International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 02 - Issue 09 || September 2017 || PP. 56-67

An Opportunistic QOS Routing Scheme for Supporting Vehicular Safety Scenario over WSN – Swive

K. Raja
Asst. Professor, Department of Information Technology, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.

Dr. R. Saminathan
Assistant Professor, Department of Computer Science & Engineering, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.

Dr. P. Anbalagan
Assistant Professor, Department of Computer Science & Engineering, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.

Abstract: Extensive research work is being carried out in Wireless Sensor Networks (WSN) to implement various applications from agriculture, deep sea, in house communication, vehicular safety to personal health care, where routing plays a vital role along with need for effective QoS. This paper focuses on investigation and delivery of optimal QoS on data interconnectivity issues over wireless sensor nodes. It also provides a multi-scalable architecture for delivery of quality of services in data interconnectivity issues for group communication applications over wireless sensor networks. An opportunistic based QoS routing scheme for vehicular safety over WSN is proposed. Implementation of SWIVE for fast moving vehicles on roadways demand an effective provisioning of QoS for data interconnectivity applications as well, to provide an excellent communication interface between wireless nodes on variable node mobility. The vehicle driver's view is augmented with location based information at spatial location, thus providing an intuitive way of establishing the communication. SWIVE is a reactive protocol scheme developed for high speed vehicle nodes deployed on high way roads and marshy situations. SWIVE has been tested and verified using OPNET Network Simulator for its functionality and QoS performance.

Keywords: Quality of Service, WSN, reactive protocol, vehicular safety scenario

Introduction

With the advancement in vehicles and development in Wireless Sensor network technology [5], the Vehicular safety has become an emerging field of study [2]. Many theoretically useful applications [7],[15] have been imagined in Mobile networks. SWIVE is specially designed for the vehicular safety scenario, the system supports on road way details, vehicular acceleration, working situation of brakes, clutches, RPM of wheel, passenger details where the minute details of vehicle is gathered, integrated, and synchronized for dynamic roadside conditions in a timely fashion [1]. The variable data is expected to be adaptive for enabling to rapidly plan, act, and react on the battlefield scenario. But, conductive radio systems such as WSN which have limited channel capacity [4] are not originally designed for packet internetwork protocols, since the nodes and protocols were not initially designed to support the dynamics of radio channeling capacities.

However, the current cognitive radio information system must be capable of acquiring vehicular safety information from various vertical and horizontal commands or control systems, sensor systems, and on way road assistive systems. The system should include information from all multiple areas of strategic operations being working together as joint forces. Information systems should be scalable and capable of hosting multiple applications to minimize the number of computing platforms on applied scenario. The primary goal of this research work is to depict situations that are commonly encountered on the road towards passenger safety and vehicle safety. To accomplish this, there is a need for network scalability and also the ability to accurately handle the mobility node failures.

This paper is organized into seven sections; literature review was carried out in Section II. Section III discusses SWIVE's mobility model describing its issues and assumptions. Section IV describes SWIVE architecture. Section V explains about the routing protocol. Section VI narrates the setting up of experimental test bed using OPNET. Section VII analysis the performance analysis and the final section comprises the summary.

1.1 Wireless Sensor Network for Vehicular Safety

For several years, the concept of vehicular safety [2] though discussed has not been properly implemented due to variable information dissemination and providing control on communicative components under stochastic scenarios. This concept requires architecture of a mesh network, adapting automatically to variable topologies. Such a network performs auto-configuration and dynamic routing. It detects the presence of

a new node, the absence of another and supports node mobility. Networks meeting these requirements were partially or fully under development [18].

Ad hoc networks involve stationary wireless nodes, mobile collector nodes which may be less ephemeral with limited mobility [17]. This paper focuses on providing efficient routing, network processing, along with information-centric networking, to increase robustness, efficiency and QoS [6], which is required for many military applications and networks.

The vehicular safety environment is mainly characterized by the requirement under the following:

[a] Wireless sensor with minimal delay constraints with priorities
[b] Reliability and availability
[c] Security features
[d] Unicast and multicast traffic
[e] Different kinds of traffic: data, voice, and video
[f] Interoperability between forces and with allied units.

2. Literature Survey

Multiple wireless communication components in vehicle join together as a network and adapt to use wireless ad hoc networks to create an inter-connected vehicular communicative space. There is a drive to interconnect troops, command centers, machinery and sensors. While there are physical test beds, most of the research is simulation based. There are several widely used network simulators like GloMoSim [5], ns2 [11], and Opnet [9] as well as others that have smaller user bases. While wireless ad hoc network simulators output detailed data, analysis is difficult due to the large volume of output and limited visualization support. The authors presented the performance of simulation study of realistic Mobile mobility study [7],[17] of WSN that uses Ad hoc on Demand Distance Vector (SPIN) routing [8][15].

Network parameters such as required bandwidth, packet loss, delay and throughput supports QoS in WSN, which is considered to be more challenging than in any fixed network. It is also difficult to support various applications with suitable QoS in WSN because it has highly dynamic node in varying topology and load conditions than fixed networks [10]. [21] defines a mobility model which helps in getting accurate results for route performance evaluation as well supports in necessary component to predict the next positions of vehicles and make smarter route decisions in many WSN routing protocols. He *et al*. [13] proposed a clustering algorithm and states that cluster head lection is based on Mobile dynamics instead of vehicle identity or relative mobility. Opportunistic routing by Yao et al. [22] is that, a stable route is likely available in unreliable multi-hop wireless networks if each node can utilize its multiple neighbors as potential forwarders. To find a stable route in terms of number of hops, Yang [23] specifies two rules: the rule of the selection of service for each node, and the rule of service priority.

