Enhancedsecure sensor protocol with information via negotiation(SSPIN)

Asha P.N#[1], S.C Lingareddy#[2] , Mahalakshmi T#[3], Archana S#[4]

[1]*Research Scholar, Research and development Center, Bharathiar University, Coiambatore India.*
[2]*HOD of Computer Science and Engineering, Alpha College of Engineering, Bangalore India.*
[3,4]*Shri Pillappa College Of Engineering, Bangalore*

Abstract--*Wireless sensor network (WSN) is a special network that is rapidly growing in the present technology, due to its wireless communication, sensing factor and processing power both in controlled and uncontrolled environment. Sensor nodes are battery operated. Reducing the energy consumption by sensor nodes is one of the major challenge. This paper enhances existing SSPIN(Secure Sensor Protocol with Information via Negotiation) with high data security, reduced energy consumption by the nodes and increased throughput. The experimental results show that the proposed system achieves high performance compared with the existing system in terms of throughput, energy consumption and packet delivery ratio. We validate our claims through analysis and simulations.*

Keywords–*Sensor node, security, energy, cryptography, ADV, REQ, DATA*

1. Introduction

Several routing algorithms are proposed and optimized to get the desired throughput but very less prominence is given to the security issues**.** SPIN (Sensor Protocols for Information via Negotiation) is a family of negotiation-based information dissemination protocols. It has not been designed with the security requirements in mind. In this paper, we propose a security extension of SSPIN, called I- SSPIN (improved Secure-SPIN), and use the simulator framework to prove its security.

The rest of the paper is organized as follows: In section 2 we give an overview of the existing system .In section 3 we propose our S-SPIN routing Protocol extension In section 4 we discuss simulator tool and section 5 we show the implementation ,section 6 we show the result, section7 paper is concluded.

A. Existing system

SPIN: Sensor protocol for Information via Negotiation, is based on data centric approach which efficiently broadcasts the information between the sensor nodes in energy constrained mode. SPIN name their data in high-level data descriptors, called metadata. The semantics of the meta-data format is application-specific and not specified in SPIN. [8].

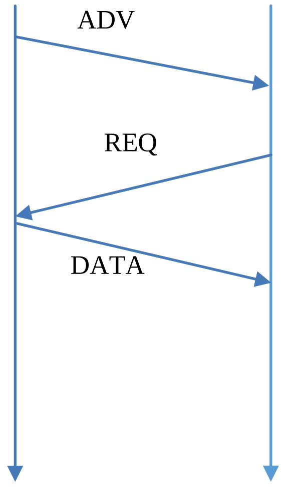


Fig.1 SPIN protocol

SPIN has three types of messages as shown in fig.1, they are [1]:

- **ADV Message:**
  A node advertises to all the nodes in the network to notify that it has data to send.
- **REQ Message:**
  A node requests the node which has the given the advertisement that it has data with it.
- **DATA Message:**
  This message contains the actual message that is requested by a node.

SPIN family:There are four family in the SPIN family:

1. SPIN-PP
2. SPIN-EC
3. SPIN-BC
4. SPIN-RL

SPIN protocol lacks the security scheme and to overcome, this problem security extension of SPIN was introduces which is called as S-SPIN(Secured-SPIN)S-SPIN has three message types: ADV, REQ, and DATA.

Protection of ADV and REQ messages was done by MAC (Message Authentication Code). Cryptographic scheme to DATA message,was not specified[11]. Assumption was done that every sensor node knows the identifiers of its neighbors, each pair of neighboring nodes share a pairwise key, and adversary cannot launch attacks against the network before neighbor discovery and key establishment phases accomplished[11]. The S-SPIN is a three-stage protocol (ADV-REQ-DATA),with each stage corresponding to one of the message types[11].

