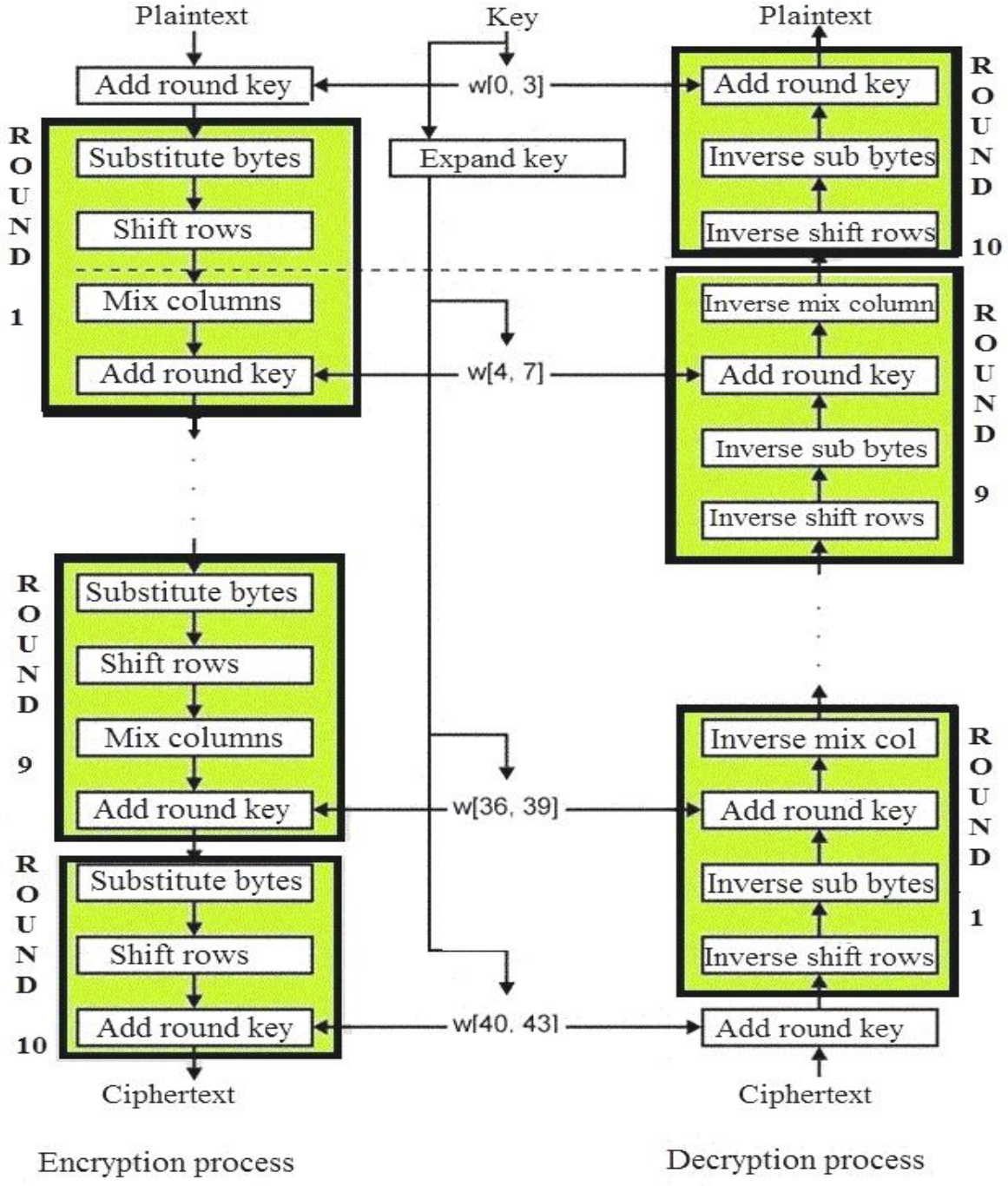

Figure 1.7 Rounds in AES algorithm

1.9 Problem Statement

The study of literature indicates that the various routing protocols had been proposed for wireless sensor networks, but very few of them take into consideration security issue along with the performance. Most of the research is focussed on optimisation of routing protocol for restricted capabilities of nodes and application specific networks. This research work focuses on enhancing the performance and security of Sensor Protocol for Information via Negotiation (SPIN) protocol under various security threats in wireless sensor networks.

1.10 Objectives

The objectives of research work have been listed below:

1. To simulate, evaluate and analyze SPIN protocol based upon performance parameters.
2. To simulate the Sybil Attack on SPIN protocol.
3. Performance analysis of SPIN protocol after implementing Sybil attack on it
4. Comparative analysis of SPIN and SPIN under Sybil attack.
5. To propose the enhanced SPIN protocol based on the analysis and findings.
6. To simulate Wormhole Attack on proposed enhanced SPIN protocol.
7. The proposed enhanced SPIN protocol is further secured based on shortcomings using cryptographic technique.
8. To compare SPIN, enhanced SPIN and SPIN with cryptographic technique based upon performance parameters and accordingly inferences are made.

CHAPTER 2

REVIEW OF LITERATURE

There are many routing protocols for wireless sensor networks, some of them consider the problem of security and some of them consider the performance of the network. In this section the emphasis is on SPIN (with multipath approach) and other protocols with multipath routing approach in wireless sensor networks. The selected findings about the SPIN based routing protocols which have been analysed for wireless sensor network are given below.

Heinzelman et.al., 1999 proposed SPIN-1 protocol for lossless network which uses the handshake protocol based approach for dissemination of data in the network. It works in three stages ADV-REQ-DATA. In this if the node has the data to send, it initiates the process by advertising ADV packet to its neighbours. On receiving the packet, neighbouring nodes check that whether it has requested or already received the packet. If not then it responds to the sender by its REQ packet. This process comes to halt if the initiator of the process sends the DATA(containing the data requested by the interested neighbour) packet back in reply. This protocol was originally designed for lossless network but it can be made adaptable to lossy networks. In this process the advertising nodes can re-advertise the missing ADV packet at regular intervals to compensate the lost packets. The interested or the requesting nodes can compensate by re-requesting the REQ and DATA packets that do not reach to them within specified time period.

Heinzelman et.al., 1999 proposed SPIN-2 protocol which is an extension of the SPIN-1 protocol by adding a simple energy-conservation heuristic technique to the SPIN-1 protocol. SPIN-2 protocol works on the calculated threshold value of the networks.SPIN-2 uses the same three stage communication model (ADV-REQ - DATA) as SPIN-1 does. When a node in SPIN-2 observes that its value is approaching a low threshold, it adapts its operations accordingly in the protocol. In general terms the node will only participate in a stage of protocol, if it believes that it can complete all other stages of the protocol without reaching to its low threshold. This conservative approach, neither does nor bar any node to

participate in any of the three stages, provides that each node must have a minimum threshold to complete that stage of the protocol.

Perrig et.al., 2002 developed a framework for SPIN in Wireless Sensor Network. This framework is executable on TinyOS operating system and has two building blocks namely SNEP(Secure Network Encryption Protocol) for data confidentiality, authentication, integrity, freshness with less communication overhead and μTESLA(the micro version of Timed, Efficient Streaming, Loss-tolerant Authentication Protocol) for data authentication. In this the sensor node is closely acquainted with base station and the base station is solely responsible for establishing a pair wise key between the nodes which can be targeted. The two nodes involved deriveindividual independent encryption, decryption keys and MAC keys for their two way communication. For the encryption it uses RC5 algorithm. This protocol does not deals with DoS (Denial of Service) attacks.

Kulik et.al., 2002 presented the optimised SPIN protocol, SPIN-PP (with a low-energy threshold) that was first optimised for the networks using point to point transmission media. Since it is easy for the nodes to communicate directly with each other without considering neighbouring nodes, the SPIN –PP works in three stages names ADV-REQ-DATA. In this the node which wants to share data sends the ADV packet to its neighbour, upon receiving the neighbouring nodes check whether it has requested advertised data. If not, it then responds by sending REQ packet for the data and then the advertising node sends the DATA packets to the interested node and the process is completed. This protocol is designed for lossless networks with symmetric communication.

Kulik et.al., 2002 enhanced SPIN-PP as SPIN-EC by adding energy conservation attribute to it. When energy is sufficient the SPIN-EC nodes work the same way as SPIN-PP works. When SPIN-EC nodes observe that the energy is reaching some threshold value then it checks before initiating any process that whether it can be completed or not i.e. the node only participates in the stage of protocol only if it believes it can complete the other stages of protocol.