3. Swive - Mobility Model

A stochastic Global Mobility Model is used to describe inter-cell movements [20], for a battle-field and a deterministic Local Mobility Model to describe intra-cell movements within a small terrain or building, while in [15], the authors applied link expiration prediction based on neighbor velocity information to several existing routing protocols. Authors in [16**]** used an adaptive algorithm to predict mobility to help location tracking of Wireless sensor nodes.

3.1 Issues

SWIVE is a reactive protocol scheme developed for high speed vehicle nodes deployed on high way roads under critical traffic situations. Following issues were considered for discussion,

a) To ascertain ***quality of service*** between various wireless sensor nodes capable of interconnecting and communicating with each other.
b) To enable and maintain complete ***session management*** between nodes during communication.
c) To provide co-operative ***resource management*** (bandwidth, energy other resources) between nodes on communication
d) Location and Quality (goodness) aware policy among ***group of communication*** enabled nodes.
e) Handle ***co-operative*** issues

4. Swive - Proposed Approach

High speed vehicular communication systems of today are geared to rather wide area coverage and moderate bandwidth demands providing services like voice communications and low data rate applications. Deployment of WSN nodes in critical communication systems suggest multiple services of tomorrow might completely differ towards offering time critical applications [14].

High bandwidth requirements and large user populations will clearly demand large portions of the frequency spectrum for nodal inter communication [13]. This natural resource is finite but, fortunately, it can be reused with multiplicity, provided the geographical distance between wireless terminals using the same portion of the spectrum is large enough. In an autonomous network with a large number of users, data messages are usually transmitted only over short distances, allowing a frequent reuse of the spectrum. Long distance transmissions may still be feasible using multi-hop store-and-forward techniques. The developed architecture does not only concentrate on the user interface aspects but also provides a scalable infrastructure to support mobile applications. Moreover this architecture also supports collaborative activity among multiple fast moving vehicles in communication end; enable decision making for overcoming the opposition force, disturbing the vital points of opposition force, working as a team to overcome the challenges.

In this work, the use of adaptive routing for collaborative navigation and information accessing tasks in an urban environment is demonstrated. A navigation function allows one or more users to roam through a remote location and guides them to selected destinations. Information browsing presents users with information about objects in their surroundings. Both functions feature support for collaboration. It supports geometric representation of the environment and also semantic and contextual signs for expressing information during heavy battle times. Compared to conventional location based systems, SWIVE not only requires integration of a wider variety of data sources to build interesting scenarios, it also creates new types of content.

4.1 SWIVE - A Mobile network support in Vehicular safety Environment

WSN are characterized by self-governing nodes, which move arbitrarily so that the topology changes dynamically. SWIVE is a QoS based WSN routing protocol for establishing digitalized communication between high speed vehicles on road. Wireless communication devices can be mounted on moving vehicles or locations on high way road, which communicate with each other through IEEE 802.16[12], IEEE 802.11 n. The Fig-1 demonstrates SWIVE implementation in high way road scenario.

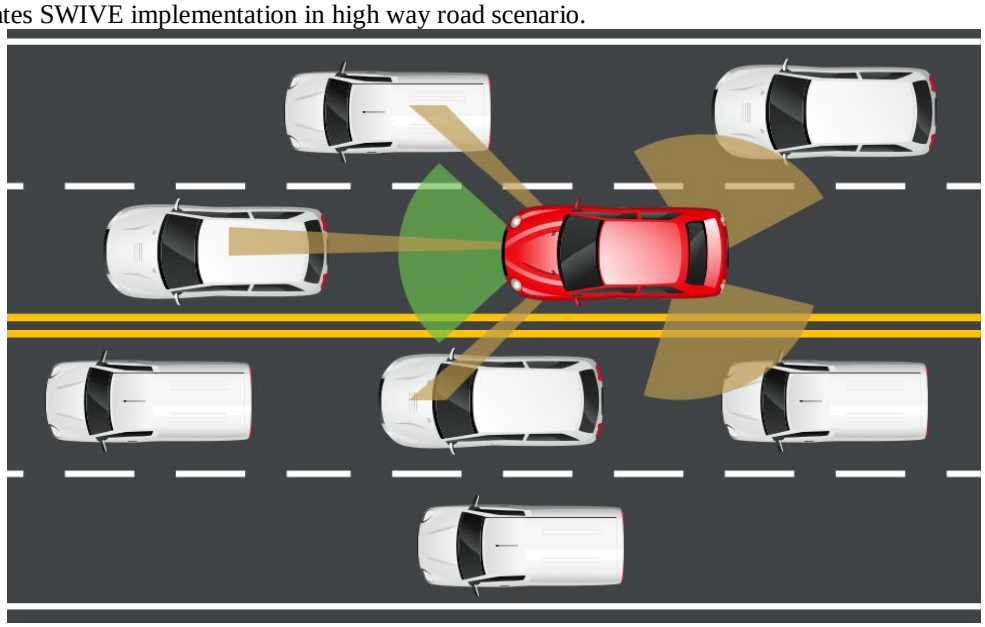

Fig. 1 SWIVE in vehicular safety supportive environment

In this scenario, the vehicles moving in high speed road belong to domain-1, while vehicle roaming in the hilly terrain belong to domain-2. Node in a domain can communicate with node in another domain through a node called Group coordinator.