ADV Stage: Once a node obtains new data, it sends an ADVmessage to its neighbors, naming the new data. The ADVmessage has the following format:

(*ADV*, *ls*, *meta*, *n*, (*l*1, *l*2, *l*3, ...), (*MAC*1, *MAC*2, *MAC*3, …))Where *ADV* is a constant message type identifier, *ls*is the identifier of the initiator *S*, *meta* is the application specified meta-data, *n* is a random integer, (*l*1, *l*2, *l*3, ...) is a identifier list of *S*'s neighbors, and (*MAC*1, *MAC*2, *MAC*3, …) is a MAC list,arranged in the order of the identifier list. Each MAC is generated by a pairwise key shared between *S* and one of its neighbors, and it covers the fields *ADV*, *S*, *meta*, *n*, (*l*1, *l*2, *l*3,...).

REQ Stage: Upon receiving an ADV message, the neighboring node first checks to see whether it has already received or requested the advertised data. If not, then checks whether *S* is one of its neighbors, and verify the correctness the corresponding MAC in the MAC list. If these verifications fail, the ADV message is dropped. Otherwise, a REQ message is generated and sent back to the initiator. The REQ message has the following format:

(*REQ*, *ld*, *n*, *MACreq*)

Where *REQ* is a message identifier, *ld*is the message sender *D*'s identifier. And *n* is an integer, equals to the one in ADV message, *MACreq*is generated by the pairwise key shared between *S* and *D[11]*.

DATA Stage:Once *S* receives an REQ message, it checks its cached ADV messages, to see if *n* exists, and did it send the message to *D*. Then, *S* recomputes*MACreq*, and compares to the one in REQ message, to ensure the message is correct. If these verifications are passed, *S* generates a DATA message contains the actual data and sends it to *D*. We do not specific which cryptographic scheme shall be used in DATA message, S-SPIN relies on users to choose an appropriate for the network.The following is the format of the DATA message:

(*DATA*, *D*, *Enc*(*S*||*n*||*data*))

Where *DATA* is a message identifier, *Enc*(*S*||*n*||*data*) is the encrypted content, *data* is the actual data[11].

Disadvantages of existing system

- High energy consumption
- It does not consider link failure
- Low packet delivery ratio

B.Proposed System

SPIN protocol is the best protocol but does not provide any security measure [1]. So we make use of SSPIN protocol to secure the data by making use of RSA cryptographic algorithm.

In the existing system only ADV and REQ is secured using SSPIN. So in our proposed system we are securing the DATA phase of SSPIN. Effective communication happens only when there is magnificent link quality. So here by using SSPIN we determine the link quality.

Every node in the WSN makes use of power source (rechargeable or non-rechargeable battery). Replacing battery every now and then becomes very tedious job, since they can be used in non-reachable locations. Sensor node consumes energy to perform the activities like sensing, computing, transmitting, etc. Where in sensor nodes consume more energy while transmission of the data than performing other operation. In order to conserve energy in transmission, AODV routing protocol is used to route the packets. SSPIN is enhanced to achieve greater energy efficiency, throughout, packet delivery ratio compared to existing system.

C. Simulation tool

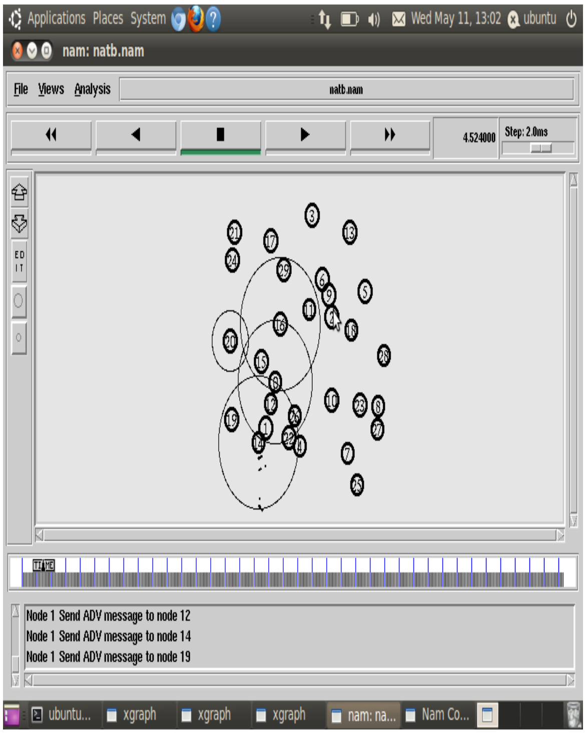
NS 2.34 (Network simulator 2.34) is an object-oriented, discrete event driven simulator developed at UC Berkley written in C++ and OTCL [10]. NS 2.34 supports platform like Ubuntu, Linux and Windows. Most commonly Ubuntu and Linux environment is used than making use of Windows. NS 2.34 implements some of the protocols like TCP, UDP, FTP, TELNET,CBR,VBR and routing algorithms such as Dijkstra [10]. In order to invoke this underlying protocol TCL language is used. NS 2.34 supports both wired and wireless communication, here for WSNs we make use of wireless communication.