Kulik et.al., 2002 proposed SPIN-BC (A three stage handshake protocol for broadcast media) in which broadcast media nodes share the single transmission media. SPIN-BC improves over SPIN-PP for broadcast networks by using cheap

one to manycommunications that is all the messages that broadcast addresses are processed by all the nodes within the range. Thus SPIN-BC does not lose much efficiency by using broadcast address. SPIN-BC is different from SPIN-PP in the terms that it uses broadcast and moreover when the node in SPIN-BC receives the ADV packet it checks whether it has requested the packet or not. If ‘not, then it sets the timer to expire chosen from predetermined interval. When the timer expires the node sends the REQ to the broadcast address specifying original advertiser in the header and other nodes other than advertisers cancel their timers. So in this redundant copies are not sent to nodes.

Woodrow & Heinzelaman, 2002 introduced SPIN-IT (sensor Protocol for Information via Negotiation- Image Transfer)a protocol for sharing images across a wireless network. This protocol is based on SPIN protocol. This protocol is designed to share and explore images or pictures over a wireless media alongside by conserving the energy and bandwidth of the network. SPIN-IT protocol is data centric which means it sets up route based on data locations instead of node addresses. That means if two nodes contain same data, a route to either of them is equally valid.

Xiao et.al., 2006 proposed a Secure SPIN Protocol based upon the SPIN protocol. This protocol is based on the same assumption of Wireless sensor network consisting of sensor nodes, sink and internet connection between them. In addition to this, Secure SPIN protocol is based on the assumption of SPIN-PP protocol, when a node advertises a ADV packet if all of its neighbour does not have enough energy left with them “blink spot” will occur. To overcome this a clustering based SPIN was proposed which divides the sensor nodes to classes and then sensor nodes are randomly selected as cluster heads from them. It used the symmetric key cryptography which does not include large cryptographic functions and ultimately does not require much of the memory and processing power.

Rehne et.al., 2010 developed a energy saving routing algorithm by dividing SPIN protocol in to three parts namely Initialisation phase, data collection phase and negotiation phase. In initialisation phase, all the sensor nodes are first synchronised to the global time. After that DATA packets are generated

periodically by running sensor application. InData Collection phase, each node obtains DATA packets from its neighbours or the sensing application. The DATA packet obtained contains the following parameters: origin node, sequence number and payload containing time stamp and the sensor readings. In this data is collected periodically until the node gets out of power or switched off. In this phase node collects the sample and generates the ADV packets based on them. In Negotiation phase, ADV packet is sent to the neighbouring node which upon receiving request the advertiser using REQ packet for the corresponding data and then actual DATA is sent.

Rehena et.al., 2011 proposed a modified version of SPIN protocol and named it as M-SPIN. This protocol was basically designed for specific application that requires quick responses like forest fire, disaster etc.In that case it is important the node must transmit information towards sink node instantly. M-SPIN protocol added new phase called distance discovery to find the distance of the sink from each sensor node based upon the hop counts from sink. This helps to determine the nodes which are far from sink node. The other phases of M-SPIN includeNegotiation and data transmission.The Negotiation is done before sending the data; therefore hop value determines the dissemination of data in the network. In data transmission phase the M-SPIN works as similar to the SPIN-BC protocol. As soon as the source node receives the request, data is immediately transferred to the requesting node. The negotiation phase is repeated for the nodes other than the sink node i.e for the intermediate nodes. The intermediate nodes send the ADV packet for the data with different hop count value. This process is continued till the data reaches the sink node.

Jing et.al., 2011 presented the improved version of SPIN protocol by removing the “blind forward” and “data inaccessible” problem as SPIN-I. This protocol has same network model as SPIN protocol. SPIN-I has a negotiation process, which was based on the three way handshake protocol. It has three phases namely: Data Broadcasting Stage, Data Requesting Stage and Data Transmission Stage. In data broadcasting stage when a sensor node has a data to send, it starts broadcasting ADV packets to its neighbour which contains the meta data i.e. data about the data. In data requesting stage the nodes upon receiving ADV packet checks its threshold energy that whether it will be able to complete the

next three stages, if not it will not make any response. Otherwise it checks whether it already has the data. If it has then it set REQ message to 1 and back its energy to the source node by REQ message. This was the big difference between SPIN and SPIN-I. In data transmission stage the source node update its neighbour list according to the energy values and REQ messages it receives. The source node judges the source nodes in its neighbour list based on the threshold time, if the flags in the neighbours list are both 0 or 1 then it filters the node whose flags are 0 and forwards data to the nodes who has largest energy value. If somehow nodes have the same value then it selects the nodes randomly to forward data. If all the flags have 0 values then it chooses the node which has larger energy value. If the time is more than threshold then flags are 1, here the “data inaccessible” problem arises, the source nodes selects the nodes which has largest value from its neighbours list and forwards the data and removes the node which do not send REQ message from the neighbours list

Kavitha & Kathikeyan, 2012 introduced the EEM-SPIN to overcome the problem faced in M-SPIN protocol by using cluster methodology and dynamic cluster heads election. In this for the formation of cluster and the election of cluster heads the Weighted Cluster Algorithm is used. A cluster is a collection of sensor nodes in a sensor network. The cluster based approach provides the most efficient use of the resources for the dynamic networks.The cluster heads are responsible for the transmission of the information and act as the routers that forward the packet from one node to another. These are also responsible for maintaining network topology. It is aware of its cluster members and the cluster heads which are at one hop from it. The cluster head selection is very much critical since they maintain the network topology.

Xu et.al., 2012 introduced a new protocol based on SPIN protocol for wireless sensor home networks called SPIN-pi having almost same architecture where most of the WSN protocols can be applied straight forwardly. SPIN-pi protocol was designed to improve routing efficiency and increasing network lifetime. This protocol introduced the concept of plug-in node and assigns the routing tasks to them. In this when a node has data to share it advertises the ADV packet and when it receives the REQ packets from the neighbours the data is sent to them. If no one is willing to send the data at that time it again sends the ADV

packets in the network. In this the non plug-in will only route the packet when there is no willing to serve it while the plug-in node will serve any ADV packet. When this protocol is compared with traditional SPIN protocol the energy consumption of the entire network reduces significantly by using plug-in nodes as REQ sender by avoiding mobile nodes which involves unnecessary communication.

Parihar, 2013 presented SPIN-G protocol which overcomes the two problems of SPIN: first it reduces the meta data negotiations to achieve it the randomised gossip in combination with data aggregation is used, secondly it achieves the balanced energy consumption distribution across the network and extends its lifetime by developing a strategy to make the sensor nodes chose the advertising neighbour with higher energy.

Khosla et.al., 2013 worked on a new protocol based on the SPIN Protocol called Shortest Path minded SPIN (SPMS). SPMS extended the existing SPIN protocol by performing multi-hop communication within a zone (which is the node's maximum transmission radius) for the request. It is based on the assumption that network is connected to minimum transmission power and a node can transmit at multiple power levels. This protocol reduces the delay and the energy consumption as compared to SPIN.

Khosla et.al., 2013 proposed the SPMS-Rec (Shortest Path Minded SPIN-Rec) which was designed to reduce the Energy consumption and Delay in the network in case of path failure. The reliability is achieved by local re-transmitting by the nodes. This protocol solves the energy consumption problem of SPIN protocol, but the node failure and network lifetime still persists.

Khosla et.al., 2013 proposed a variant to SPMS-Rec called request suppression(SPMS-Rec-RS) whose purpose was to reduce the number of requests for the same data, hence reducing the redundant data. This protocol is assumed to provide the reduce in the rate of redundant data by 63-87%.

Sahoo & Puthal et.al., 2014 introduced a new protocol called energy efficient Data centric RoUtinG protocol called DRUG based on SPIN protocol. In this adaptive data centric approach is used to find an optimal routing path from source to sink was proposed. When the sensor nodes are deployed randomly in a

restricted area with single sink, DRUG protocol uses three types of messages to communicate between different nodes: ADV, for data advertisement whenever a node has new data to send, ACK: for sending an ACK message when it wishes to receive data, DATA: containing the actual data with Meta data. ADV and ACK messages contain only meta-data. In this the ADV and ACK messages will be cheaper to transmit and receive their corresponding DATA messages. The DRUG protocol is resource aware, resource adaptive and data centric like SPIN protocol. It transmits its data with three way handshake like SPIN does but it transmits it with unicast whereas SPIN transmit it using multicast.