4.2 Design and Analysis

SWIVE is proposed as protocol which identifies optimal QoS enabled routing path for providing media data interconnectivity services over multiple group communication applications. SWIVE is advantageous over LEACH and SPIN in the following factors.

a) The additional delay of route maintenance in LEACH had been controlled in SWIVE and hence the end-to-end delay is minimized.
b) Flooding is controlled, due to an increase in the number of nodes, by effective cluster procedures; hence throughput is better compared with SPIN and LEACH.
c) Issue of controlled Hand-off procedures improves the quality of the setup.

4.3 SWIVE – Architecture and Functionality

SWIVE architecture has the following components / module based on the functionality as shown in Fig. 2

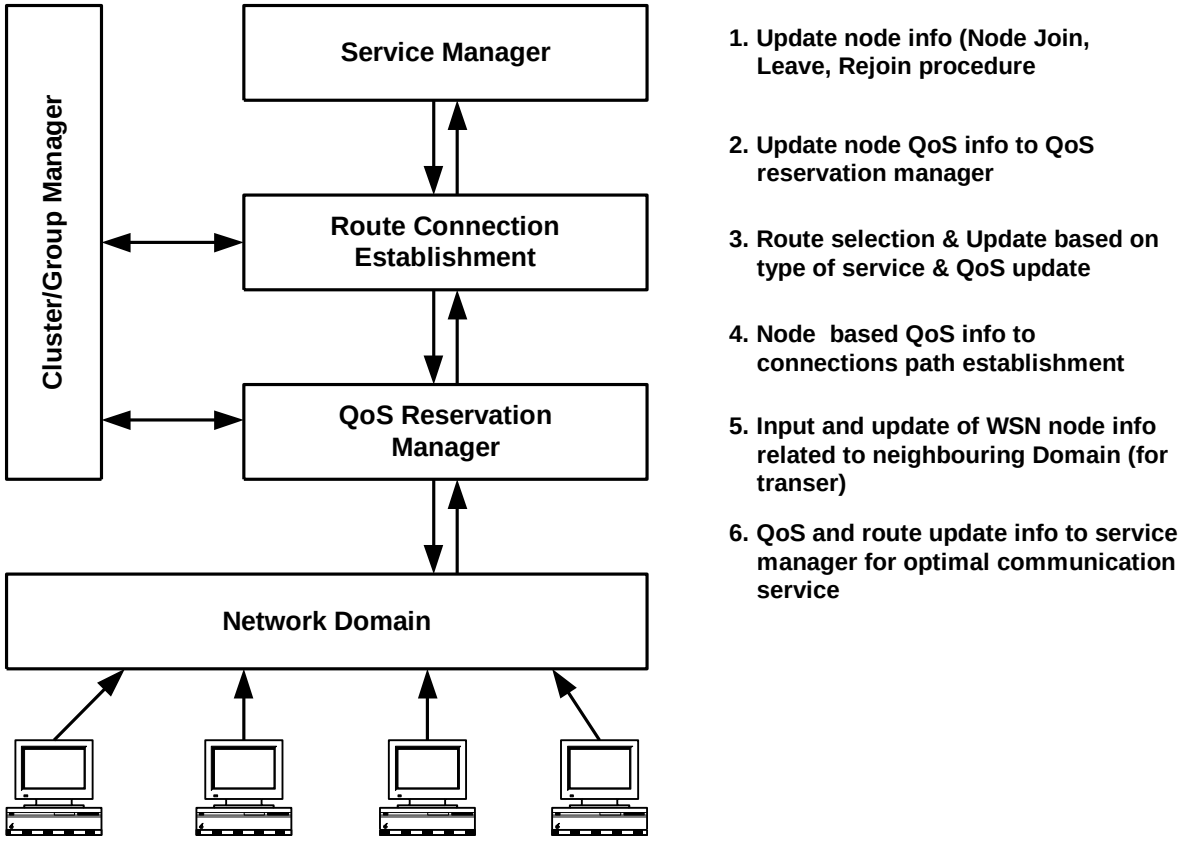

Fig. 2 SWIVE Architecture with functionality modules

[a] **Network Domain**: Network Cluster controller, which maintains information of all registered node.
[b] **Cluster / Group Manager**: Group Coordinator, which clusters the nodes into group. The group Head or cluster head is identified based on Election algorithm.
[c] **QoS Reservation Manager**: The QoS parameters of all the nodes are updated and maintained by the Reservation Manager of this component.
[d] **Route Connection Manager**: To identify the optimal route path based on available QoS and connection management required for the type of service.
[e] **Service Manager**: To establish the connection between the nodes and to provide the expected service.

SWIVE works on cluster based management, which split the nodes into domain/cluster, and establishes domain/cluster head with a node which possess the highest bandwidth capacity and node communication link. The domain/cluster head (Group Coordinator) establish path between nodes in the same domain/cluster.

If nodes in one domain need to communicate with nodes in another domain then the domain head (Group Coordinator) establishes a path with the help of another cluster domain head. Even though cluster head may add delay in between a communication path, but still this protocol creates minimal flooding packets in network and hence reduce delay in round trip time.

SWIVE scheme works as a hybrid reactive protocol in its behavior, such that its component modules are activated initially when the service is invoked but the module exhibits its behavior only when the session is in use. Hence when modules are invoked, the process is not triggered, but when the session is put into use, the components get activated.

