ISSN 2277-3061

A Survey of Wireless Sensor Network Routing Protocols based on SPIN

Surabhi Midha
M.Tech (CSE) Research Scholar
NIT, Jalandhar
surabhi.121210@gmail.com
Anand Nayyar
Assistant Professor
Department of Computer Applications & IT
KCL Institute of Management and Technology, Jalandhar, Punjab
anand_nayyar@yahoo.co.in

ABSTRACT

SPIN(Sensor Protocols for Information via Negotiation) comprises of a set of adaptive protocols that proficiently disseminate data in wireless sensor network(WSN).SPIN overcomes certain deficiencies associated with some of the data dissemination protocols & brings in more efficiency. WSNs have limited energy and hence efficiency of protocol has a significant impact on network's lifetime. Many protocols have been developed that are based on SPIN and are its modifications. This paper presents a survey on SPIN protocol and the various protocols devised which use SPIN as a base in one or another way.

Indexing terms/Keywords

Wireless sensor network (WSN); SPIN(Sensor protocol for Information via Negotiation); Data dissemination protocol; Routing.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATION JOURNAL OF COMPUTERS AND TECHNOLOGY
Vol. 13, No. 6
editorijctonline@gmail.com
www.cirworld.org/journals

1. INTRODUCTION

WSNs consist of sensor nodes that sense the environment and when networked, these aggregate the information that provides deeper insight into environment's view. The sensors usually relay this data collected to sink nodes that connect them to other networks like the internet. Users can obtain this data from the sinks. WSNs are constrained in terms of energy usage (since energy supply is limited), computing power and communication resources (limited bandwidth restricts communication between nodes).SPIN is a set of negotiation based protocols. It treats all nodes as potential sinks. The protocol has two main innovative ideas: Negotiation and resource-adaptation. The nodes negotiate with each other before transmitting information, so that only useful data gets transferred. For negotiation, nodes describe or name their data using meta-data. The nodes poll their resources prior to transmission. Each node has a resource manager that maintains track of resource usage. The nodes can cut back on some doings when energy's less [1].

2. MOTIVATION

WSNs are constrained in case of energy, computation power and inter-node communication. Data dissemination protocols are used to distribute the information amongst sensor nodes in a WSN. Hence, efficient protocols are needed for these. Conventional protocols, like classic flooding, suffer from certain drawbacks like implosion, overlap and resource blindness. Through negotiation & resource-adaptation, SPIN overcomes these deficiencies [1]. Thus, SPIN is a more efficient data dissemination protocol than the conventional ones. A lot many variants of SPIN have been developed which use this efficient protocol as their base.

All this depicts the importance of SPIN protocol and its use in devising many other protocols which draw on the lines of SPIN.

3. ORGANIZATION OF SURVEY

Section 4 gives an overview of SPIN. Section 5 consists of the survey of the various protocols based on SPIN. Section 6 discusses the conclusion and the future scope with respect to SPIN.

4. OVERVIEW OF SPIN

SPIN protocols are data-centric. The authors of SPIN [1], mention four protocols as a part of the SPIN protocols. Following are some details associated with these protocols:

SPIN Messages

- ADV: new data advertisement message containing meta-data.
- REQ: Request for data.
- DATA: data message

Meta-Data: SPIN doesn't specify meta-data's format which is considered to be application specific. However, if for sensor data X, x is the meta-data descriptor, the size of x in bytes ought to be lesser than size of X.

The following sub-sections discuss the four SPIN protocols.

4.1. SPIN-PP

SPIN-PP [1] is for point-to-point transmission. The protocol begins when a node advertises new data that it wants to disseminate. It sends ADV message to its neighbors. If the neighboring node needs the data, it sends REQ message. The initiator responds by sending DATA message containing the required data. Figure 1 indicates data dissemination in SPIN-PP. Node B request data from node A which had advertised its data to B. After receiving the data, B further advertises data to its neighbors. If node B has its own data, it can aggregate it with the received data. Every node needs to be aware of its one-hop neighbors only. SPIN-PP has been designed for lossless networks, but can be adapted for lossy or mobile networks.

