# A POWER-EFFICIENT SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

IMAN ALMOMANI Member IEEE, EMAD ALMASHAKBEH
Computer Science Department
King Abdullah II School for Information Technology (KASIT)
The University of Jordan
AMMAN 11942 JORDAN
i.momani@ju.edu.jo, e.mashakbeh@gmail.com

*Abstract:* - Wireless Sensor Network (WSN) is a hot research area due to its use in many military and civilian applications. WSN consists of distributed small, low power and limited capabilities sensors that are scattered in the network field to sense different parameters in the environment. The sensed data will be sent to a more powerful node called sink node (Base Station). The sink node is usually connected to a power supply and is used to process the data and to connect the sensor network to other networks like the Internet. One of the major challenges in such networks is how to provide connection between the sensors and the sink node and how to exchange the data while maintaining the security requirements and taking into consideration their limited resources in terms of energy, memory and available bandwidth. In this paper a power-efficient, secure routing protocol is proposed to help managing the resources in WSN networks. The proposed protocol is a hybrid of two major categories of protocols in WSNs, namely tree-based and cluster-based protocols. The proposed protocol is combined with a Fuzzy Logic inference system to aid in the selection of the best route based on a combination of three factors: the path length, the available power and the node reputation resulted from the Intrusion Detection System (IDS). The proposed protocol uses three Fuzzy Inference Systems (FIS) that are implemented in two tiers. Tier one will choose the best route in terms of shortest length and high power. Tier two provides a security assessment for the selected route.

*Key-Words:* - Wireless Sensor Network (WSN), Security; Routing, Power Saving, Clustering, Intrusion Detection System (IDS), Fuzzy Logic

## 1 Introduction

Wireless Sensor Network (WSN) consists of small devices called sensors that have the capability to sense specific parameters of the surrounding environment [1] [2] [3] [4]. Such kind of wireless networks is used in many applications [5] [6] nowadays because of their features, like coverage, easy of deployment, cheap, etc. This makes WSN the best network option to use in many scenarios. On the other hand, this type of network has many constraints because of the limited resources in these small devices; such as Energy and memory limitations.

A basic part in the configuration of such networks is how sensors exchange data; a specialised routing protocol is needed to control transmission phase. Designing such a routing protocol for these limited-resources devices which sometimes deployed randomly is a big challenge for researchers in this area. Many protocols were developed for this purpose but few of the proposed solutions were designed to consider both the limited resources and the security constraints at the same time [1].

This paper proposes a new protocol, which is a hybrid of two basic categories in WSN; tree-based routing protocol and cluster-based routing protocol to take the advantages of the two protocols and merge them in one new protocol. The new proposed protocol provides secure connections between the sensor nodes and the sink node with minimum cost in terms of delay and power consumption.

The rest of this paper is organised as follows; section 2 reviews related work. Section 3 discusses the proposed protocol while evaluation of the protocol is presented in section 4. Section 5 concludes the paper and presents avenues for future work.

## 2 Related Work

Routing protocol is an important aspect and hot research area in WSN. The limited resources in sensor devices put the researchers in an unenviable position as this introduces major challenges for

researchers to create or define a suitable routing protocol. Many researchers proposed ideas and protocol solutions for this useful network that is characterised by its limited resources. .

The previously proposed protocols focused either on energy efficiency or on security, while a very few attempts focused on achieving the two majors concepts together fairly.

In this section, a review of existing protocols that are related to the new proposed protocol is presented. Some of these routing protocols are tree-based the others are cluster-based. The design criteria and goals for a routing protocol that are followed by sensor networks researchers [3]: security, energy efficiency, simplicity of the algorithm with small computation and small footprint, robustness of the connection, scalability, location-based, self topology construction and definition and Mobility. Most of the work presented in the literature had focused on the energy efficiency and few of them had achieved most of the above goals.

Tree based routing protocol proposed in [7] constructs a tree between nodes in order to send messages to root using parent-child links, two parameters to control the construction; maximum number of children a node can have and maximum depth the tree can have. As number of children increases (decreases) the depth will decreases (increases). They use an address scheme that uses the idea of binary search tree to assign logical network addresses to the nodes.

Park and Jung [8] proposed a plus tree routing protocol that utilizes the neighbors' links in order to find a shorter path than using only parent-child links. To transmit a message to the destination, plus tree first constructs the parent-child links and after tree construction each node broadcasts its ID to its neighbors and constructs the neighbor table that will be used to find the shortest path, otherwise the parent-child links will be used. Plus tree solve shortest path and link failure, but without considering energy consumption.

TBRP [9] proposed by Zeynali and others tries to balance the energy load among all nodes. TBRP introduce new clustering factor for cluster head election and also a fuzzy spanning tree for sending aggregated data to the sink.

The authors in [10] proposed another improved routing protocol called ImpTR for zigbee networks. ImpTR enhances the tree routing by constructing a neighbor table that can be used to transmit the message through neighbors' links if the path will be shorter than the parent-child links. ImpTR assign a block of addresses to each router so that each router can assign an address to its children (routers or sensors) and by performing some processing the node can choose whether to transmit the message using neighbors' links or parent-child links. However, ImpTR did not consider the energy balancing between nodes.