The results of NS 2.34 simulation can be either text based or animated. The results of NS 2.34 is shown on NAM (network animator) tool or on graph (Xgraph).

D. Implementation

There are five modules as follows:

Network module**:**An undirected graph G (V, E) where the set of vertices V represent the sensor nodes in the network and E represents set of edges in the graph which represents the physical or logical links between the sensor nodes. Sensor nodes are placed at a same level. Two nodes that can communicate directly with each other are connected by an edge in the graph. Let N denote a network of m number of nodes, $N_1, N_2, \ldots N_m$ and let D denote a collection of n data items $d_1, d_2, \ldots d_n$ distributed in the network. For each pair of sensor nodes $N_i$andN_j, let t_{ij} denote the delay of transmitting a data item of unit-size between these two nodes.



Node 1 Send ADV message to node 12
Node 1 Send ADV message to node 14
Node 1 Send ADV message to node 19

Fig.2 Source nodes broadcasting their ADV message to other neighbor nodes in WSN.

In fig2 we have simulated for 30 nodes (0-29) using NS 2.34. Nodes are placed in X, Y and Z co-ordinates (Z axis is 0, since NS 2.34 is two-dimensional). And initial position of all the 30 nodes are set and here nodes are mobile.

SSPIN Protocol**:** SSPIN can be used to improve the security of SPIN [1]. In data communication, security plays a vital role. There some limitations, though we have many routing protocols in WSNs. SSPIN protocol as three phases:

ADV:The primary goal of sensor nodes in WSN is to collect the information from the physical world. When sensor node has the data with it, it advertises its message to its neighbor nodes, saying that it has got the data. An ADV message is sent to all the nodes in WSN. The ADV message format is as shown below [1]:

(ADV, l$_s$, meta, n, (l$_1$, l$_2$, l$_3$…..), (MAC$_1$, MAC$_{2,}$ MAC$_3$…))

Where ADV is message identifier, l$_s$ is identifier of the initiator S, meta is application specified meta-data, n is random integer, (l$_1$, l$_{2,}$ l$_3$) are identifiers list of S neighbors, (MAC$_1$, MAC$_{2,}$ MAC$_3$…) is MAC list [1]. Here ADV represents the advertisement.

REQ:When the source has sent the ADV message to all the other sensor node. Only the interested node will send the REQ message asking the source node to send the data.The message format is as below [1]:

(REQ, l$_d$, n, MAC$_{req}$)

Where REQ is message identifier, l$_d$ message sender for D's identifier and n is an integer equals to the one in ADV message, MAC$_{req}$is pare-wise key generated between S and D [1]. Here REQ represents request made by the sensor node.

DATA:Once the source node sends advertise message about its data in the WSN, it verifies the ADV message sent by it to other nodes. And even verifies the REQ message sent by the other node, before sending the DATA. The format for DATA is as below [10]:

(DATA, D, E$_{nc}$(S||n||data))

Where DATA is message identifier, Enc (S||n||data) is the encrypted content, data is actual data. [10]. Here DATA represents the data (or information) transmitted by the source node to its destination.