4.2. SPIN-EC

SPIN-EC [1] incorporates energy-conservation heuristic to SPIN-PP protocol. If a node obtains some new data, it only starts the three-stage protocol (ADV-REQ-DATA), if it has enough energy to take part in full protocol with its neighbors. If node receives ADV message, it sends out REQ only if it has sufficient energy to send REQ & receive DATA.

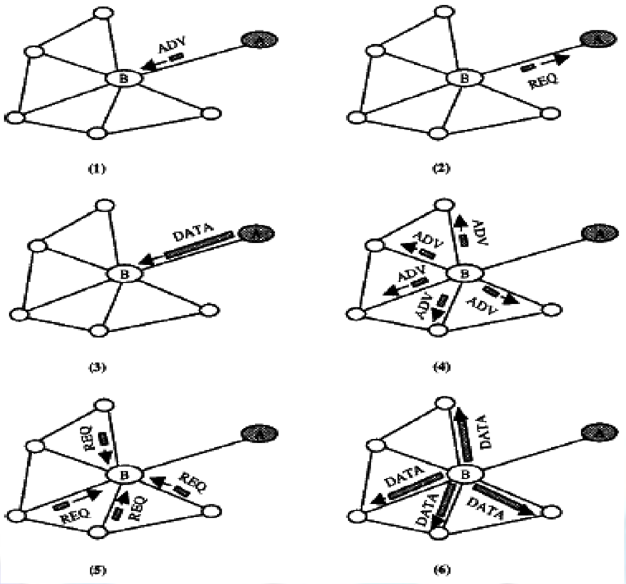


Figure 1: SPIN-PP protocol. Node A advertises its data to node B (1). Node B sends request for the data to A (2). After receiving data (3), node B sends advertisement to its neighbors (4), who further request back to B.

4.3. SPIN-BC

SPIN-BC [1] is for broadcast media. All the messages are transmitted to broadcast address and processed by all nodes in sender's transmission range. The example in figure 2 clarifies its operation.

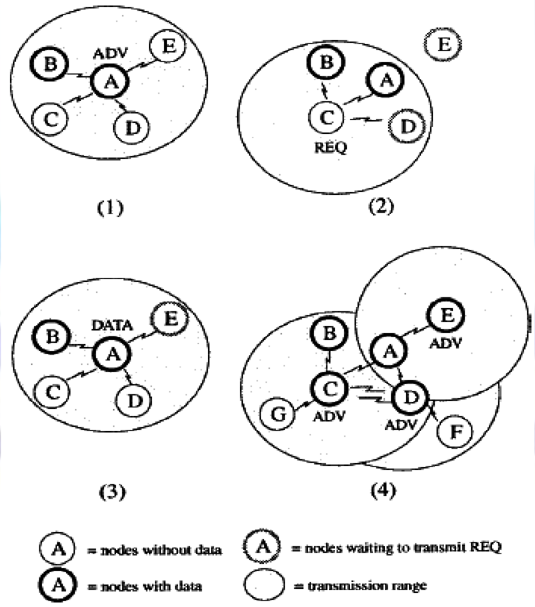


Figure 2: SPIN-BC protocol. Node A sends ADV message to its neighbors (1). Node C broadcasts a request with A mentioned as the originator (2), and suppressing D's request. After getting requested data (3), E's request too is suppressed, and C, D & E send advertisements to their neighbors.

4.4. SPIN-RL

SPIN-RL [1] is reliable version of SPIN-BC for lossy networks. Each node maintains track of which advertisements it happens to hear from which nodes, and if it does not get the data in certain time period after requesting, it re-requests. In SPIN-RL nodes restrain the rate at which they resend data. If node sends particular chunk of data in DATA message, it waits for pre-set time duration before answering any more requests for the same data.