The SWIVE architecture adopts the following functionality of Mobile node on as-is-basis:

a).When a new node (n) wishes to join a domain, then node n, needs to send a register message to Group Coordinator (GC), which in turn may send a reply message to join the domain. A node, which has to cater various types of services, sends REQ (Route Request) message with service type to GC for establishment of

new route. GC sends REP (Route Reply) to nodes, which should function as source, destination and hand-off. If any node in the domain misses its neighbor for route update and communication then it send ERR (error) message to GC. Every node sends its set of QoS parameter to GC at frequent time intervals.

b). Similar to new node (n) joining the domain cluster, any node (m) can quit or re-join the domain at a time, as the nodes are consistently on mobility.

c.) SWIVE QoS reservation manager consistently updates the QoS parameter(s) of all its registered nodes.

5. ROUTING PROCEDURE

With hybrid reactive protocols, each node maintains the routes to all other nodes in the network by periodic exchange of control messages. When a node needs to send a packet to any other node in the network, the route is immediately available. The main advantage of hybrid reactive protocols is that they do not introduce a delay before sending data, but determines multiple paths for routing. Furthermore, these protocols are useful for traffic patterns where large subsets of nodes are communicating with another large subset of nodes, and where the source and destination pairs are changing over time. The route implementation in the platform adopts a hysteresis mechanism, based on received power / signal measurements:

a) Before a link to another node is accepted, the receiving power of the corresponding HELLO [14], must be above a threshold, which is set to -85 dBm in experiments.
b) As long as it is above the threshold and equal to -94 dBm, the link is considered to be valid.

In the presence of topological changes like node appearance, disappearance and node mobility, the protocol SWIVE, detects these changes and updates the routes accordingly, in order to maintain the shortest route to any destination in the network. The measurements concerning the bandwidth are collected at regular intervals of time. The model considers TCP flows and measure the bandwidth obtained at the destination node.

Scenario 1: Route Discovery

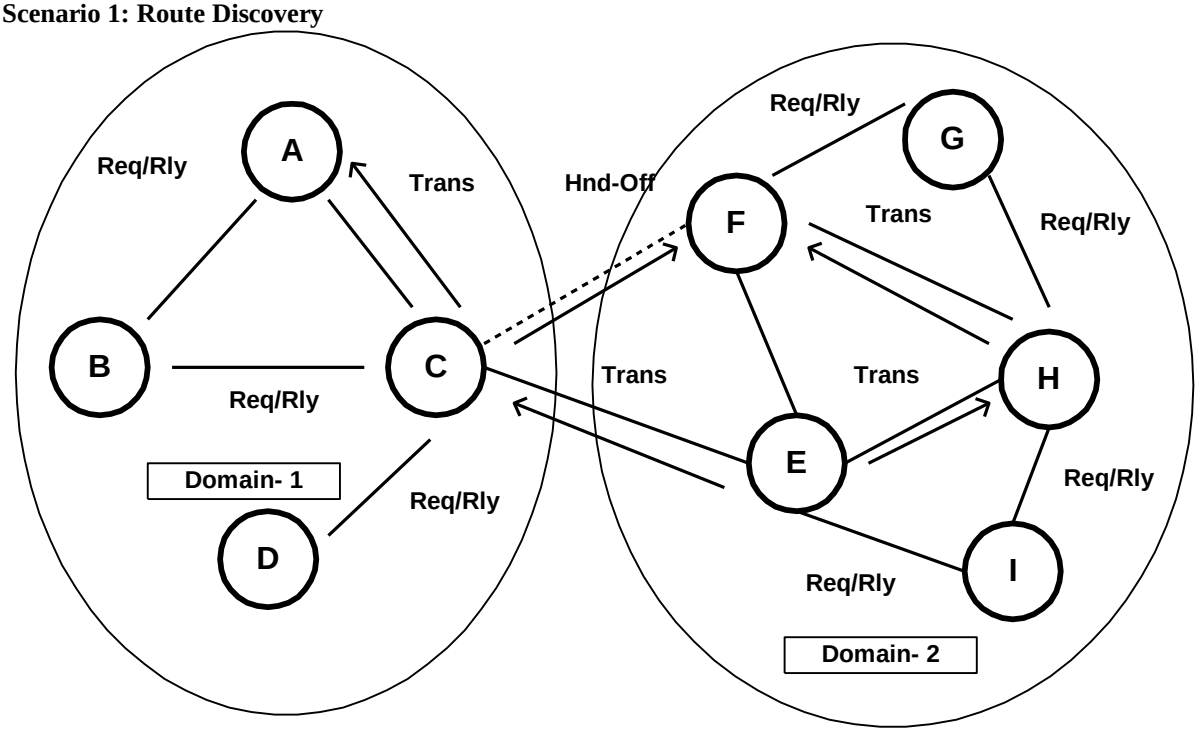

Fig. 3 Cluster group communication for Route Discovery

Fig-3 shows two domains. The node with IEEE802.15.6 configuration is declared as a cluster controller based on its communication and coverage range. In cluster-1, the node-A (IEEE802.15.6 configuration) and node-B (IEEE802.15.6 configuration) are registered as domain controller-1 or clusters. The node-C and node F (IEEE802.11g configuration) is available between domain-1 and domain-2 coverage range. But it node-F is registered in domain-2 due to its high signal strength from domain-2 than domain-1. The node-H (IEEE802.15 configuration) and node-E (IEEE802.15.6 configuration) are registered within domain controller-2. All these nodes send their connection information with available bandwidth and packet loss percentage to their corresponding domain controllers.