The proprieties of S-SPIN are listed below [1]:

- If two nodes n$_i$andn$_j$neighbors to each other then, n$_i$ and n$_j$ can be directly connected or can be connected by adversarial relay.
- If the node n$_j$ is a honest node than upon receiving the advertisement from node n$_i$ it will send a request (REQ) to the source node.

RSA Encryption Algorithm:

RSA is an asymmetric cryptographic algorithm that is named after three scientists by name Rivest, Shamir and Adleman. RSA algorithm makes use of two keys: private and public key (hence the name asymmetric algorithm). This public key is known to both sender and receiver, whereas private key is known only to the receiver. There many other cryptographic algorithm, RSA is the most powerful algorithm compared to symmetric cryptographic techniques like AES, DES, etc. Here for our purpose we consider RSA in two phases one for encryption and other for decryption.

RSA Encryption Algorithm:

- Input: RSA public key (n, e), Plain text m ∈ [0, n-1]
- Output: Cipher text c
- Begin

```
        i.   Compute c = $m^e$ mod n 2
        ii.  Return c
•   End
```

Securing the data in the real world plays a vital role. The data that has to be transmitted from source to destination is encrypted using RSA encryption algorithm. This encrypted data is termed as Cipher text. Here n is a constant, e is the key used to encrypt the data to be sent. C is the chipper text of the original data to be sent, computed by m^e mod n 2 [1].

RSA Decryption Algorithm:

When the data is encrypted using RSA decryption algorithm the cipher text can be decrypted to obtain the actual data. The following is RSA decryption technique [1]:

```
•   Input: Public key (n, e), Private key d, Cipher text c
•   Output: Plain text m
•   begin
        i.   Compute m = $c^d$ mod n
        ii.  Return m.
•   End
```

Here n is a constant, e is the key used to encrypt the data to be sent, d is the decryption key used to get the plain text out of cipher text [1]. C is the cipher text of the original data to be sent computed by c^d mod n. m is the plain text obtained and is the data which was transmitted by the source sensor node [1].

E. Performance Analysis:

In order to achieve low energy consumption and high security the proposed system introduced an Improved SSPIN protocol. The modified SSPIN protocol has three phases. They are:

1. Advertising Phase
2. REQ Phase
3. Data transmission Phase

In "Advertising Phase" when a node has a data it advertises the other nodes that it has a data. Upon receiving an ADV message, each neighbor node verifies whether it has already received or requested the advertised data. In REQ Phase, the neighbor node sends REQ while current energy and link quality values are above threshold. The link quality of the node is calculated by using below formula,

Link Quality = (Transmission Radius-Distance)/velocity

The proposed system achieves better data transmission when the energy level and link quality of node is high. In "Data Transmission" phase the RSA algorithm is used to encrypt the data and it can be send to destination. Then RSA Decryption Algorithm is used to decrypt the transmitted data.

The performance of the proposed system is compared with the existing system.