The review of literature indicates that each protocol has either focussed on the application specific platform or on the performance which includes the lifetime enhancement of the network. But hardly few them considers security as an essential parameter. The findings about the shortcomings of the protocols are discussed in table 1.

Table 1: Shortcomings in Existing Protocols

Sr. No.	Author's Name	Protocol Name	Shortcomings
1.	Heinzelman et.al., 1999	SPIN-1	Designed only for lossless networks. If the packet gets lost the interested node has to initiate the whole process again.
2.	Heinzelman et.al., 1999	SPIN-2	Extension of SPIN-1 with energy conservation strategy. In this a node can only participate in communication process if it has the threshold energy. If a node has sensitive data to send with energy less than threshold, it will not be able to participate and leads to loss of data.
3.	Perrig et.al., 2002	Framework for SPIN(SNEP and μTESLA)	It does not deal with DoS (Denial of Service) attacks.
4.	Kulik et.al., 2002	SPIN-PP	It was designed only for point to point lossless networks with symmetric communication. It also uses single communication media.
5.	Kulik et.al., 2002	SPIN-EC	If the node has sensitive data to send and has energy less than threshold then it may create loss of information.
6.	Kulik et.al., 2002	SPIN-BC	Designed especially for broadcast network.

7.	Woodrow &Heinzelaman, 2002	SPIN-IT	Designed specifically for sharing images across the network. So it is application specific.
8.	Xiao et.al., 2006	Secure-SPIN	Although it forms the classes of network with CH, but has overhead of selecting the CH in the network which consumes energy.
9.	Rehne et.al., 2010	Energy saving SPIN algorithm	The excess processing in each phase leads to increased delay in the network.
10.	Rehena et.al., 2011	M-SPIN	It increases the networks overhead due to repeated process of distance discovery for intermediate nodes.
11.	Jing et.al., 2011	SPIN-I	In this if during the selection of random nodes in the networks, somehow a node with sensitive data is not selected it may lead to delay causing faulty decision making.
12.	Kavitha & Kathikeyan, 2012	EEM-SPIN	The cluster head selection increases overhead.
13.	Xu et.al., 2012	SPIN-pi	Consecutively sending ADV packet by plug-in node may lead to node isolation.
14.	Parihar, 2013	SPIN-G	It does not consider overlapping problem.
15.	Khosla et.al., 2013	SPIN-SMPS	The nodes present on the corner of communication zone may not utilize their radio power efficiently.
16.	Khosla et.al., 2013	SPMS-Rec	Node failure and network lifetime problem.
17.	Khosla et.al., 2013	SPMS-Rec-RS	Node failure and network lifetime.
18.	Sahoo & Puthal et.al., 2014	DRUG based SPIN	It uses unicast addressing and does not consider scalability of the network.

CHAPTER 3

SIMULATION SET UP AND METHODOLOGY

This chapter provides an insight in to the implementation part of the research work. The various research challenges in routing and security issues of WSN are identified in the literature review. Hence some tool is required to validate the explored challenges. The Network Simulator version 2.34(NS-2.34) is selected to simulate and analyse the selected SPIN protocol for the various security threats against the performance metrics.

3.1 Simulation Tool (NS-2.34)

Network Simulator version 2 is abbreviated as NS2. NS2 is an event driven simulator developed at university of California at Berkeley, USA as part of real network simulator in 1989. In 1995 NS2 was made the part of VINT project at LBL under the support of DARPA. NS2 is not a finished and final product instead the bugs in this are still being discovered and fixed. It is still the part of ongoing research and development. The users are themselves responsible for verifying their simulation, since the models implemented in the simulator are not exactly matching with the real ones (McCanne & Floyd, 2002).

NS2 provides substantial support for simulation of routing, and multicast protocols over wired and wireless networks. It can be implemented on Linux-based as well as Microsoft Windows operating systems.

NS2 is very helpful in networking research which involves varying the network parameters or creating multiple scenarios with different parameters.NS2 implements various network protocols such as TCP and UPD, traffic source behaviour such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms. NS2 also implements multicasting and some of the MAC layer protocols for LAN simulations (ns-2, 2011).

3.1.1 Features of NS2

NS2 is object oriented simulator written in C++ (front-end), with an Otcl interpreter at front-end. NS2 supports variety of protocols, traffic models etc .The various features of NS2 are listed below (McCanne & Floyd, 2002):

- Protocols Support: TCP, UDP, HTTP, Routing algorithms.
- Traffic Models: CBR, VBR, Web etc.
- Error Models: Uniform, Bursty etc
- Radio Propagation, Mobility models
- Energy Models
- Topology Generation tools
- Visualization Tools

3.2 NS2 Structure

A simplified user view in figure 3.1 shows that NS2 is an object oriented OTcl interpreter that has network component object, simulation event scheduler object and network set up module.NS2 is based on two languages C++ and OTcl (ns-2, 2011).

- C++ Event Scheduler at the back-end.
  - For defining protocols etc.
- OTcl (Object oriented Toolkit command language) at the front-end which includes:
  - Creating scenarios
  - Extension to protocols defined in C++
  - Objects that are created in OTcl have corresponding objects in C++.
  - Instructs the traffic source when to initiate and halt transmission of packets through event scheduler.

Tcl is highly dynamic programming language that can be used in wide range of applications like networking, creating web applications. Tcl is basically cross platform language, highly extensible and is fully compatible with C Programming language (McCanne & Floyd, 2002).

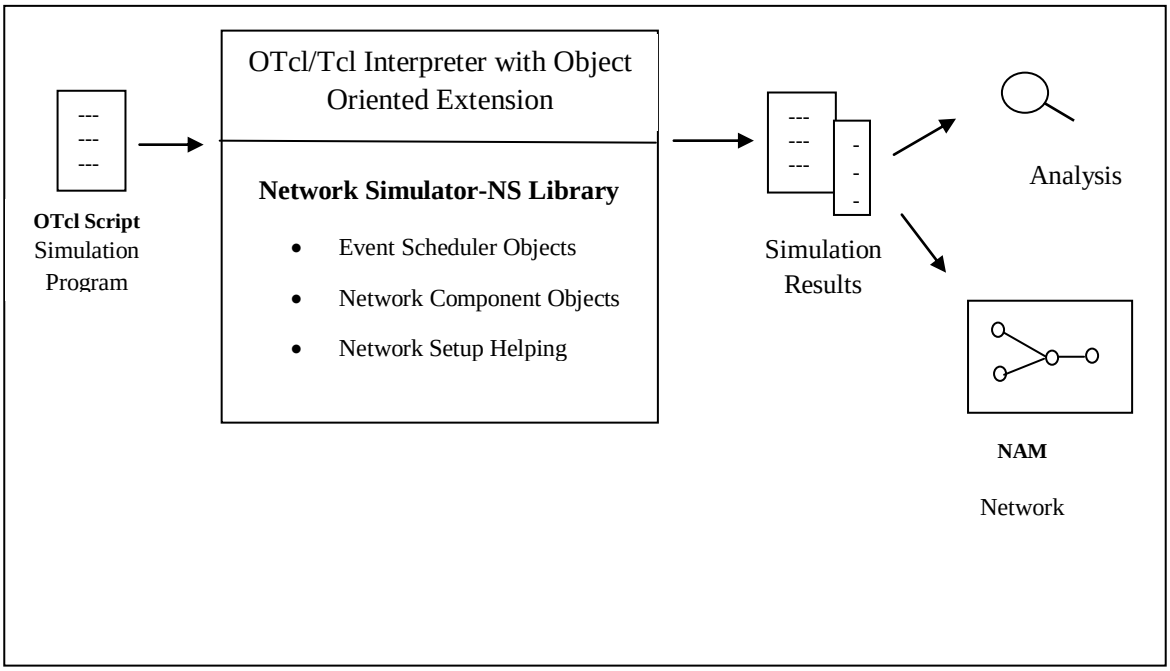

Fig 3.1 Simplified user view of NS2 (ns-2, 2011)

3.3 Operating System Used

In this research work Ubuntu-12.04 LTS (version 12.04 with long term support) is used as a platform to install NS-2.34. It is available for free and is developed and maintained by an open source community.

Features of Ubuntu-12.04 are as follows:

- Extensive performance,
- Robustness, reliability,
- Security,
- Improved virtualisation support,
- New Graphical user interface (GUI) manager.