In above scenario1, the node-A in domain-1, want to stream data to node-B so it sends a route request message (Req) to domain 1, which consistently updates its domain node information, and finds a path. Once the path is found, it sends a Transmit (Tran) message to node-A and Receive (Recv) message to node-B, transmit and receive messages contains route information and port numbers.

The node-E in domain-2, needs to stream to node-F, hence the route request message (Req) is send to domain-2. The domain -2 understands its domain node information, and updates the path. Once the path is identified then the data Transmit (Tran) message is sent to node-D, Hand-Off message to node-G and Receive (Recv) message to node-F, transmit, hand-off and receive message contains route information and port numbers.

Scenario 2: Intra domain based Communication

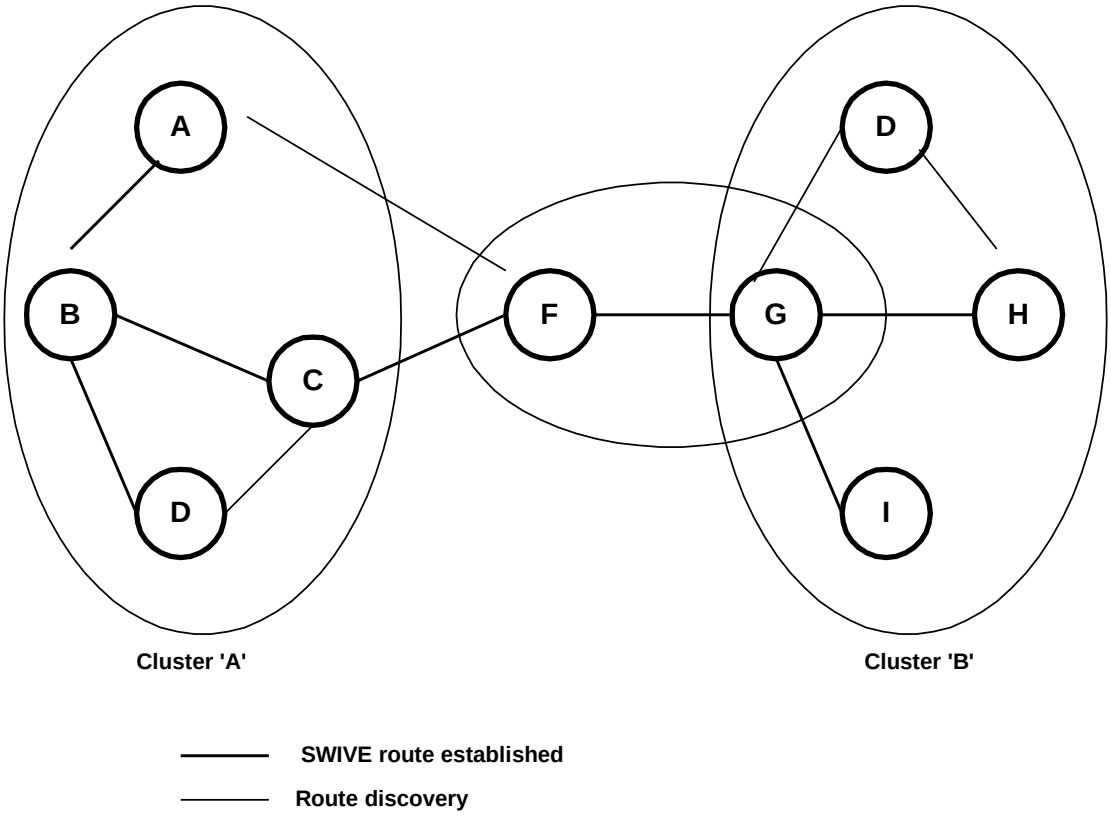

Fig. 4 Intra Cluster communication between WSN nodes

Scenario 2 explains the communication established between nodes in domain-1 needs to communicate with nodes in domain-2 as shown in Fig. 4. Node-A in cluster A sends route request message to node G in cluster-C, which checks that the destination node-G is not in its domain. Then the Controller node in Cluster A sends route request message to its nearby cluster, which happens to be cluster controller-B in our scenario. The Cluster controller-B receives the route request message and then it checks for the destination node-I in its domain. Once the node-G is in cluster-2 then the cluster controller-2 makes path to cluster controller-2. Here the node-A can communicate to node-G through the path of node-C, but the node-C is in cluster-C so it can't communicate directly.

Definitions:

rBwd – required bandwidth observed by Service Discovery Manager
rPdr - packet delivery ratio
rBwl – Available Bandwidth
rPlp - Packet Loss
rDelay – Round Trip Delay
Vector NodeList [ ] – List of Nodes
Vector RouteList [ ] - List of Routes

1: Determine node location and Update Configuration

Vector NodeList [ ] = AddNode (Node.Location, Node. Config)

2: Check Node.Status( )

```
If (Node.Status = ACTIVE & Node.Type = HAND_OFF) THEN
{
   Update_QoS (Node_i, Node_j, Node_k,..n-1, rBwd, rPlp, rDelay)
   Set Node_i.n = Node.Neighbour
   AddNode (Node_i..n)
}
If (Node.Status = IDLE or Node.Staus = NOI) // Not In use
   RemoveNode (Node_i..n)
```