5. SURVEY OF SPIN-BASED PROTOCOLS

5.1. SPIN-IT

SPIN-IT [2], (SPIN-Image Transfer) is a routing protocol for mobile & ad-hoc networks that allows efficient image retrieval on the basis of meta-data queries. SPIN-IT provides low bandwidth query based communication before image data's transfer. Its working is as follows:

Nodes request data by sending REQ message to broadcast address. All nodes in transmission range receive the request & keep account of the REQ messages received utilizing originating number identifier & unique request sequence number. New requests are re-broadcasted. Each node includes its source-ID to REQ header for setting up reverse path route. When request arrives at node having the needed data, it sends DATA message back to the node that requested it. The authors mention that in protocol's current implementation, its ROUTE-REPLY message that's used do that if requesting node gets multiple replies. It can select the 'optimal' source.
For simulation, authors use DSR (Dynamic Source Routing) [3] in which route-record is maintained in ROUTE-REPLY packet header. The "data" involved will be huge being image data, so shortest path routing might not be optimal. Routes can be formed based on stability or energy-constraints. SPIN-IT can flexibly use various types of routing.
Figure 3 clarifies the working of SPIN-IT.

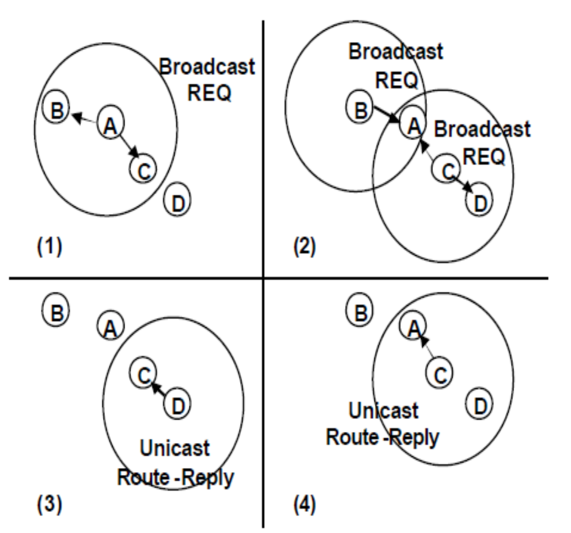


Figure 3: Node A sends REQ (1). Node B & C re-broadcast request. Node D has the needed data & sends ROUTE-REPLY back to C (3). Node C forwards ROUTE-REPLY to node A.

5.1.1. Alternative Protocol

Using centralized directory has been mentioned as an alternative to distributed method of SPIN-IT. Each node maintains route to central node (which maintains directory of all nodes and map of existing network topology).UPDATE messages are sent to central node, so that it can maintain the map. Nodes request data from central node which replies after performing directory look-up.
SPIN-IT has overhead of REQ packets flooded through network and ROUTE-REPLY from source to requesting node. For centralized scheme, overhead are UPDATE messages to central node, REQ & ROUTE-REPLY messages between requester & central node. The simulation results show that SPIN-IT is more proficient when new data's arrival at each node is higher than arrival of new requests for data at every node. Centralized scheme is better when number of updates is lesser.

5.2. Secure-SPIN

Secure-SPIN (Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks) [4] is secure extension of SPIN protocol. It follows a clustering-based SPIN approach, which divides nodes into different classes & each class does random selection of Cluster-Head (CH). Table 1 summarizes the notations used.

Table 1. Notation summary

Notation	Meaning
AC	Authentication code
Ks	Sink's privacy key
Kses	Session key
PSAC	Personal Sensor Authentication Code
Ki	Sensor node's privacy key
H()	Hash function
MAC	Message authentication Code

Its working is as follows:
Sink has list of all keys of nodes. Sink assigns CDMA code to each node. The task manager node gives Kses to all sinks in each session. Sink creates AC by encrypting Kses with sink's Ks & then output is hashed.

AC=H(EKs(Kses))

Sink sends AC to every node through CH. Each node creates PSAC using AC XOR its privacy key Ki.