3.4 Performance Metrics for Evaluation

To check the performance of SPIN there are several parameters to check its effectiveness in the network. The routing protocols are either evaluated on the basis of their operations or on the basis of their routing algorithm. In this study the throughput, packet delivery ratio, energy spent, average delay is used as metrics to evaluate the performance. The reason behind the selection of these parameters for metrics is that it helps in effectively finding the routing algorithm's efficiency.

3.4.1 Throughput

It is the ratio of total data packets received by a receiver from a sender to the final packet received by receiver. The throughput is measured in KBPS (Kilo Bytes per Second).

$$\text{Throughput} = \frac{\sum \text{Packets received} * \text{packet size}}{\sum \text{Simulation time}}$$

3.4.2 Packet Delivery Ratio

The ratio of the number of data packets originated at application layer by CBR source to the packets delivered at CBR sink i.e. at destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol. It is measured in % ratio.

$$\text{Pdr} = \frac{\sum_{i=0}^{n} \text{Packets Received}}{\sum_{i=0}^{n} \text{Packets Sent}}$$

3.4.3 Energy Spent

It is the average energy spent by the nodes for communication in the network. It is measured in Joules/sec.

$$\text{Average Energy Spent} = \sum \frac{\text{Energy Consumed}}{\text{Time}}$$

3.4.4 Average Delay

It is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue (waiting time) in data packet transmission. Only the data packets that are successfully delivered to destinations are counted.

$$\text{Average Delay} = \frac{\sum(\text{Packets arrive time} - \text{Packet Sent time})}{\sum \text{Number of connections}}$$

The lower value of end to end delay means the better performance of the protocol. It is measured in micro seconds.

3.5 Methodology Used

The proposed research work has been carried out in phases as follows:

Phase 1 To Study and Simulate the SPIN Protocol

In this phase SPIN is analysed by simulating on NS 2.34 using configuration shown in table 1. The results are analysed against selected performance metrics.

Phase 2 To Implement Sybil Attack on SPIN Protocol

In this phase the Sybil attack is implemented on SPIN protocol and the various vulnerabilities of SPIN protocol are studied and analysed critically. The simulation parameters used are shown in table 1.

The results are recorded against the performance metrics and the inference is drawn for enhancing the SPIN protocol.

Phase 3 To Analyse and Implement Enhanced SPIN Protocol

This phase is divided in to two stages to analyse the proposed E-SPIN protocol.

Stage 1: In this stage the proposed E-SPIN protocol is enhanced by adding security parameters to it. The Message authentication code is added to provide security to data in E-SPIN.

Stage 2: In this Wormhole attack is implemented on E-SPIN to check for its security and based on performance parameters the inference is drawn.

Phase 4 To Enhance the E-SPIN Protocol Using Cryptographic Technique

In this the E-SPIN protocol is further enhanced to increase its security along with maintaining the performance of the E-SPIN protocol. The encryption algorithm called Advanced Encryption Standard (AES) is incorporated to E-SPIN protocol to counter further attacks by encrypting the DATA in the communication process of SPIN protocol. The basic working of proposed AES-SPIN is same as that of SPIN protocol.

Phase 5 Comparative Analysis of SPIN, E-SPIN and AES-SPIN Protocol

In this phase the performance of SPIN, E-SPIN and AES-SPIN protocol is analysed critically for their performance based upon their throughput, average delay, packet delivery ratio and energy spent.

3.6 Simulation Parameters

The simulation parameters for simulating protocols in wireless sensor networks are defined in table 1. The same configuration is followed throughout this research work for implementing and analysing the various protocols implemented for study. The results for the simulation are drawn using Abstract Window Toolkit (AWK).

Table 2: Simulation Parameters

Parameters	**Value**
Number of Nodes	50
Topography Dimension	500*500
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground Model
MAC Type	802.11 MAC Layer
Packet Size	500 bytes
Routing Protocol	SPIN
Interface Queue	Drop Tail/Priority Queue
Channel	Wireless Channel
Link Layer Type	LL
Antenna Type	Omni direction

CHAPTER 4

RESULTS AND DISCUSSIONS

This chapter presents the discussion of results of the research work. The simulated results are analysed and discussed using graphs. Initially the simulation of SPIN protocol is performed and Sybil Attack is implemented on it. The observations are recorded in the form of graphs against their corresponding performance metrics.

4.1 Analysis of SPIN Protocol

A topology of wireless sensor networks with 50 nodes is created; transmission of packets between the nodes is done using SPIN protocol with Sybil nodes in the network. The parameters such as end to end delay, throughput, packet delivery ratio, energy spent are calculated and the output is shown graphically.

4.1.1 Throughput

The throughput of SPIN protocol has degraded in the presence of Sybil attack because of the fact that under attack a single node presents multiple identities and all the traffic migrates to these malicious nodes, which in turns get

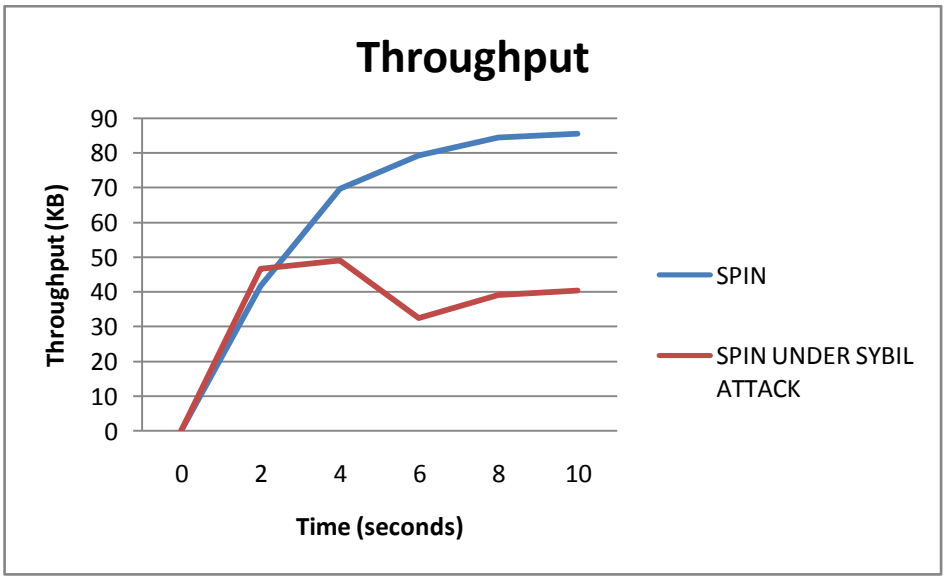

Figure 4.1 Throughput of SPIN and SPIN under Attack

dropped by Sybil nodes, so the throughput of network decreases. Figure 4.1 shows the effect of Sybil attack on SPIN protocol.

4.1.2 Packet Delivery Ratio

The packet delivery ratio of SPIN protocol under Sybil Attack has decreased drastically beacuse the packets intended for the legitimte node are comnsumed by sybil nodes that pretends to be legitimate node or having route to destination which ultimately drops them. Hence Pdr is reduced as shown in figure 4.2.

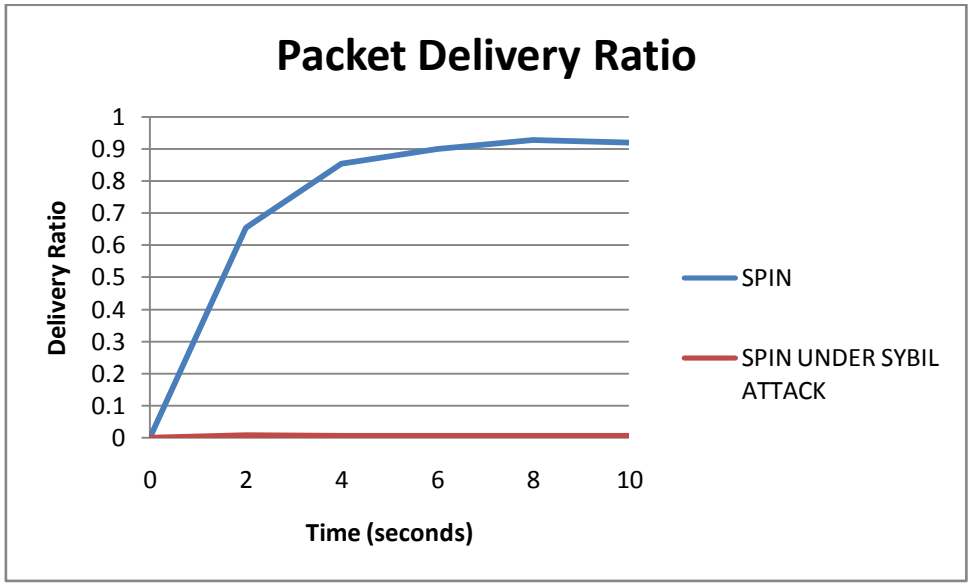

Figure 4.2 Pdr of SPIN and SPIN under Attack

4.1.3 Energy Spent

In figure 4.3 it is observed that the battery power of sensor nodes are slightly more drained in the presence of Sybil nodes because the duplicate nodes start troubling the routing of packets by sending wrong route information to legitimate nodes in the network. The overall energy spent under Sybil attack has increased because of presence of multiple images of single node by malicious nodes.