3: Check and Update Neighbour

```
If (Nodei Is.Neighbour Node_j..n) then
    AddNode (Node_j..n)                    // attach as neighbor
If (Node_i.Is.rBwd OR Is.rPlp OR Is.rDelay) then
    AddNode(Node_i)                        // attach as acceptable QoS
```

4: Define Route

```
If (! Route.Status = EXISTS)
   Vector RouteList[ ]  =  AddRoute (Route_a )
Else
   CreateRoute (Route I, NodeList [ ] & Node.Status=ACTIVE)
If (! path.Status = (Nodei, Node_j.))
   ReEstablishSession( )
Else
{
   RouteList = Add (Node_i, Node_j …) →RouteList [ ] where 'a' to 'z' being possible routes defined
   CreateRoute (Route_a)
}
```

5.1 Neighbor Discovery

Each node must detect the neighbor nodes with which it has a direct link. For this, each node periodically broadcasts *Hello messages*, containing the list of neighbors known to the node and their link status.

The link status can be either symmetric (if communication is possible in both directions), asymmetric (if communication is only possible in one direction). The *Hello messages* are received by all one-hop neighbors, but are not forwarded. They are broadcasted once, per refreshing period, called *Hello interval* by 25 to 50 ms. Thus, *Hello* advertisement messages enable each node to discover its one-hop neighbors, as well as its two-hop neighbors. This neighborhood and two-hop neighborhood information has an associated holding time, after which it is no longer valid and to be refreshed.

5.2 Navigation & Negotiation

In the navigation mode, the battlefield jawan should select a specific target node or a desired target location of a certain soldier type on a terrain or in a building or location. The system then computes the shortest path in a known network of possible routes. It is interactive and reacts to the user's movements. It continuously re-computes the shortest path to the target if the user goes afield or decides to take another route. If two or more users are present, a number of collaborative interactions are possible. The communication interface provides the list of members that have joined the collaboration session.

5.3 Enable QoS

To maintain and reserve the required QoS for the session, algorithm SWIVE_QoS ( ) checks and identifies the supportive QoS for the required service between conference parties and insists the QoS Reservation manager to provide the QoS for the session to be effective.

Procedure SWIVE_QoS

```
Begin
1. Consider Route ← Oi            // Identify all possible routes
2. If Bandwidth (Oi) <= th_limit
      Then Flag ← normal          // Provide support on QoS
   Endif                          // Decide the best path based on traffic bandwidth
```

3. If Bandwidth (Oi) > th_{limit} and Bandwidth (Ri) <= $MinTol_{limit}$
Then Flag ← control
Endif (* since all paths are nearly full, select another best path, minimize the allocation of resource *)
4. If Bandwidth (Oi) > $MinTol_{limit}$ and Bandwidth (Oi) <= $MaxTol_{limit}$
Then Flag ← alert
Endif (* don't allow any packets through the path into reconstruction *)
5 If Bandwidth (Oi)>= $MaxTol_{limit}$
Then Flag ← CreateRoute ()
Endif
6. Route ← Ii
If Bi >= Bo
Then Transfer_Data
Else
Route ← Ij // consider next route
Endif
End

5.4 Setting Threshold limit for QoS in a session or routes updates

Depending upon the number of packets (P_n), the size of the packet (P_s) number of hops (h_s)and available bandwidth of the network (B_a) for a session, the threshold limit (th_{limit}) of route can be identified based upon service in use and on available bandwidth.

$P_{al} = Ba / (P_s * h_s)$

$th_{limit} = P_{al}$ / avg (B_a in use)

When a route or session crosses the expected threshold limit in use, then the chances of SWIVE to lose its QoS is high. The aim of setting a tolerance limit for route involves, such as introducing a *gauge* which limits the flow of transfer of packets from over-crowding or creating congestion.

$MinTol_{limit} = th_{limit} + th_{limit} / 2$

$MaxToll_{imit} = MinTol_{limit} + th_{limit} / 4$

5.5 Bandwidth measurements for TCP flows

The bandwidth availability between any two nodes in the multi-hop network can be analyzed based on the random topology. Table-1 shows that the traffic from source "c", one-hop away, is favored with regard to traffic of source "h", which is three-hops away. It also shows that when both "h" and "g" send TCP flows to "b", three-hop away, both receive approximately the same ratio of bandwidth. As being observed, when both TCP sources use the same hop from the destination, the bandwidth sharing is optimally fair. However, an unfair bandwidth sharing is noticed, even though both sources are two-hops away. Node "b" receives 102 bps from "i", whereas node "b" receives at 152 bps from "e".

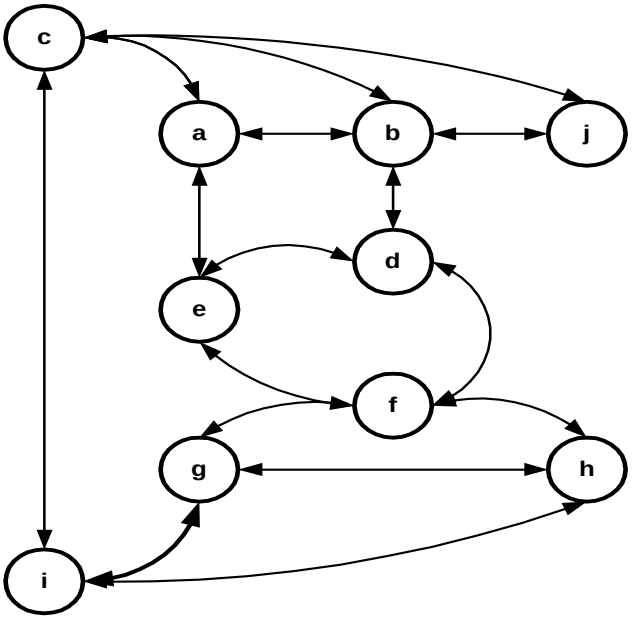

Fig. 5 SWIVE Route Maintenance

This experiment is repeated and similar results were obtained. Even though node "i" involves to send TCP flow to node "b", the throughput is limited (i.e. 102 bps), whereas node "e" gets the same ratio of bandwidth as in earlier iteration, which evicts the unfairness of TCP compared to UDP.