PSAC=AC XOR Ki

The node that wants to be CH sends request message containing its PSAC. The sink authenticates the node by getting node's key as per its PSAC. If privacy key exists in its list, its authenticated to be legal node. Sink decides if the node can be CH or not. If it can, then sink transmits all nodes' privacy key in this class to CH.

In ADV message phase, the node that wants to share its data, encrypts ADV message with its PSAC and sends it to CH. The CH using sending node's private key & current AC decrypts the received ADV.

In REQ sending phase, the CH sends REQ message to source node.

In DATA message phase, if node wishes to transmit data to its CH, it XORs data with its PSAC, subsequently appends MAC and transmits packet to CH using its CDMA code. The CH upon reception of data, draws out Ki corresponding to the code and checks MAC to check data alteration. If data hasn't been altered, sink XORs data with Ki and current AC. Original data is obtained as a result.

The security protocol is applicable to sink-CH and CH-node communication. The authors mention that data authentication is achieved by encrypting ADV message with PSAC.As PSAC is generated by Ki, data confidentiality is ensured.MAC code ensures data integrity. Use of session key provides data freshness. Further CDMA technique improves secure communication.

5.3. S-SPIN

S-SPIN [5]**,** is secure extension of SPIN that uses the ADV-REQ-DATA message scheme. The authors use MAC (Message Authentication Code) to protect ADV & REQ messages. A cryptographic scheme for DATA message hasn't been specified, as its assumed to be application-specific. Its assumed each pair of neighboring nodes share a pair wise key.

In ADV Stage, once a node has new data, it sends ADV message to its neighbors. The initiator is denoted by symbol *S*. In the ADV message a MAC list (containing MAC in order of identifier list for its neighbors) and an integer *n* are included.

In REQ stage, the neighboring node, if in need of the advertised data, at first verifies the correctness of corresponding MAC in MAC list. MAC_{req} is created from pair wise key between S & destination (D) .If verified, REQ message (including the integer *n* & MAC_{req}) is sent to the initiator.

In DATA stage, *S* checks *n* and then checks MAC_{req}. If its verified to be okay, S sends DATA message to D.

5.4. ESPIN

In "Energy Conservative Wireless Sensor Networks for Black Pepper Monitoring in Tropical Area"[6],the authors propose ESPIN(Energy-efficient SPIN) to solve energy saving problem, with the idea of designing energy-efficient solution for monitoring black pepper agriculture in tropical areas. Figure 4 shows the system architecture considered. The system has 15 nodes, a base station that's connected to client terminal by Internet. The gathered data is sent to client terminal through GPRS.

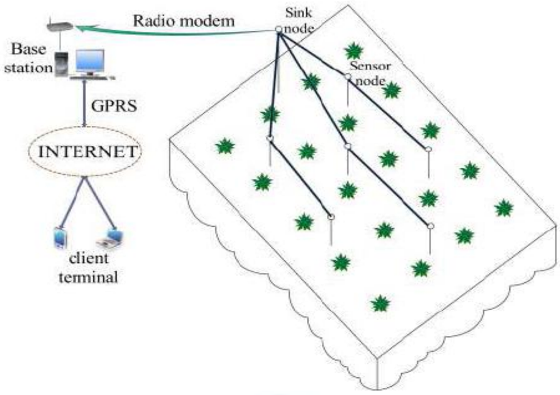


Figure 4: System Architecture

5.4.1. Phases in ESPIN

The phases involved are discussed below. If the requesting node is an intermediate one, then negotiation phase is repeated.

Distance discovery phase: Sink node broadcasts Startup packet containing hop as a field. Initial value of hop=1.On receiving Startup packet, a node stores this hop value as its hop distance from sink. It re-broadcasts start up packet after incrementing hop value by 1.On receiving Startup packets from multiple intermediate nodes, the node sets the distance to minimum hop distance out of all the received hop distances. This process is continued, until every node receives Startup packet.

Negotiation phase: Source node sends ADV message. The receiving node, checks if its nearer to sink or not as compared to node that has sent ADV message. If hop distance of receiving node is smaller than hop distance included in ADV message received, then REQ message is sent to sending node (which then sends DATA message).