Shah and Rabaey [11] proposed Energy-aware reactive routing protocol that increases the survivability of networks using sub-optimal paths occasionally. To achieve this, multiple paths are found between source and destinations, and depending on the energy metric, each path is assigned a probability of being chosen. Every time data is to be sent from the source to destination, one of the paths is randomly selected depending on the probabilities. The protocol has three phases: first, setup phase that finds all the routes from source to destination and their energy costs. Second, data Communication phase or data propagation in which data is sent from source to destination, using the information from the earlier phase, and paths are chosen probabilistically according to the energy costs that were calculated earlier. Finally, route maintenance is used to keep all the paths alive.

Secure and Energy-Efficient Multipath (SEEM) is a routing protocol which is an edited version of multipath routing protocols [1]. The difference lies in the method of establishing, selecting, and maintaining the routing path. In SEEM a Base Station (BS) plays a server role that means it aggregates, calculates data, selects and maintains routing paths, and energy consumption. Sensors collect data from the surrounding environments; send data to the BS, and forward packets.

In topology construction phase, BSs broadcast two types of messages Neighbour Discovery (ND) message which starts to discover the neighbours list for each node, the second message is Neighbour Collection (NC) message, the purpose of this message is to help nodes recognise neighbours that were not collected by ND message, and let nodes set a timer to send back the neighbours list to the BS. After collecting the neighbours' information the BS has a general view of the topology of the network, therefore it can generate a weighted sub-graph.

In the second phase, data transmission phase, the BS broadcasts Data Enquiry (DE) message to a specific node. Each receiving node checks if it is the intended recipient for this DE. If not, it rebroadcasts it. If yes, the node sends Data Enquiry Reply (DER) message to the BS, then the BS calculates the shortest path using a modified version of Breadth First Search (BFS). After finding the path, the BS sends Route Reply (RR) packet to this specific node using the selected path. Upon receiving the RR

packet, the node knows which path it can use to communicate with the BS, to confirm the receiving of the RR packet the node sends an Acknowledge (ACK) message which also contains the number of data packets that will be sent using the same path.

Even though it is true that SEEM has strength points, but at the same time there are some weaknesses in achieving the power efficiency concept in sensors nodes, there are three reasons behind this. The first reason is that in topology construction phase there are too many messages that are sent and with a huge number of nodes this is power consuming. The second reason is that although SEEM defends selective forwarding attacks but if the compromised nodes still forward packets, power consuming will happen during the defending, therefore SEEM needs to check the energy level not only by calculating the transmitted packet. The third reason is that there is an overhead in exchanging some extra messages which can be deleted for example in neighbour discovery when a message does not arrive using two levels of messages, discarding the message would be a better option.

Low Energy Adaptive Clustering Hierarchy (LEACH) protocol [12] is a cluster-based protocol that divides the sensor nodes into cluster formation, by selecting some nodes as Cluster Heads (CHs) and the remaining nodes are selected as clusters members [4]. Choosing the CH is based on certain criteria like the amount of power on this node and how many nodes around this CH elected it (a special equation is used for selecting the CH) [4]. The CH role is to distribute the load and energy consumption in the network. In LEACH the CH nodes aggregate and compress data coming from sensors in its group and sends the aggregated data packet to the BS in order to reduce the amount of information that must be transmitted to the BS. More information about placement of the CH can be found in [13].

Authentication Confidentiality (AC) is a cluster-based secure routing protocol for WSN [2]. It uses the clusters that are generated by LEACH. The idea behind this protocol is to decide how to provide LEACH with authentication and confidentiality characteristics without considering the power consumption. In other words, this protocol is used when satisfying the security requirements is more important than power consuming.
The problem here is that when a protocol focuses on a certain problem (achieving a certain criterion), this lead to contradiction or to weaken other concept(s). The weaknesses of AC is energy consumption, even despite the waste in the energy, internal attacks [14] problems was not completely solved.

# 3 The Proposed Protocol

In this paper a new routing protocol is proposed, this protocol is basically a hybrid of the tree-based routing protocols and the cluster-based protocols. The idea of the new protocol is to take advantages of these two basic protocol categories. The new protocol is divided into 4 stages:

1. Cluster formation.
2. Exchanging messages phase.
3. Drawing a directed weighted graph.
4. Selecting the best path.

Some assumptions are made regarding the new protocol:

- LEACH protocol is used for the purpose of WSN clusters formation.
- Each node and cluster head has its own ID. These IDs are known by the BS which also binds the ID with the main functionality of the node.
- Each node has its own public, private keys and the BS knows all nodes' public keys.
- Energy consumption for each task is known, like energy consumption for transmission task.
- All nodes have the same energy consumption for the same task.
- The BS assumes a certain level of power for each node when it draws a weighted graph.
- Each packet that is sent to the BS contains the energy level of the sensor node.

## 3.1 Stage 1: Cluster Formation

In this step all nodes are grouped in clusters form, where one hop is used between each node and the cluster head. LEACH protocol will be used in cluster formation as shown in Fig. 1.