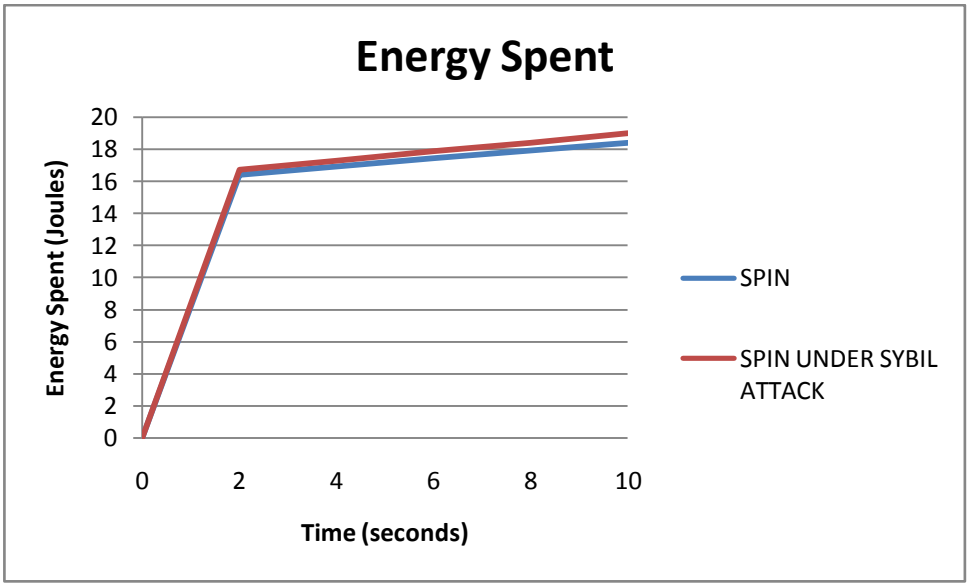

Figure 4.3 Energy Spent of SPIN and SPIN under Attack

4.1.4 Average Delay

The figure 4.4 represents the average delay for SPIN protocol has increased under Sybil attack because the packets are being consumed by Sybil nodes and are never forwarded thereby increasing the average delay in the network.

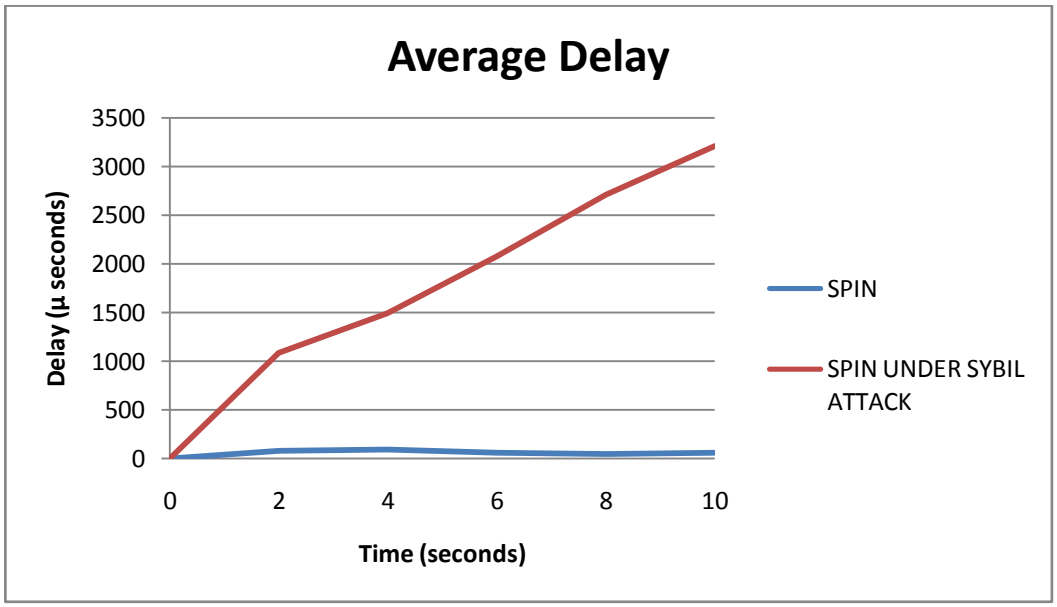

Figure 4.4 Average Delay of SPIN protocol and SPIN under Attack

It can be inferred from the above graphs that while implementing Sybil attack in wireless sensor network the performance parameters deteriorate at very fast pace. So there is a need to develop a more secure protocol for Wireless Sensor

Networks which should be able to provide the good network performance under different security threats.

4.2 Proposed E-SPIN protocol based on SPIN protocol

The motive of implementing the Sybil attack on the SPIN protocol is to measure its security flaws. The simulation results show that there is need of improvement in existing SPIN protocol because under attack the performance has degraded heavily. So based upon the findings the enhanced SPIN protocol called as E-SPIN (Enhanced-SPIN) is proposed which considers performance along with the security. E-SPIN is developed as a protocol in NS2 which adds message authentication code to each ADV and REQ packet being sent. It is assumed that that each node knows its single hop neighbour. The MPR flooding algorithm is used to broadcast the data in the network.

The proposed E-SPIN protocol has the same working as that of existing SPIN protocol except for authentication that is being done for ADV, REQ at each stage of the communication process. E-SPIN is simulated on NS2 under Wormhole Attack on it and the results are recorded against performance metrics.

4.2.1 Implementation of WORMHOLE Attack on E-SPIN

In the next phase the performance of Proposed E-SPIN protocol is evaluated under Wormhole attack in wireless sensor networks. It is assumed to be the most severe attack in wireless sensor networks. WORMHOLE is implemented on proposed E-SPIN protocol using the same topology and compared against the proposed E-SPIN protocol.

4.2.1.1 Throughput

When Wormhole Attack is implemented on E-SPIN protocol and it is observed that throughput of the network has degraded drastically as shown in the figure 4.5 because of the presence of wormhole of nodes in the network which tunnels the packets between them and replays in the network or drops them.

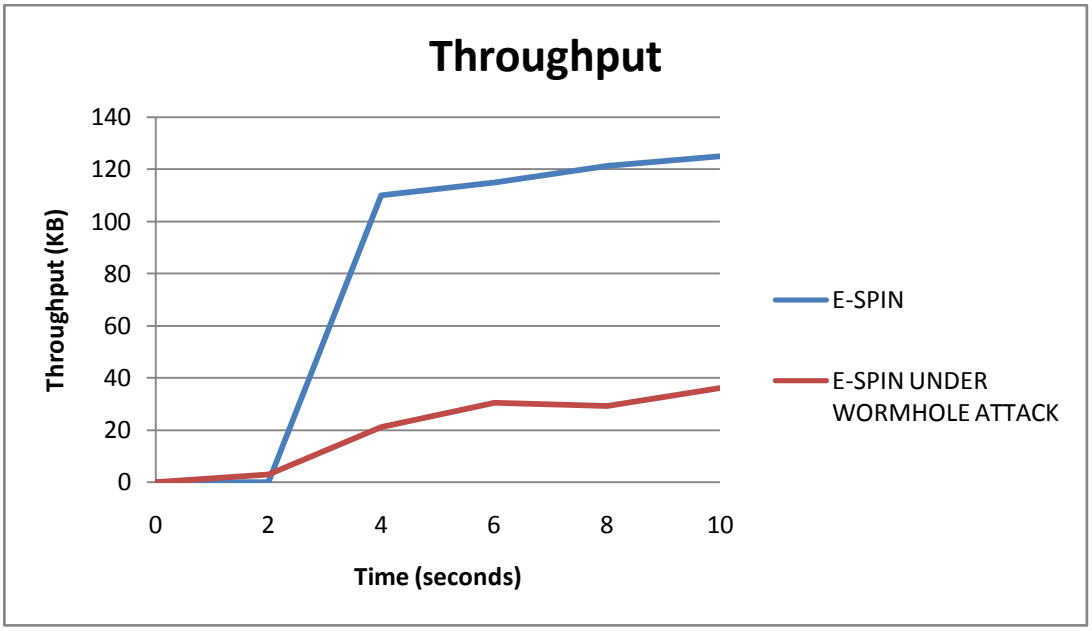

Figure 4.5 Throughput of E-SPIN and E-SPIN under Attack

4.2.1.2 Packet Delivery Ratio

The Wormhole attack degrades the Packet delivery ratio (Pdr) of the network shown in the figure 4.6. The packet delivery ratio has reduced significantly which degrades the quality of the network. In this the wormhole node is able to steal the packets from source node and tunnels them to another wormhole node in the network which ultimately drops them .