Data transmission phase: This phase is same as in SPIN protocol.

5.5. SPMS

Shortest Path Minded SPIN (SPMS) [7], utilizes multi-hop model for data transmission & thus avoids exponential energy usage with distance. It keeps routing table for a zone, defined as node’s highest power level. Every node can create routing table with shortest path by employing Bellman-Ford algorithm. The Steps involved include:

- Node having data to share, advertises it.
- Neighbor needing that data, sends request message. If the node that sent the advertisement isn’t the next hop neighbor, it waits a certain amount of time before sending request.
- Data is sent to requesting node through shortest path (except in case of node failure).

In case of node failure, if previous node on shortest path fails, current node transmits request to node, from which it had initially got advertisement message. PRONE (Primary Originator Node) is maintained by each node ,which is energy-proficient data source while SCONE(Secondary Originator Node) is alternative node in case PRONE fails.

5.6. SPMS-Rec

SPMS-Recursive(SPMS-Rec) [8], has been designed to decrease energy usage for data dissemination when node or network links fail. In SPMS, if relay node, in request transmission stage discovers that its next hop is not available, it drops the packet. The destination on timing out tries alternate way of sending request. This energy wastage problem is solved by SPMS-Rec by enabling each intermediate node to detect broken route. It omits costly end-point timeouts by making intermediate nodes save transient state information, so as to find & recoup from failures locally. On receiving ADV message, an interested node doesn’t instantly send REQ but waits for a timeout. The destination D transmits REQ to PRONE (energy-wise preferred source to obtain data) via shortest path in multi-hop manner. SCONE is alternative source of data, if PRONE fails. The intermediate relay node, attempts sending REQ via shortest path and sets a timer. If timer times out, it transmits REQ via alternate way and begins another timer. Once this timer expires, it sends REQ directly or drops it. The source on receiving REQ, begins data transmission to destination D. Figure 5 clarifies data dissemination in SPMS-Rec.

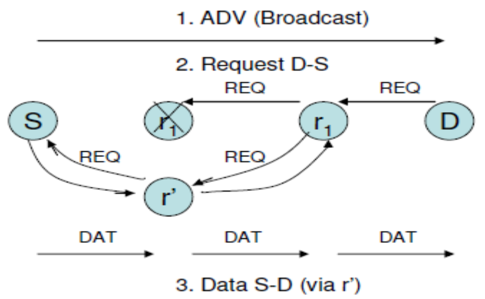


Figure 5: Data dissemination in SPMS-Rec

5.7. SPMS-Rec-RS

SPMS-Rec Request Suppression (SPMS-Rec-RS), [8] is an extension of SPMS-Rec mentioned along with SPMS-Rec. It decreases the redundant transmissions by suppressing redundant requests. Consider a node *P* that has initiated or forwarded a request for data from node *S.* During wait for data, it receives request for same data from node *Q.* Node *P* can opt for suppressing the forwarding of request if its already attempting to obtain that data or already possesses it. This protocol involves increased maintenance of state by intermediate nodes, since nodes have to maintain not only request packet forwarded, but also id of nodes whose requests have been repressed.

5.8. EDAS

Energy and Distance Aware data dissemination protocol based on SPIN (EDAS) [9], classifies nodes as primary nodes that transfer data to their zones or secondary nodes that receive data. Its working is as follows:

1. Primary node broadcasts an advertisement to its neighbors.

2. Neighbors receiving the advertisement set their timer inversely proportional to N^m.

3. The neighbor to time-out first, becomes primary node and broadcasts advertisement.

4. If the primary node broadcasting the original advertisement, hears advertisement message again, it transmits data to the node from which it got the message.

5. If a node which hasn't timed-out, receives advertisement message again, becomes the secondary node and sends a request message to node from which it received the message.