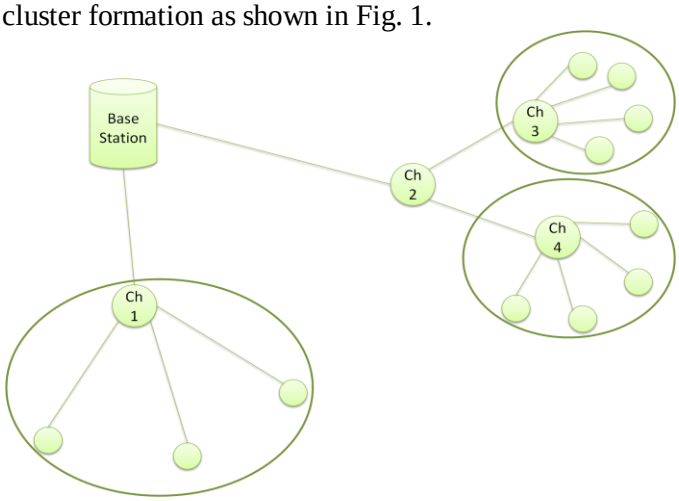



**Fig. 1** Hybrid Model (Cluster-based and Tree-based)

### 3.2 Stage 2: Exchanging Messages

In this stage the BS starts exchanging messages in order to draw the directed and weighted graph in the next stage.

Since the network consists of sensor devices with limited resources, this means message exchanging should not consume the power and the memory as much as possible, therefore, in this stage the proposed protocol decreases the number of required messages when compared to SEEM to two messages only Sensor Neighbour (SN) message and Sensor Neighbour Reply (SNR), as following:

1. The BS broadcast SN packet. Each node rebroadcast this packet and puts itself as a previous hop. When a node receives this packet for the first time, it generates a neighbour list, then it puts the node's name that in the previous hop in its neighbour list (this list has an ascending order), then it checks if this packet sequence number is in the packet sequence number list or not, if yes it drops it, if not, the node puts its name in the previous hop and rebroadcasts the packet, and sets a variable set timer with random number to broadcast after this time a SNR packet which contains the neighbour list as shown in Fig. 2.

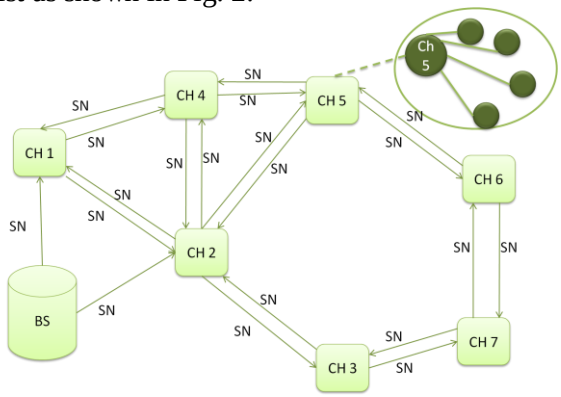



**Fig. 2** SN packet broadcasting by BS

The following example will illustrate this step. We need to clarify that each node in the above and following figures represents cluster head.

Assume that SN packet is broadcasted by the BS and arrived to node 3 (CH 3) from node 2, node 3 will act as follows:

- Generate the neighbour list
- Insert the previous hop node name into the list which is here 2.
- Checks the packet sequence number (assume its number here 1 since it is the first packet) and since this is the first time the packet arrived to node 3 it inserts the sequence number in the packet sequence number list and then rebroadcasts the packet.
- Node 3 sets the timer to broadcast the SNR packet. This timer will be set will be set based on criteria that is measured by simulation experiments.
- Node 3 will do the same steps when it receives the packet from node 7.

2. Each node receives the SNR packet checks to see whether the node that sent the SNR packet is in its neighbour's list. If not, it adds this node to the list, then it checks the sequence number of the packet if it does exist in the packet sequence number list, if it exists, then it drops the packet and does not rebroadcast it, to avoid the loop problem. If the sequence number does not exist, the node puts its name in the previous hop and rebroadcast the packet as shown in Fig. 3.

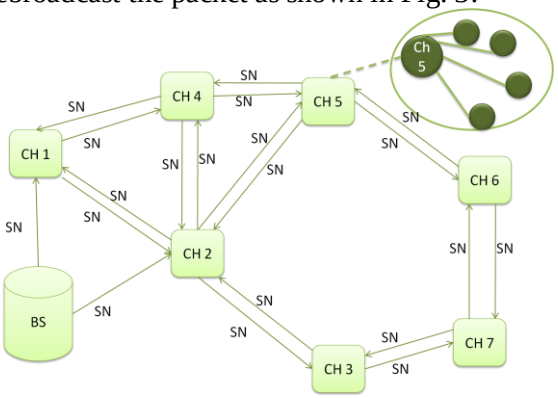



**Fig. 3** Replying with SNR packet from each node

To clarify this point the previous example will be completed:

- Node number 7 broadcasts the SNR packet.
- SNR packet arrives to node number 3, at this time node number 3 checks if node number 7 in its neighbour list or not, and here if it is not so, node 3 adds node 7 to its neighbour list.
- Then node number 3 checks the packet sequence number (assume its number is 2 since it is the second packet) and rebroadcast the packet.

### 3.3 Stage 3: Drawing the directed weighted graph

This stage starts after the SNR messages arrived to the BS, thus it will start by drawing a weighted and directed graph for the network. According to the above assumptions, we assume each node will start with total energy 6000m/w.