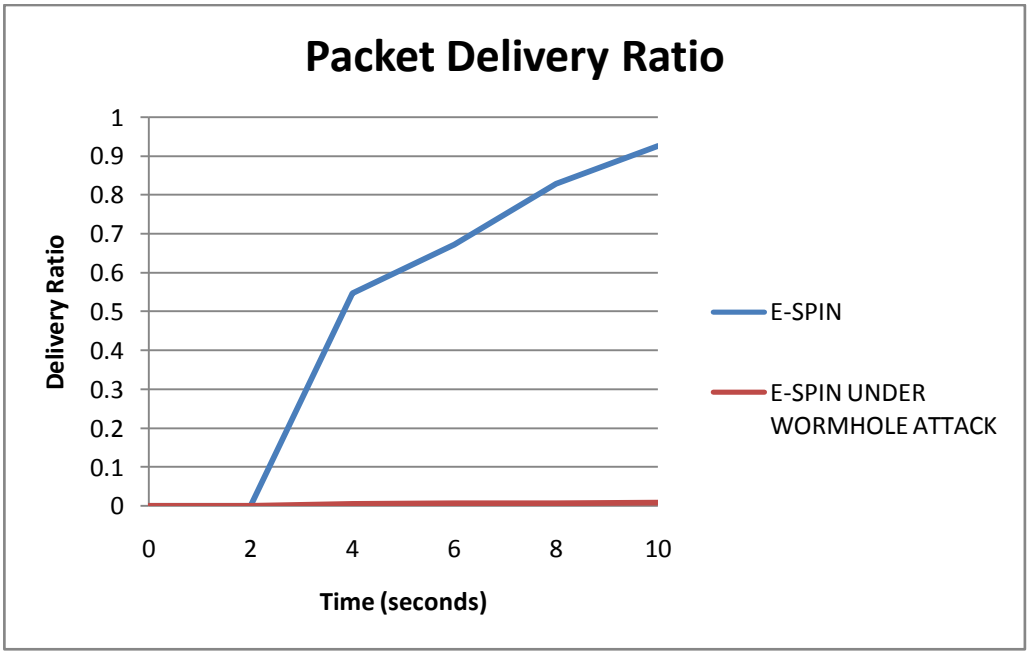

Figure 4.6 Pdr of E-SPIN and E-SPIN under Attack

4.2.1.3 Energy Spent

The energy spent by E-SPIN protocol under Wormhole attack has increased at a constant rate as the wormhole nodes started participating in the routing process by creating tunnel, the energy consumption increases. The energy spent has slight variation towards the end of simulation by little amount in the presence of wormhole nodes as shown in figure 4.7.

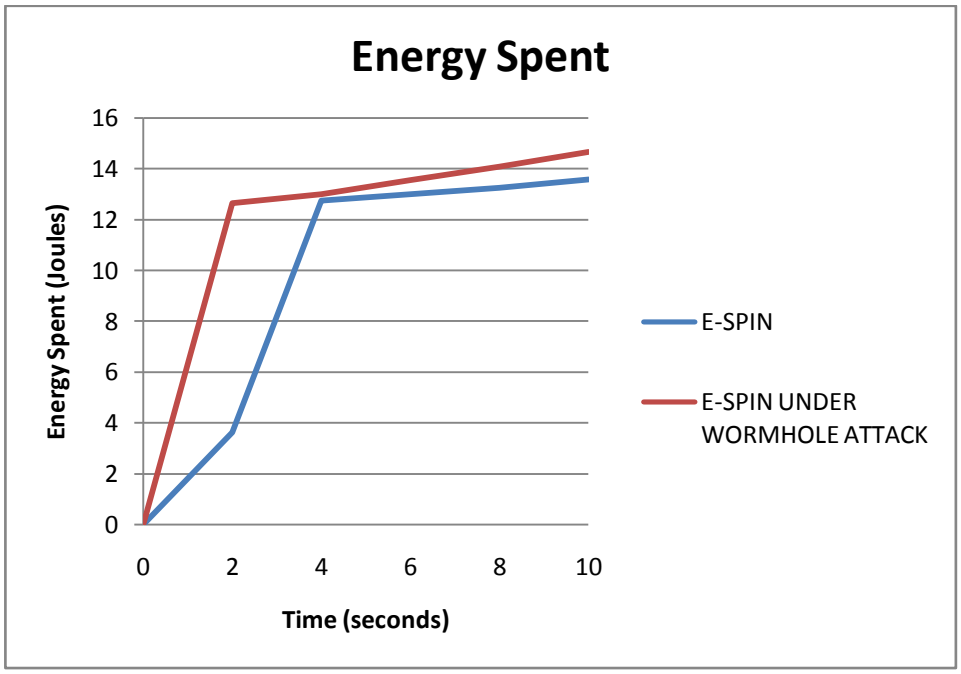

Figure 4.7 Energy Spent of E-SPIN and E-SPIN under Attack

4.2.1.4 Average Delay

In figure 4.8 the average delay under normal conditions is almost negligible as compared to average delay under wormhole attack. The delay under wormhole attack shows the fluctuating behaviour, initially it is zero but as the simulation time increases it shows constant increase in phases because wormhole nodes start sensing the packets from source node and drop them. So the packets never reach their destination instead they are replayed in the network thereby increasing the overall delay of the network.

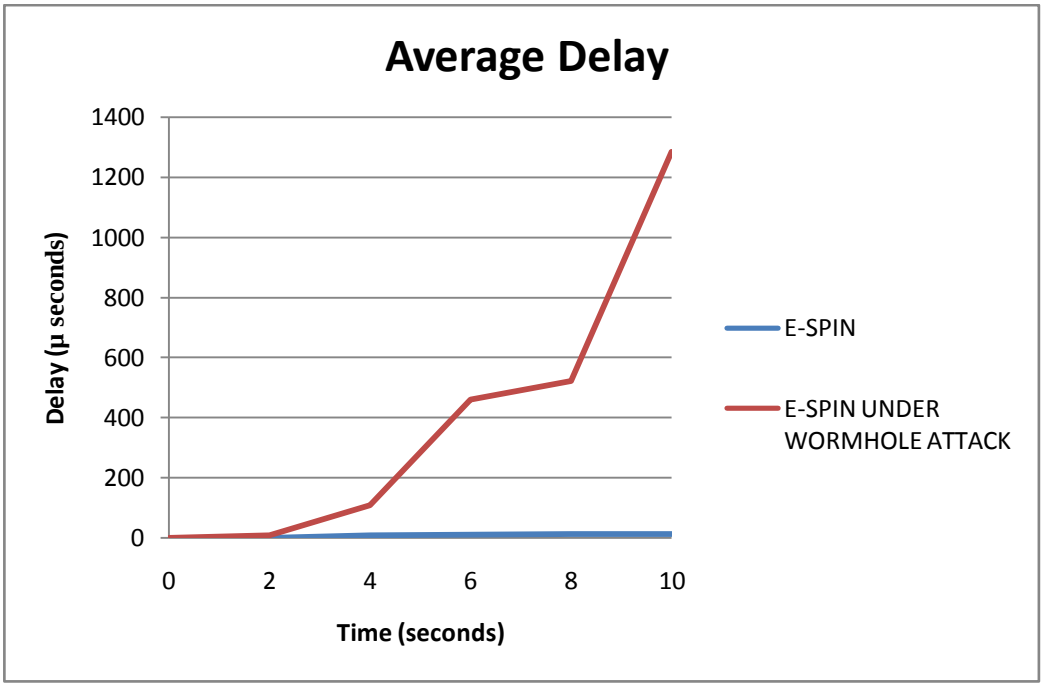

Figure 4.8 Average Delay of E-SPIN and E-SPIN under Attack

4.3 Enhancement of proposed E-SPIN Protocol and its comparative analysis

It is clear from the observation in section 4.2 that Wormhole Attack has deteriorated the network performance of our proposed E-SPIN Protocol to a larger extent. The delay, Pdr which determines the performance of the protocol in a network has increased and decreased respectively by very large rate. So there is need for a mechanism to counter this attack on the proposed E-SPIN protocol. After much considerations and study the enhancement to E-SPIN protocol is proposed by adding AES encryption scheme in to it. AES provides the three basic aspects of security for the DATA being sent namely authenticity and confidentiality along with integrity of the data. The performance parameters are recorded for SPIN, Proposed E-SPIN and AES-SPIN Protocols in a comparative graph and the inference is made.