6. If a node hears the advertisement for first time, proceed to step 2.

7. All nodes repeat the above process, until they get the needed data [10].

5.9. CBS

Cluster Based SPIN (CBS) [11], is a combination of LEACH and SPIN. The network is organized into clusters. Nodes take turn to become cluster-head (CH), hence CHs "rotate" to balance energy usage in network. Its working is as follows:

After cluster creation, each node wanting to disseminate its data in network, advertise it to CH and then CH request for data. After receiving data, it advertises it to neighboring CHs. After data delivery to CHs is done then CH propagate data amongst its member nodes in SPIN style. All CHs do the same procedure. Hence data is disseminated in the whole network.

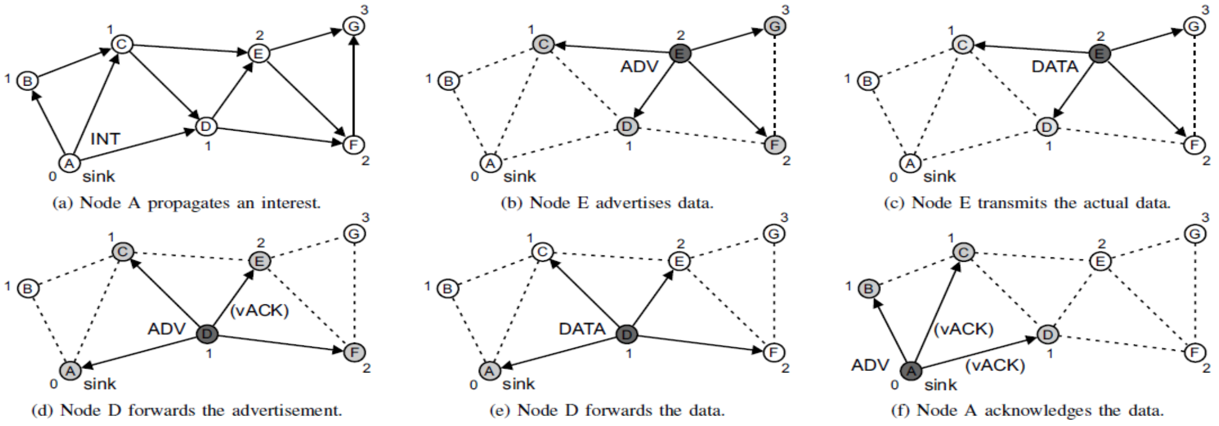
5.10. D3

D3 (Data-centric Data Dissemination) [12] unites the benefits of data-centric routing like SPIN and Directed Diffusion (DD) [13]. Following message types have been specified in D3:

- INT: Interest, which is propagated from a node to rest of the nodes. It describes what type of data sink is interested in. Depth of a node, which is its hop distance to sink, with respect to interest too is stored by each node.
- ADV: Data advertisement. A node which has data of some interest, it informs all neighbors about it using interest identifier & its depth.
- DATA: Data message

Its working is as follows:

The basic working is evident in Figure 6. Node A begins with transmitting data interest to all nodes via flooding. When node E has new data, it advertises it to its neighboring nodes(C, D, F & G) & a time slot for data transmission is affirmed. It sends data to interested neighbors(C & D) in the decided time slot. Node F & G, switch off their radios & ignore the data for its irrelevant for them. The series of advertisement & data transmission continues (Fig.6(d) and Fig.6(e)), till it reaches the sink (origin of interest). Forwarded ADV messages too are utilized as virtual acknowledgements (vACK).The reception of data is acknowledged by sink.



(a) Node A propagates an interest.

(b) Node E advertises data.

(c) Node E transmits the actual data.

(d) Node D forwards the advertisement.

(e) Node D forwards the data.

(f) Node A acknowledges the data.

Figure 6: The D3 protocol working

5.11. SPIN-I

SPIN-I [14] routing algorithm targets the “blindly forward” and “data inaccessible” problems of SPIN. It includes three phases, which are as follows:

Data broadcasting stage: When source node has new data, it broadcasts ADV message to its neighbors and starts a timer.