As shown in Fig. 4, the edge weight is the power for the node that the edge out from, edges that out from the BS have infinity power because the BS is not limited with power.

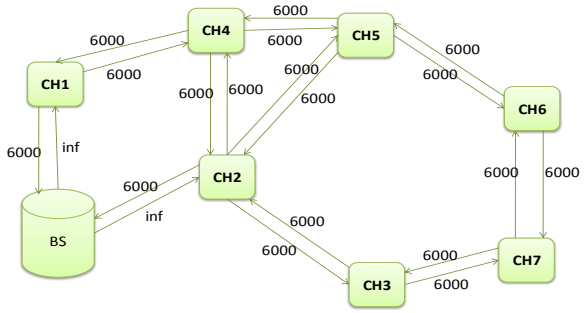



**Fig. 4** Weighted graph Generation by BS

### 3.4 Stage 4: Select the best path

In this step the BS selects the best path for the corresponding node. A fuzzy logic will be used to selects the path not only according to absolute shortest path, but it will also consider the remaining energy and the results values that output from the Intrusion Detection System (IDS).

That means if there is a node in the shortest path with a remaining energy and/or the level of the IDS less than the required level, then this path will not be chosen as a best path, but if the algorithm does not find any path with the required level then this level will be decreased based on the requirements of the sensor network itself. The path will be selected in cluster head level; in cluster level the best path is from/to the node to/from the cluster head.

After selecting the path, the BS sends Selected Route (SR) packet to the corresponding node (CH) using the selected path. SR packet contains the CH ID and the node ID, each node (CH) receives this packet asks itself if it is the intended receipt of this packet or not. If not, the node forwards the packet using the selected route. If yes, the corresponding node (CH) knows the communication path with the BS and sends ACK message for this packet to the BS using the same path. This packet includes the energy level of this node and the number of packets that will be sent to the BS, to let the BS knows whether packet loss occurred or not. If the ACK message did not arrive after a certain amount of time, BS runs the algorithm again. Fig5. shows the pseudo code of the propose protocol.

The proposed protocol achieves three major security requirements: authentication, authorization, and integrity. These requirements are achieved as each message sent except SN packet (the reason of including the SNR packet in this process is to ensure that the received neighbour list is correct since all the network graph will be drawn based on these lists) contains the data and the signature. Encryption technique that is used in forming the signature of the node requires less computational power and memory. Such encryption techniques are based on what is called Elliptic Curve Cryptography [15].

The BS receives the message from the node then it decrypts the message using the public key of this node. As mentioned before, the BS has all nodes' public keys. Then BS compares the power level that is encrypted in the message with the assumed power level that is calculated by the BS. This level is calculated based on the number of sending/receiving packets from this node. Sometimes, this value does not fit exactly the sent value but it should be within a specific range from it. This range plus minus is determined based on the experiments, taking into account the node role if it is CH or member in the cluster. After comparing the power values and finding that they are accepted, the BS accept the information. Otherwise, it will send a warning message for the administrator and for all nodes in the compromised path to freeze any sending or receiving actions.

The proposed protocol not only achieves the above security requirements which are classified as prevention mechanisms that trying to protect the system from the external attackers that are not authorised or authenticated to access the system resources but it also provides the following:

- Detection mechanism: that is proposed in this paper to protect the network from the internal attackers that are authorised and authenticated to access the network resources. This technique called Intrusion Detection System (IDS) that will monitor the sensors themselves and report their misbehaving actions.
- Defending sinkhole or wormhole attacks: Because the BS selects the path, so the compromised node cannot stay in the path for long time.
- Defending selective forwarding attack: From the definition of this type of attack, it can be concluded that it consumes power. To solve this problem the BS compares the energy level that it assumes or calculates with the energy level that comes from the node, if it is the same or nearby therefore, there is no problem, but if the difference is bigger than the expected range then the BS knows that there is a compromised node in the path and it sends a warning message through this path to inform the nodes and sends a warning message to the administrator.

**Base Station side:**

1. Broadcast (SN)
2. Gathering (SNR)
3. For each node (Generate table for each node contains the node ID, function, neighbor list, power level)
4. Calculate Hash (data packet) = digest
5. IF digest != Decryption $_{PubKeySigner}$ (Signature) THEN
6. Send (Warning Msg to the Admin) AND STOP
7. ELSE {

// emptied the contents of the received SNR packet

8. Classify (SNR)
9. Draw graph
10. Route= run FL
11. Send SR (route)
12. Set timer = "VAL"
13. IF timer expires THEN ACK=false
14. IFACK=TRUE then{
15. timer = Infinity // this means no need for execute BFS algorithm another time
16. VALIDATE // the received packet
17. Decrease (power level)
18. IF !Compare (p, power come from packet) THEN
19. // (p) power level that is filled in the BS tables
    a. {Send warning (route, admin)
    b. route2= run FL
    c. IF Compare (route, route2) THEN Delete route } }
20. ELSE IF timer = 0 THEN route = run **FLS (Fuzzy Logic System)**
21. If (ACK arrived) THEN{
22. VALIDATE
23. Decrease (power level)
24. If !Compare (p, power come from packet)
25. {Send warning (route, admin)
    a. route2= run BFS algorithm
    b. if compare (route, route2) THEN Delete route}}}