An analysis of the available bandwidth being shared between co-existing TCP flows is studied. In the experiment reported in Table-1, where two sources send TCP flows to the same destination "b" is shown in Fig. 5.

Source	Destination	Route	No. of Hops	Throughput
C	b	c → b	1	380 bps
H	b	h→ f → d→b	3	210 bps
H	b	h→ f → d →b	3	240 bps
G	b	g → f →d→b	3	200 bps
I	b	i→c →b	2	80 bps
E	b	e→ d →b	2	152 bps
I	b	i→c →b	2	102 bps
H	b	h→f →d →b	3	347 bps

Table 1 Traffic intensity between nodes in network and possible paths

The experiment is initialized by using a source "b" which sends UDP traffic and TCP traffic to the destination "h". The bandwidth obtained by each flow is measured and its results are reported in Table-1. It can be understood that the bandwidth part received by the UDP flow is much higher than obtained by the TCP flow. Here, the UDP flow receives a bandwidth which is 150 times more than the bandwidth ratio obtained by TCP flow (source rate of 5 Mbps). For instance, at a source rate of 500 bps, UDP traffic receives a bandwidth which is 9 times more than TCP. This phenomenon is naturally expected and observed, as TCP control congestion, hence reduces the TCP transmission window on congestion signaled by packet loss, or time-outs, hence UDP traffic is still highly favored than regard to TCP traffic. Hence it can be concluded, that based on "bandwidth in use" metric for the available minimal bandwidth UDP performs better, while for bandwidth availability at nodes compared to TCP.

6. SIMULATOR TEST-BED

To evaluate the proposed architecture SWIVE, the simulation experiments can be carried out using the OPNet Simulator [19]. The simulation experiments consist of up to 25 Wireless sensor which includes Wireless sensor and gateways. The simulation area used for these experiments is a square of 1000m x 1000m with the maximal transmission range of 250m. Up to 50% of the Wireless sensor seek Internet connectivity. In the simulation experiments, hybrid-1and hybrid-2 refers to hybrid gateway discovery mechanism based on 1-hop and 2-hop neighbors respectively.

6.1 Setting up the experimental Test-bed

The experiment is carried out with 200 nodes using a simulated test-bed with varying mobility speed, direction, distance between inter communication nodes as shown in Table-2. OPNet simulator is used in analyzing the performance of SWIVE over LEACH and SPIN.

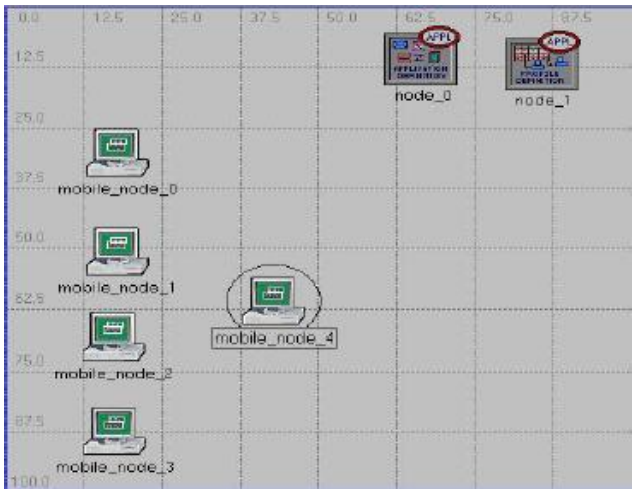

Fig. 6 Deployment of test-bed scenario

Nodes employed 1) No of TCP sessions created / managed 2) No of nodes in use	 10, 15, 20, 25 sessions in use 200
Service Type: Data Transfer	Provides associative grouping of service calls Dynamic provisioning of Service Level Agreement (SLA) based on Ad hoc network behavior
Behavior depends upon	Node mobility intensity between defined time intervals Nature of node mobility Intensity of data traffic created.

Table 2 Experimental Test Bed

The goal helps to understand the impact of high speed vehicle's transmission rate, bit-rate, packet size on throughput and delay. The experiments used a fixed test-bed, which is simulated in lab and another in a limited 100 mobile node deployment as shown in Fig.6.

6.2 Mobility and communication models

The nodes considered as wireless sensors in WSNs move according to the random waypoint mobility model [3]. The speed of non-gateway WSN nodes is randomly chosen between 2 m/s and 20 m/s while that of Mobile gateway is between 0 m/s and 5 m/s. The pause time was 10 and 50 milli-seconds for Wireless sensor and Mobile handoff nodes respectively. In the simulation, 20 nodes as sources are used to generate packets at the rate of four packets per second. The packet size of 512 bytes was used throughout the simulation. All simulation experiments were run for 10 seconds and each data point in the graphical results is based on the average of five simulation runs.

The performance analysis is determined based on Throughput, Delay Observed, average of hops covered and Packet Loss observed which are the major factors involved for determining the quality of services.