4.3.1 Throughput

The throughput achieved in E-SPIN and AES-SPIN protocol is almost same but better than the existing SPIN protocol under normal conditions as shown in figure 4.9. So it can be inferred that proposed protocols outperform SPIN protocol in terms of throughput.

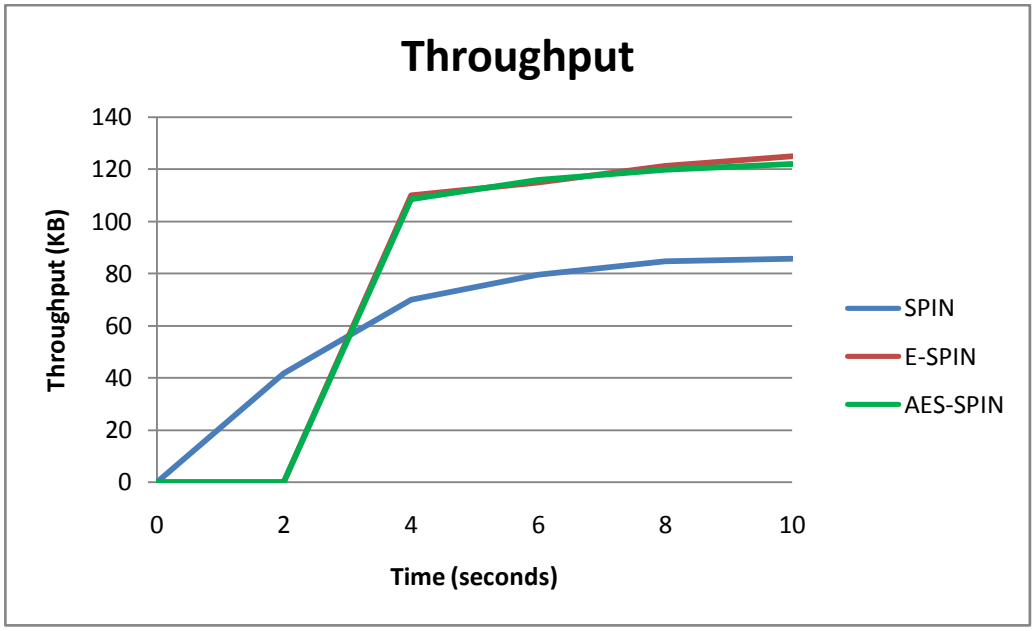

Figure 4.9 Throughput of SPIN, E-SPIN and AES-SPIN

4.3.2 Packet Delivery Ratio

As figure 4.10 shows that Pdr achieved in E-SPIN and AES-SPIN is less than existing SPIN protocol. So it can be inferred that increased security in E-SPIN and AES-SPIN has degraded their Pdr.

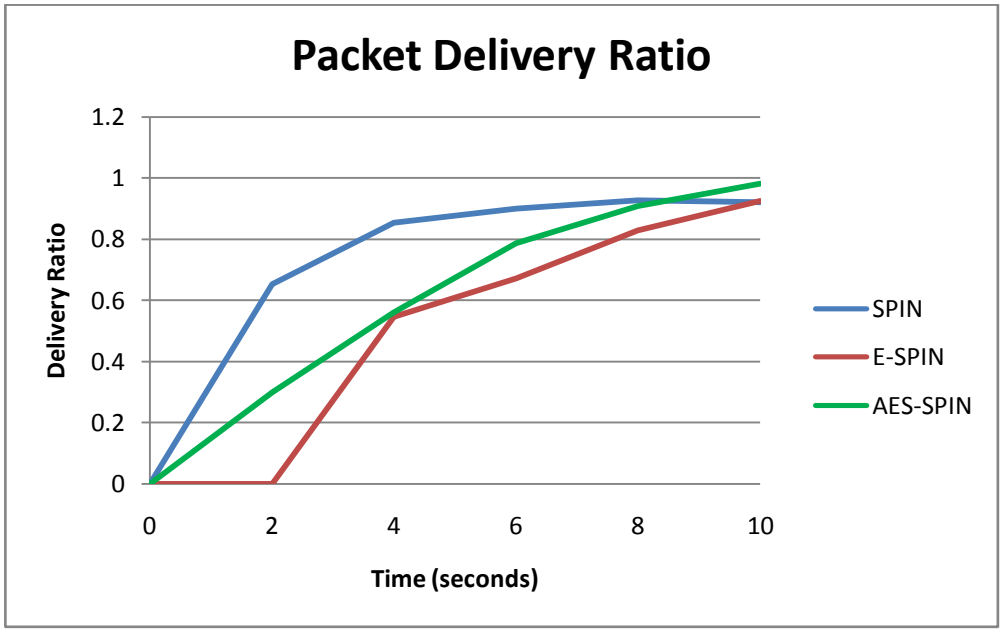

Figure 4.10 Pdr of SPIN, E-SPIN and AES-SPIN

4.3.3 Energy Spent

It is clear from figure 4.11 that the energy spent in E-SPIN and AES-SPIN is almost same and outperforms SPIN protocol, it means these protocols can provide better network lifetime with more security than SPIN protocol.

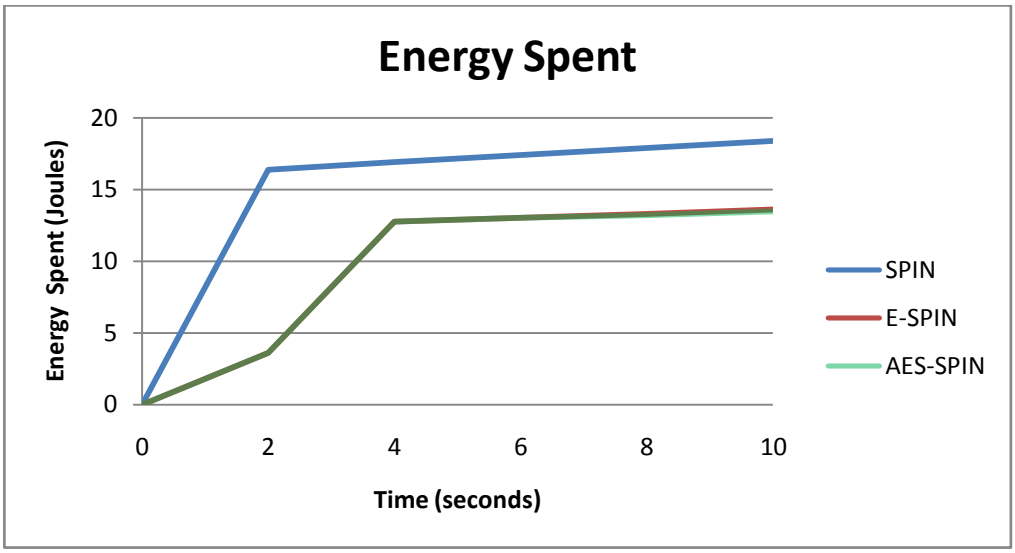

Figure 4.11 Energy Spent of SPIN, E-SPIN and AES-SPIN

4.3.4 Average Delay

The average delay of E-SPIN and AES-SPIN is less than the SPIN which shows fluctuating behaviour as shown in figure 4.12. It means that the proposed protocols are better than SPIN protocol in terms of average delay, as lesser the delay better is the performance of protocol.