**Node side:**

1. IF(Arrived packet=SN or SNR) THEN{
2. Generate neighborlist
3. IF ! (prev-hop, neighborlist){
   Add (Prev-hop, neighbor-lst)
   IF !(PktSeqNo,pkt-seq-no-table) THEN{
   Add(PktSeqNo,pkt-seq-no-table)
   Rebroadcast }
4. ELSE Drop }
5. IF(Arrived packet =SR or ACK or data) THEN{
6. IF !(PktSeqNo,pkt-seq-no-table) THEN{
   a. Add(PktSeqNo,pkt-seq-no-table)
   b. Forward (route) }
7. ELSE Drop }
8. IF(send packet) THEN{
9. P= left-power
10. Generate (packet)
11. IF !(generate(packet=SN or SNR)) THEN Add (packet, p)
12. IF (SN) THEN broadcast
13. IF (SNR) THEN{
    a. Decrypt the signature
    b. Broadcast}
14. IF (SR or ACK or data) THEN{
    a. Decrypt the signature
    b. forward (route) }

**Fig. 5** Psuedo-code of the proposed protocol

# 4 Protocol Evaluation

To evaluate the proposed protocol, MATLAB Fuzzy Logic (FL) Inference System is implemented [16] [17] [18]. The purpose of integrating FL with the proposed protocol is to allow taking the effect of not only the energy level and the shortest path to choose the best route, but it also takes into consideration the security level of this selected route.

The proposed protocol uses three Fuzzy Inference Systems (FIS) that are implemented in two tiers as shown in Fig. 6. In tier one, the route selection FIS will combine both the effect of shortest path in terms of number of hops and the power level in order to choose the most efficient route. The other FIS in this tier represents the IDS system that provides a security feedback about the selected route and how much it is secure. These two FISs, the Route Selection systems and the IDS system, are completely independent systems. Each system has its own criteria (inputs) and applies different functions as will be explained in the following subsections.

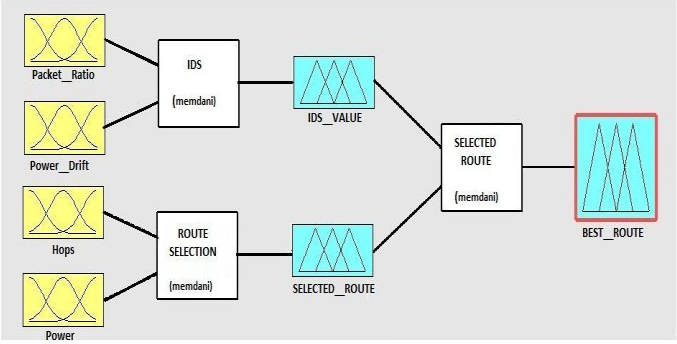



**Fig. 6** Two Tier Fuzzy System for selecting the efficient secure route

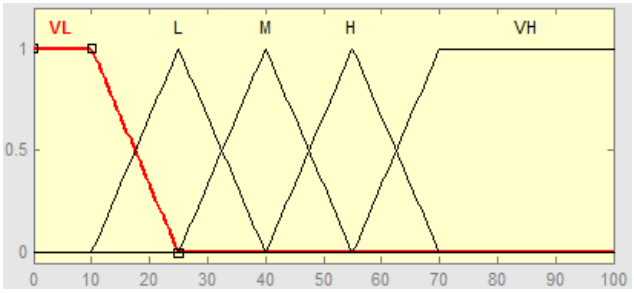
The outputs of the two fuzzy systems in the first tier are combined to feed the input of the fuzzy system in the second tier. The output of the fuzzy system in the second tier will provide the most secure-efficient route.

## 4.1 Intrusion detection System (IDS)

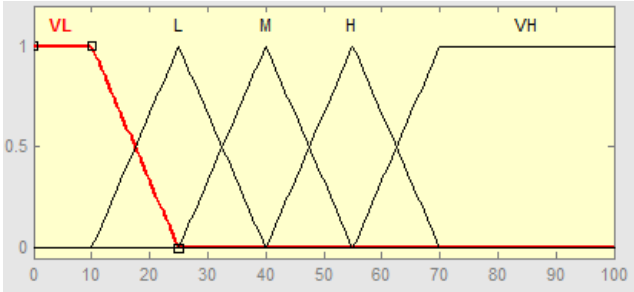
This system has two input parameters which are the packet ratio and the power drift. The packet ratio is percentage of the packet sent by BS to the packet received by BS, in terms of data packets, and it is computed as follows:

$$\text{Packet ratio} == \frac{\text{No.Pkt}_{\text{Sent}}}{\text{No.Pkt}_{\text{Rcvd}}} * 100\ \%.$$

The *No.PktSent* is the number of packets that are sent by the base station, in terms of orders, to the target node through a specific route. The *No.PktRrcvd* is the number of packets received by the BS from the same node and through the same route. This ratio gives an indication regarding the existence of compromised node(s) on that route. The BS should receive reply packets equal to the number of request packets it had sent. For example if the BS sent ten requests for getting data from node *x* on route *Rx*, then BS should receive about ten replies and the packet ratio will be 100 % which means the BS receives exactly the same number of packets it sends. Nevertheless, when this percentage goes down, the possibility of having internal attacker increases and in such scenario another parameter is needed which is the Power Drift to ensure this possibility. Fig. 7a shows the fuzzy membership for the Packet Ratio over the route which varies from Very Low (VL) to Very High (VH). The high the ratio is the high the value will be assigned. For example, if the packet ratio is low (10%), that means the number of received packets is larger than the number of packets sent by the BS. This case could be a sign for the existence of an internal attacker which sends un-required data to waste the energy of the sensor network.