Data requesting stage: After neighbors receive ADV message, they estimate if they have sufficient energy to complete the work of three stages. If the node has the data broadcasted, it sets the REQ message flag as 1, returns its energy value to source node by REQ message. If neighbors don’t possess the data, but have sufficient energy to carry out the work, flag of REQ message is set to 0, and its sent back along with energy value to source node.

Data transmission stage: The source node filters the nodes whose flags are 0 and sends data to node with highest energy value. If they possess equal energy value, random selection is done. If the timer duration is greater than threshold, and all flags are 1,”data inaccessible” problem occurs. The source node chooses a node with highest value from its neighbor list and sends data necessarily. It then deletes the nodes from neighbor list, who don’t request data.

5.12. MS-SPIN

MS-SPIN [15] involves main features of SPIN and tackles the security issues as well. Its based on the concept of secure multicasting. Its assumed that each node has a private key, used to confirm authenticity. Table 2 summarizes the terminology used.

Table 2.Terminology summary

Terminology	Properties
Node	Sensor node that acts as source or sink or relay node.
Cluster Head	Nearest to Secondary Centralized Authority, has maximum energy, chosen by secondary CA, does IP address allocation to nodes, authentication of nodes, notifies secondary CA for successful address allocation.
Secondary CA	Fixed node, chooses Cluster Head (CH), does authentication of CH.Maintains information about all nodes in cluster,respond to main CA after secondary IP address allocation
Main CA	Main Centralized Authority that coordinates with secondary CAs, authenticates secondary CAs.
Find packet	Packet broadcasted to find out nearest secondary CA
Ack-packet	Packet sent by sink to source notifying about reception of initial packet
End-packet	Packet from source to destination, notifying end of data transfer.
Office	Main center for data storage

Its working involves the following phases:

1. Initial phase: Nodes try to figure out the *Secondary CA* using *Find-packet*, to which they have to connect.

2. Setup phase: Allocation of secondary IP addresses to nodes is accomplished in this. It further includes setting up *Main CA, Secondary CA* and *CH.* After Secondary CA setup procedure completion *Ack-packet* is sent *to Main CA* and similarly after CH setup completion, *Ack-packet* is transmitted to *Secondary CA.*

When the authentications fails, report is sent to *office, e.g.* in setting up *main CA,* if a *secondary CA* isn't authenticated using private key*, office* is informed about it.

3. Data Communication phase: If a node has some data, it'll send that prior to accepting new data.

On receiving *adv packet,* if node is in wait for some data it'll ensure if it wants the data. If it wants it or has to route it, then it decrypts the IP address (secondary IP address) and transmits request at secondary IP address. *End-packet* signifies end of data transmission.

On sending an *adv packet,* node adds its encrypted secondary IP address .It waits for request from neighbors. The source node multicasts the data at its secondary IP address.

5.13. M-SPIN

M-SPIN (Modified-SPIN) [16], aims at sending information only to sink instead of disseminating it in entire network. Its working is follows:

1. Distance Discovery: Each node finds its distance from the sink in terms of hops.

2. Negotiation: The source node transmits ADV message. Receiving node checks if its closer to sink or not as compared to node sending ADV message. This is the prime difference between negotiation phase of SPIN-BC and this protocol. If node's own hop distance is smaller than hop distance received in ADV message, it sends REQ to sending node.

3. Data Transmission: This phase is same as SPIN-BC.

5.14. SPIN-Pi

SPIN-Pi [17] takes advantage of the plug-in nodes and tends to improve WSN routing protocol in WHSN(Wireless Home Sensor Networks).Its working is as follows:

The source node broadcasts ADV packets to neighboring nodes. The plug-in nodes of neighbors send request (REQ).If no REQ is received in certain time period, the source re-broadcasts ADV. After neighbors get its ADV, they send REQ in original manner. The use of plug-in nodes only, for first receipt of ADV, reduces energy consumption.