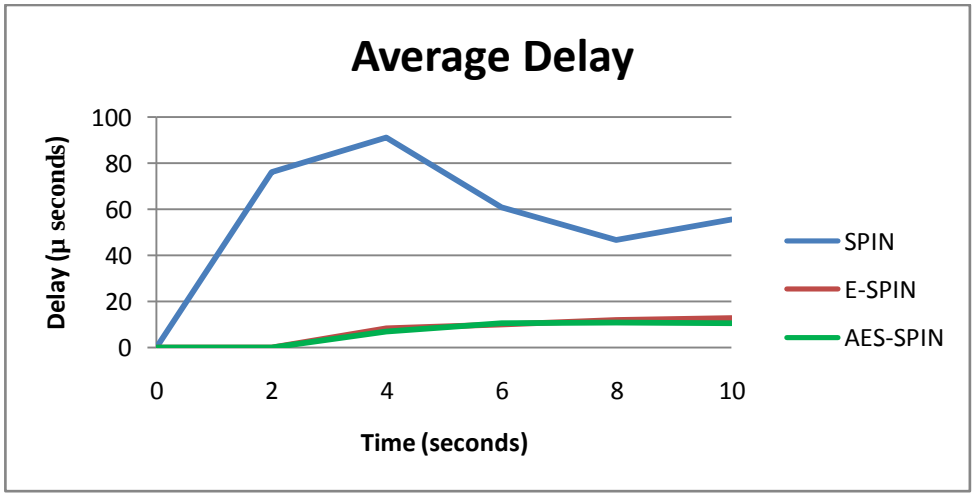

Figure 4.12 Average Delay of SPIN, E-SPIN and AES-SPIN

CHAPTER 5

CONCLUSION AND FUTURE WORK

It is evident from literature study that the performance and security in wireless sensor network has always been a prime concern. But most of the research work on SPIN protocol is either focussed on performance or security, none of them consider both as the basis of the research work. This research work has been carried out on enhancing the performance along with security of SPIN in wireless sensor networks.

In first phase of this study, the SPIN protocol is analysed under Sybil Attack and the results show that SPIN does not provide any strong security mechanism to secure its ADV, REQ and DATA packets but only provides the way to disseminate information in the network as the parameters for performance metrics recorded have degraded. So in order to provide security, Message Authentication Code (MAC) is applied to provide the authenticity and integrity to ADV and REQ packets in SPIN without encrypting DATA packets; which is referred as enhanced SPIN (E-SPIN).

The E-SPIN is then tested for its security by implementing Wormhole attack and it has been found that E-SPIN is still vulnerable to attack i.e. the wormhole nodes are still able to sense and drop the packets which degrade the performance of the network based on performance metrics. In order to further enhance the performance along with security, the E-SPIN is further modified with cryptographic technique called AES to provide security to DATA packets.

The results show that E-SPIN and AES-SPIN outperforms the existing SPIN protocol in terms of Delay, Throughput, Energy Spent along with maintenance of the security issues. But as the security of SPIN protocol is increased in E-SPIN and AES-SPIN the packet delivery ratio of the protocol gets affected. So it can be concluded that enhancing the security has compromised Pdr, but overall enhanced protocols provide better network security as they implement MAC and AES for securing the network. It has also been found that E-SPIN and AES-SPIN protocol are deployable in the networks which demand the better performance along with enhanced security.

The future work for this study varies from network structure to application demands. Different network structures and application have different demands. As of now the proposed E- SPIN and AES-SPIN can be analysed under different network size for denser network using application specific performance metrics like jitter, routing overhead and network lifetime. The enhanced protocols security could also be investigated with respect to various types attacks to which wireless sensor networks are vulnerable.

REFERENCES

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

Bhunia, D., Kar, P., & Bhattacharrya, S. (2014). Wireless Sensor Network And Mobile Ad Hoc Network. Retrieved FEB 05, 2014, from http://ciemcal.org/wireless-sensor-network-and-mobile-ad-hoc-network/

Das, A.X., Eapen, C., Ashok, A., Tripath, S., Shadi, R. M. (2012).Dynamic Event Based Energy Efficient Routing Protocol For Wireless Sensor Networks (WSNs). International Journal of Engineering and Advanced Technology (IJEAT). 1(6), 262-265.

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. InSystem Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on (pp. 10-pp). IEEE.

Heinzelman, W. R., Kulik, J., & Balakrishnan, H. (1999, August). Adaptive protocols for information dissemination in wireless sensor networks. InProceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (pp. 174-185). ACM.

Hu, Y. C., Perrig, A., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. Selected Areas in Communications, IEEE Journal on, 24(2), 370-380.

Jing, L., Liu, F., & Li, Y. (2011, October). Energy saving routing algorithm based on SPIN protocol in WSN. In Image Analysis and Signal Processing (IASP), 2011 International Conference on (pp. 416-419). IEEE.

KaK, A., (2014,March 26). AES: The Advanced Encryption Standard. Retrieved May 10, 2014, from Purdue University: https://engineering.purdue.edu/KaK/Compsec/NewLectures/Lecture8.pdf

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.

Kavitha, M., & Karthikeyan, K. (2012, November). Comparison of data centric protocols for WSN and energy enhanced M-Spin (EEM-SPIN). In International Journal of Engineering Research and Technology (Vol. 1, No. 9 (November-2012)). ESRSA Publications.

Khosla, R., Zhong, X., Khanna, G., Bagchi, S., & Coylem, E. I. (2007, March). Performance Comparison of SPIN based Push-Pull Protocols. In WCNC (pp. 3990-3995).

Kulik, J., Heinzelman, W., & Balakrishnan, H. (2002). Negotiation-based protocols for disseminating information in wireless sensor networks. Wireless Networks, 8(2/3), 169-185.

Li, Y. X., Qin, L., & Liang, Q. (2010, December). Research on wireless sensor network security. In Computational Intelligence and Security (CIS), 2010 International Conference on (pp. 493-496). IEEE.

Mangla, P., & Arora, V., (2013)Comparative Study and Analysis of Data Centric Routing Protocols of Wireless Sensor Network Based on Energy Consumption.International Journal of Scientific and Research Publications, 310.

McCanne, S., & Floyd,S. (2002, July 3). The Network Simulator –ns2. Retrived October 11, 2013, from information sciences institute: http://www.isi.edu/nsnam/ns

Modirkhazeni, A., Ithnin, N., & Ibrahim, O. (2010, September). Secure multipath routing protocols in wireless sensor networks: a security survey analysis. InNetwork Applications Protocols and Services (NETAPPS), 2010 Second International Conference on (pp. 228-233). IEEE.

Ns-2. (2011). Retrieved December 21,2013, from Network Simulator: http://www.nsnam.org/developers

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

Parihar, P. S. (2013). Wireless Ad-Hoc and Sensor Networks: Tcp Enhancement (TCP-MANET) For Wireless Ad-Hoc Networks and Data Dissemination Protocol (Spin-G) In Wireless Sensor Networks. networks, 2(9).

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless networks, 8(5), 521-534.

Rehena, Z., Kumar, K., Roy, S., & Mukherjee, N. (2010, July). SPIN implementation in TinyOS environment using nesC. In Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on (pp. 1-6). IEEE.

Rehena, Z., Roy, S., & Mukherjee, N. (2011, January). A modified SPIN for wireless sensor networks. In Communication Systems and Networks (COMSNETS), 2011 Third International Conference on (pp. 1-4). IEEE.

Sahoo, B. P. S., & Puthal, D. (2014). DRUG: An Energy-Efficient Data-Centric Routing Protocol for Wireless Sensor Network. arXiv preprint arXiv:1404.4685.

Sharif, L., & Ahmed, M. (2010). The Wormhole Routing Attack in Wireless Sensor Networks (WSN). JIPS, 6(2), 177-184.

Woodrow, E., & Heinzelman, W. (2002, June). SPIN-IT: a data centric routing protocol for image retrieval in wireless networks. In Image Processing. 2002. Proceedings. 2002 International Conference on (Vol. 3, pp. 913-916). IEEE.

Xiao, D., Wei, M., & Zhou, Y. (2006, May). Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks. In Industrial Electronics and Applications, 2006 1ST IEEE Conference on (pp. 1-4). IEEE.

Xu, Y., Wu, S., Tan, R., Chen, Z., Zha, M., & Tsou, T. (2013). Architecture and Routing Protocols for Smart Wireless Home Sensor Networks. International Journal of Distributed Sensor Networks, 2013.