**a)** Fuzzy membership for the Packet Ratio over the route.




**b)** Fuzzy membership for the Power Drift over the route.

**Fig. 7** Fuzzy Membership Functions for the IDS

The Power Drift is computed as the percentage of difference between the power level value included in the signed packet sent by the node to the BS and the

power value calculated by the BS for this node knowing the original power the node started with and how many packets are sent and received by this node and how much these packets cost it in terms of energy. Fig.7b depicts the Fuzzy membership for the Power Drift over the route which also varies from Very Low (VL) to Very High (VH). The higher the Power Drift value is, the higher the value will be assigned. For example if the packet ratio was 100% that means the number of requests equal the number of responses and in this case the power consumed by this node could be calculated by the BS. If this value differs from the power level sent and signed by node in a big way (VH power drift) this indicate that the node is providing incorrect power level for attacking purposes.

The calculated values of both Packet ratio and the Power Drift will be entered into the FIS of the IDS and by using the IF-THEN table or rules, the output will be calculated and a value will be assigned for the specified route varies from VL to VH as shown in Table 1.

**Table 1.** Fuzzy IF-THEN rules for the IDS

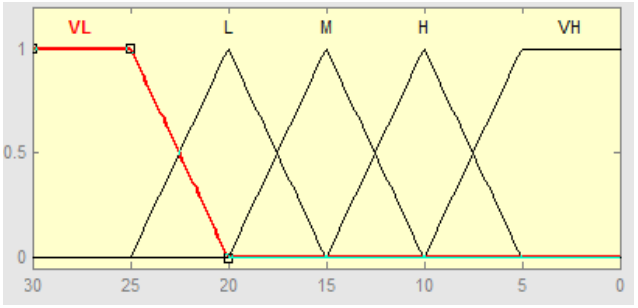
| Power Drift \ Packet Ratio | VL | L | M | H | VH |
|---|---|---|---|---|---|
| **VL** | VH | H | M | L | VL |
| **L** | VH | H | M | L | VL |
| **M** | M | L | M | L | VL |
| **H** | VH | H | H | M | L |
| **VH** | VH | H | M | M | M |

For example if the Packet ratio is VH and the Power Drift is VL that means the possibility of having compromised nodes on this route is Very Low (VL). On the other hand, if the Packet Ratio is VL and Power Drift is VH, then this route is not secure and the possibility that it is compromised is Very High (VH). The rest of the table is self explanatory.

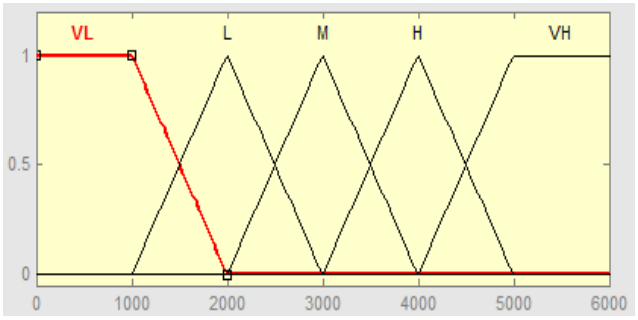
## 4.2 Route Selection

This FIS is created to select the best route in terms of the shortest path (number of hops) and the power level. Fig. 8a shows the fuzzy membership for the hop count that is ranged between 0 and 30 hops mapped into five different fuzzy memberships Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH). Increasing the number of hops implies a decreasing on the assigned value and vice versa. Therefore, the VH value is assigned to the short paths ranged from 1-5 hops where the VL value is assigned to the long paths with more than 25 hops.

Fig. 8b shows the fuzzy membership for the actual power of the sensor nodes which takes values between zero to six thousands and it is in measured in Milli-watt. VL for example is assigned to sensors with actual power between (0-1000m/w) while VH is assigned to sensor nodes with actual power ranges from 5000m/w to 6000m/w.




a) Fuzzy membership for hop count (0-30)




b) Fuzzy membership for the actual power (0-6000m/w)

**Fig. 8** Fuzzy Membership Functions for the Route Selection System

The calculated values of both hop count and the actual power level will be entered into the FIS of the Route Selection and by using the IF-THEN table or rules, the output will be calculated and a value will be assigned for the specified route varies from VL to VH as shown in Table 2. FIS is interested to choose the route which has the highest average power and with minimum number of hops. As can be noticed in Table 2, the route with VH value in terms of hops (shortest) and VH value in terms of power is classified as VH route that should be selected.