6. CONCLUSION AND FUTURE SCOPE

SPIN protocol is a popular data dissemination protocol that overcomes problems like implosion in classic data dissemination protocols (e.g. flooding). A number of modifications of SPIN have been manifested in this survey, an indication of its utility. Thus the SPIN protocol and its variants can be efficiently used in WSN.As mentioned in [14], SPIN is apt for small or medium scaled networks. Though SPIN-I targets this point, scope for further modification of SPIN to suit large-scaled networks exists. Similarly, as observed, SPIN as such doesn't provide security mechanisms along with it, hence leading to development of protocols that add security aspect to SPIN [4, 5] .Possibility to modify SPIN and incorporate more security features does exist. So does, the possibility of optimizing its energy consumption, which is an implied prospect for any routing protocol in WSN.

REFERENCES

[1] Kulik, Joanna, Wendi Heinzelman, and Hari Balakrishnan. "Negotiation-based protocols for disseminating information in wireless sensor networks." Wireless networks 8.2/3 (2002): 169-185.

[2]Woodrow, Edward, and Wendi Heinzelman. "SPIN-IT: a data centric routing protocol for image retrieval in wireless networks." Image Processing. 2002. Proceedings. 2002 International Conference on. Vol. 3. IEEE, 2002.

[3] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." Mobile computing. Springer US, 1996. 153-181.

[4] Xiao, Debao, Meijuan Wei, and Ying Zhou. "Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks." Industrial Electronics and Applications, 2006 1ST IEEE Conference on. IEEE, 2006.

[5] Tang, Liang, and QiaoLiang Li. "S-SPIN: A provably secure routing protocol for wireless sensor networks." Communication Software and Networks, 2009. ICCSN'09. International Conference on. IEEE, 2009.

[6] Li, Jing, and Chong Shen. "Energy Conservative Wireless Sensor Networks for Black Pepper Monitoring in Tropical Area."

[7] Khanna, Gunjan, Saurabh Bagchi, and Yu-Sung Wu. "Fault tolerant energy aware data dissemination protocol in sensor networks." Dependable Systems and Networks, 2004 International Conference on. IEEE, 2004.

[8] Khosla, Ravish, et al. "Performance Comparison of SPIN based Push-Pull Protocols." WCNC. 2007.

[9] Seo, Jaewan, et al. "EDAS: energy and distance aware protocol based on SPIN for wireless sensor networks." Transactions on Computational Science VI. Springer Berlin Heidelberg, 2009. 115-130.

[10] Marina L. Gavrilova, C. J. Kenneth Tan. Transactions on Computational Science VI.Springer,2009.Google books. Web.16 Apr. 2014. http://books.google.com

[11] Tabibzadeh, Masoud, Mehdi Sarram, and Mohammad Ghasemzadeh. "Adaptable Protocol for Time Critical Information Dissemination via Negotiation in Large Scale Wireless Sensor Network." Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on. Vol. 2. IEEE, 2009.

[12] Ditzel, Maarten, and Koen Langendoen. "D3: Data-centric data dissemination in wireless sensor networks." Wireless Technology, 2005. The European Conference on. IEEE, 2005.

[13] Intanagonwiwat, Chalermek, Ramesh Govindan, and Deborah Estrin. "Directed diffusion: a scalable and robust communication paradigm for sensor networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000.

[14] Jing, Luwei, Feng Liu, and Yuling Li. "Energy saving routing algorithm based on SPIN protocol in WSN." Image Analysis and Signal Processing (IASP), 2011 International Conference on. IEEE, 2011.

[15] Dhurandher, Sanjay K., et al. "An Efficient and Secure Routing Protocol for Wireless Sensor Networks using Multicasting." Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom). IEEE, 2010.

[16] Rehena, Zeenat, Sarbani Roy, and Nandini Mukherjee. "A modified SPIN for wireless sensor networks." Communication Systems and Networks (COMSNETS), 2011 Third International Conference on. IEEE, 2011.

[17] Tan, Ruochen, et al. "Improving routing protocols of WSN in WHSN." Communication Technology (ICCT), 2012 IEEE 14th International Conference on. IEEE, 2012.