F.Results

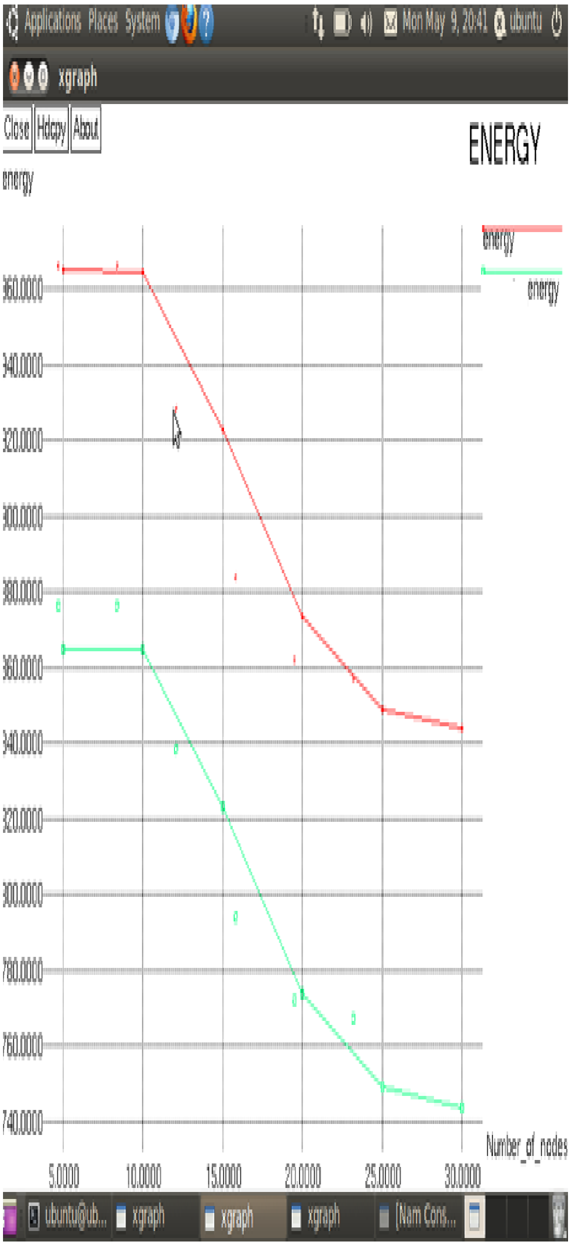


Figure 3 Energy Graph

Energy is calculated using the below formula:
Energy in Joules,
Energy Consumption = IE – RE
Where IE – Initial Energy
RE - Remaining Energy

Fig 3 shows the decreases energy consumption compared to the existing system.

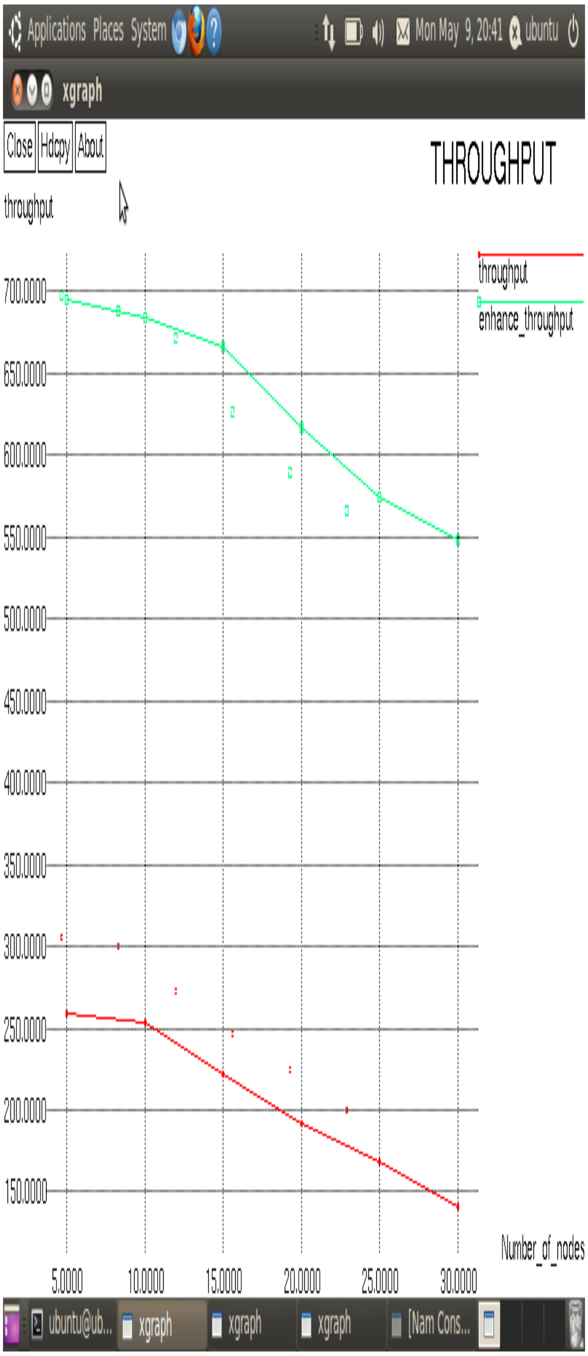


Figure 4 Throughput graph

Throughput is calculated using the below formula:

TP = (Byte*8)/2*interval*1000

Where TP – Throughput

Fig 4 shows the increased throughput of our proposed system.