**Table 2** Fuzzy IF-THEN rules for the Route Selection System.

| Power \ Hops | VL | L | M | H | VH |
|---|---|---|---|---|---|
| VL | VL | L | L | M | M |
| L | VL | L | L | M | M |
| M | L | L | M | M | H |
| H | L | M | M | H | H |
| VH | H | H | VH | VH | VH |

## 4.2 Best Secure Route

This represent tier two of the FIS applied by the proposed protocol. It depends on the outputs of tier one FISs which are the IDS and Route Selection. It provides a security assessment for the selected route. It is studying how much this route that has been chosen based on its length and power is secure.

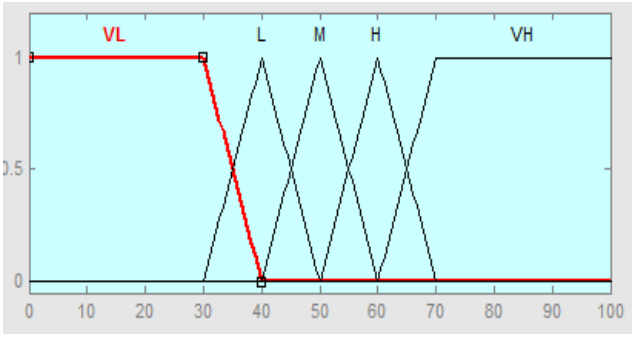
Fig. 9a shows the Fuzzy membership for the IDS as an output form the IDS FIS and as an input to the Best Secure Route System. For example, if the IDS FIS gives a 90% for a specific route. That means, the possibility that this route is compromised is Very High (VH) and so on.

Fig.9 b shows the Fuzzy membership for the best Route Selection as output from the Route Selection FIS and as an input to the Best Secure Route System. For example, if the Route Selection FIS gives 100% for a specific route. That means, this route is the best in terms of length and power and therefore it is assigned a Very High (VH) value.

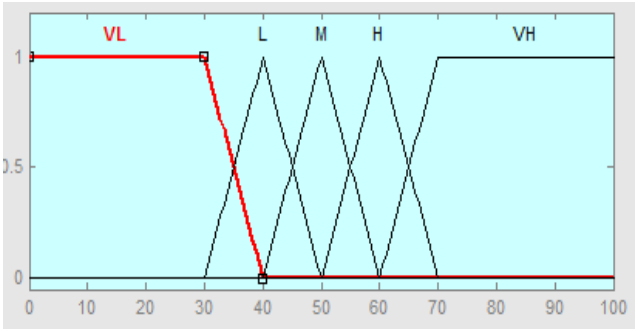
The values of the above two fuzzy memberships will be entered as inputs to the Best Secure Route fuzzy system (tier two) which gives a percentage value and an output value with two possibilities: GOOD or BAD, as shown in Fig.9 c.

Depending on the IF-THEN rules shown in Table 3, it can be decided how secure the selected route is. For example a percentage of 70% means it is good enough to be considered efficient and secure. But when it is 30% or less we can say it is very poor. Using FIS, it can be decided how good and how bad the route is at the same time. For example, 60 % means the route is 60% Good and 40% bad. Therefore, when IDS has a percentage within the VL area and Best Route has a percentage within VL area that means the possibility of having a compromised node is very low also the percentage of the route of being efficient is very low as well. In this scenario we cannot consider this route as the best and secure at the same time. It is secure and poor path because it has a very low percentage of being an efficient in terms of length and power.

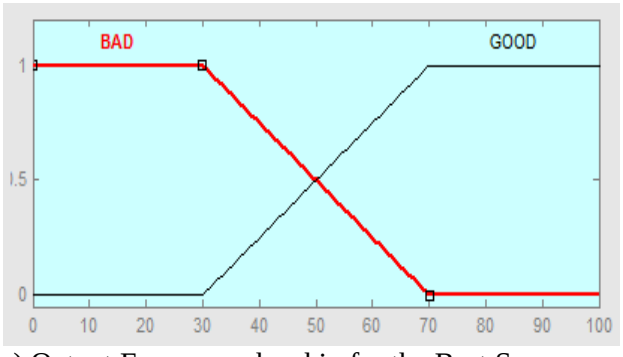
A route is considered the GOOD and secure when IDS value is Low (L) or Very Low (VL) and Best Route value is Medium (M), High (H) or Very high (VH).




a) Fuzzy membership for IDS as output from IDS FIS and as an input for the best secure route system.




b) Fuzzy membership for best route as output from Route Selection FIS and as an input for the best secure route system.




c) Output Fuzzy membership for the Best Secure System.

**Fig. 9** Fuzzy Membership Functions for the Best Secure Route System

**Table 3** Fuzzy IF-THEN rules for the Best Secure Route.

| Best route \ IDS | VL | L | M | H | VH |
|---|---|---|---|---|---|
| **VL** | BAD | BAD | BAD | BAD | BAD |
| **L** | BAD | BAD | BAD | BAD | BAD |
| **M** | GOOD | GOOD | BAD | BAD | BAD |
| **H** | GOOD | GOOD | BAD | BAD | BAD |
| **VH** | GOOD | GOOD | BAD | BAD | BAD |

## 3 Conclusions and Future Work

In this paper, a new routing protocol for Wireless Sensor Network (WSN) was proposed. The new protocol is a hybrid of cluster-based protocol and tree-based protocol to achieve the security requirements and the energy saving requirement. At the same time, the BS plays a server role and all computations are made using it since it does not have power limitations. To confirm the effectiveness of the proposed protocol, MATLAB fuzzy logic simulator is used. Two tier Fuzzy Inference System (FIS) is defined to select the efficient route in terms of delay and energy and at the same time this route needs to be secure and does not include any compromised nodes.

The proposed protocol used in the first step the LEACH protocol in cluster formation process, but as LEACH protocol has weaknesses [19] and the purpose is to improve the weakness of previous protocols, therefore the plans for future work include the use another formation protocol similar to that used by Lung et al. [20].

*References:*

[1] N. Nasser and Y. Chen, SEEM: Secure and Energy-efficient Multipath Routing Protocol for Wireless Sensor Networks, *Computer Communications*, Vol.30, Issue 11-12, May 2007.

[2] R. Srinath, A. Reddy, and R.Srinivasan, AC: Cluster Based Secure Routing Protocol for WSN, *Third IEEE International Conference on Networking and Services (ICNS)*, 2007.

[3] J. Ibriq, I. Mahgoub, Cluster-based Routing in Wireless Sensor Networks: Issues and Challenges, *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'04)*, San Jose, California, USA, 2004, pp. 759-766.

[4] J. Al-Karaki and A. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey, *IEEE Wireless Communication*, Vol.11, Issue 6, 2004.

[5] DANIEL-IOAN CURIAC, CONSTANTIN VOLOSENCU, Redundancy and Its Applications in Wireless Sensor Networks: A Survey, *WSEAS TRANSACTIONS on COMPUTERS*, Vol. 8, Issue 4, 2009, pp. 705-714.

[6] DANIEL-IOAN CURIAC, Implementing Time Series Identification Methodology Using Wireless Sensor Networks, *WSEAS TRANSACTIONS on COMPUTERS*, Vol. 9, Issue 3, 2010, pp. 309- 318.

[7] L. Hester, Y. Huang, O. Andric, A. Allen, P.Chen, neuRFon™ Netform: A Self-Organizing Wireless Sensor Network, *Proceedings. Eleventh International Conference on Computer Communications and Networks*, pp. 364 - 369 , 2002.

[8] Yongsuk Park and Eun-Sun Jung, Plus-Tree: A Routing Protocol for Wireless Sensor Networks, *Springer-Verlag Berlin Heidelberg*, pp. 638–646, 2007.

[9] Mohammad Zeynali, Leili Mohammad Khanli, and Amir Mollanejad, TBRP: Novel Tree Based Routing Protocol in Wireless Sensor Network, *International Journal of Grid and Distributed Computing*, Vol. 2, No. 4, December, 2009.

[10] M. Al-Harbawi, M. F. A. Rasid, and N. K. Noordin, Improved Tree Routing (ImpTR) Protocol for ZigBee Network, *International Journal of Computer Science and Network Security*, VOL.9 No.10, October 2009.

[11] Rahul C. Shah and Jan M. Rabaey, Energy Aware Routing for Low Energy Ad Hoc Sensor Networks, *IEEE Wireless Communications and Networking Conference (WCNC)*, vol.1, pp. 350-355, Orlando, 2002.

[12] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, Energy-Efficient Communication Protocol for Wireless Microsensor Networks, *Proceedings of the Hawaii International Conference on System Sciences*, January 4-7, 2000, Maui, Hawaii.

[13] M. Younis and K. Akkaya, Strategies and Techniques for Node Placement in Wireless Sensor Networks: A survey, *Ad hoc Networks*, Vol. 6, Issue 4, May 2007.

[14] MILAN TUBA, DUSAN BULATOVIC, Design of an Intrusion Detection System Based on Bayesian Networks, *WSEAS TRANSACTIONS on COMPUTERS*, Vol. 8, Issue 5, 2009, pp. 799- 809.

[15] Kapil A. Gwalani, Omar Elkeelany, Design and Evaluation of FPGA Based Hardware Accelerator for Elliptic Curve Cryptography Scalar Multiplication, *WSEAS TRANSACTIONS on COMPUTERS*, Vol. 8, Issue 5, 2009, pp. 884-893.

[16] MATHWORK, *MATLAB*, 2007th Edition, Society for Industrial and Applied Mathematics, Philadelphia, PA, 2007.

[17] L. Zadeh, *Soft Computing and Fuzzy Logic*, *Software, IEEE* Vol. 11, Issue 6, 1994, pp. 48 – 56.

[18] L. Zadeh, Soft computing, Fuzzy Logic and Recognition Technology, in: Fuzzy Systems Proceedings, 1998. *The 1998 IEEE International Conference on Computational Intelligenc*e, Vol. 2, 1998, pp. 1678- 1679.

[19] G. M. Shafiullah, A. Gyasi-Agyei, P.J Wolfs, *A* Survey of Energy-Efficient and QoS-Aware Routing Protocols for Wireless Sensor Networks, *Springer Science*, 2008.

[20] C. Lung, C. Zhou, Using hierarchical agglomerative clustering in wireless sensor networks: An energy-efficient and flexible approach, *Ad Hoc Network*, Vol.8, Issue 3, October 2009.