The graph is plotted for 30 Nodes and the increased throughput compared to existing system.

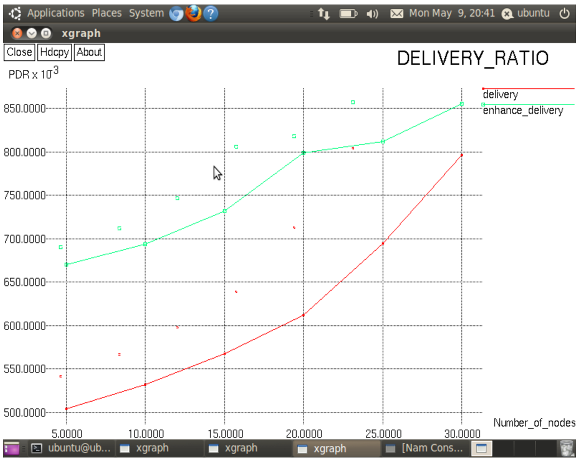


Figure 5 Delivery ratio

Packet Delivery Ratio (PDR) is calculated using the below formula:

PDR= DR/DR+DL

Where DR – Data Received

DL – Data Lost

Fig 5 shows the increased packet delivery ratio compared to the existing system. The graph is plotted for 30 Nodes versus PDR where the PDR is increased to 850 when compared to existing system 800

G.Conclusion

SSPIN is a security protocol and energy efficient protocol. The DATA phase of SSPIN is secured using an powerful and efficient RSA algorithm. Using SSPIN even the DATA is secured along with both ADV and REQ. With SSPIN, RSA algorithm is used to secure the DATA. RSA encryption algorithm is used to encrypt the data by the source node. And RSA decryption algorithm is used by the receiver in order to decrypt the actual data. Along with security, SSPIN is improved to conserve energy while data transmission.The experimental results show that the proposed system achieves better performance compared with existing system in terms of end to end delay, energy consumption, and throughput and packet delivery ratio.

In future, better and efficient algorithm can be used to secure the DATA with SSPIN protocol.

H.References

[1]Asha P.N, Dr. S.C Lingareddy, EmmanualRajarathnam, SantoshKowshik H.R, “Secure Protocol for Data Transmission in Wireless Sensor Networks”,ICC 2014 - COMPUTER NETWORKS AND SECURITY ISBN: 9789351072447

[2]https://en.wikipedia.org/wiki/Wireless_sensor_network#/issues

[3]C.Siva Ram Murthy and B.S.Manoj: Ad hoc Wireless Netwoks, 2nd Edition, Pearson Education, 2005.

[4]http://www.writing.ucsb.edu/faculty/holms/2E_motes_report.pdf.

[5]http://en.m.wikipedia.org/wiki/sensor_node#/issues

[6]Vikash Kumar, Anshu Jain and P N Barwal, "wireless sensor networks: security issues, challenges and solutions", IJICT, Vol. 4, 2014.

[7]Aashima single and ratikasachdeva, "Review on security issue and attacks in wireless sensor network, IJARCSSE, vol. 3, April-2013.

[8] Geetu,SoniaJuneja," Performance Analysis of SPIN and LEACH Routing Protocol in WSN", international Journal Of Computational Engineering Research (ijceronline.com)Vol. 2Issue. 5

[9] Jyoti, HarkeshSehrawat, DevenderSharma,"Energy Efficient M-SPIN Protocol", IJSER, vol.3,October-2012.

[10] nile.wpi.edu/NS/

[11]Liang Tang ,QiaoLiang Li "S-SPIN: A Provably Secure Routing Protocol for
Wireless Sensor Networks", 2009 International Conference on Communication Software and Networks