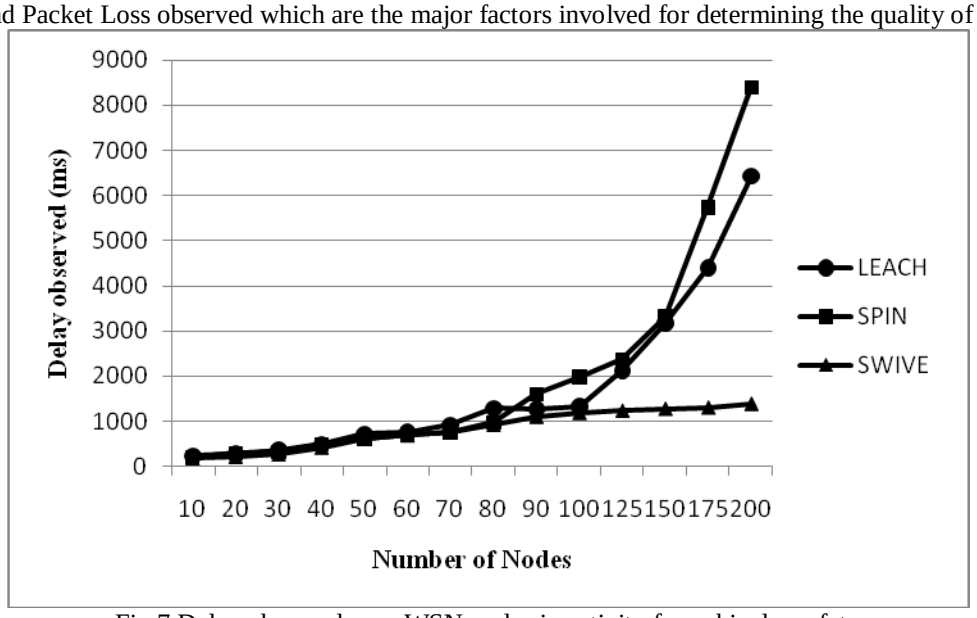

Fig.7 Delay observed over WSN nodes in activity for vehicular safety

The performance of mobile node behavior suggests of the observed delay for 200 nodes in mobile activity. Fig-7 shows three approaches being followed over LEACH protocol and SPIN implementation over WSN and SWIVE. The average Delay observed in SWIVE is 1200ms compared to SPIN which demonstrates 4080ms on average while LEACH shows 3200ms. The performance of SWIVE towards delay controlling and monitoring is optimized due to buffer enhancement at hand-off between intra-clusters. The sudden increase in spike over SPIN and LEACH shows that delay is un-controlled until 80 nodes and when 100 nodes are crossed the performance of protocol is uncontrolled and hence may lead to saturation.

Fig-8 discusses on the packet delivery ratio achieved over 200 nodes simulated over 10 seconds. The performance of SWIVE is comparatively higher in delivery ration compared to SPIN and LEACH. LEACH adopts intra handoff between cluster nodes within the cluster of nodes engaged in communication through

cluster heads hence time taken to establish a route is naturally higher than SWIVE. The time taken to establish route in SPIN depends on each WSN node negotiate with another WSN node to suggest route establishment.

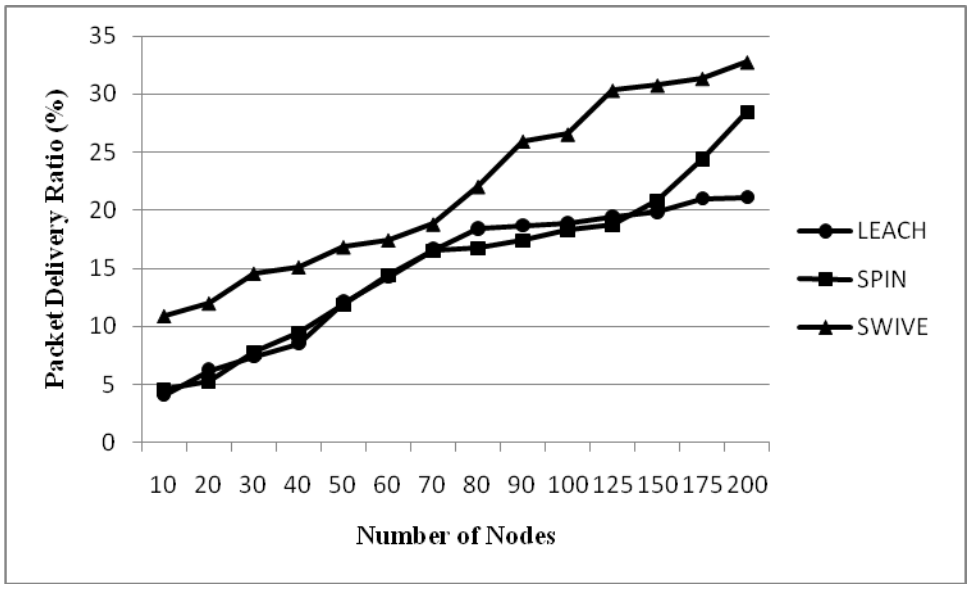

Fig.8 Packet Delivery Ratio observed variable number of nodes

SWIVE demonstrates 65.47% of delivery rate while SPIN shows 51.49% of average delivery rate and LEACH demonstrates 38.05% delivery rate over 1 second. Fig-9 shows maximal throughput achieved by SWIVE over LEACH and SPIN.

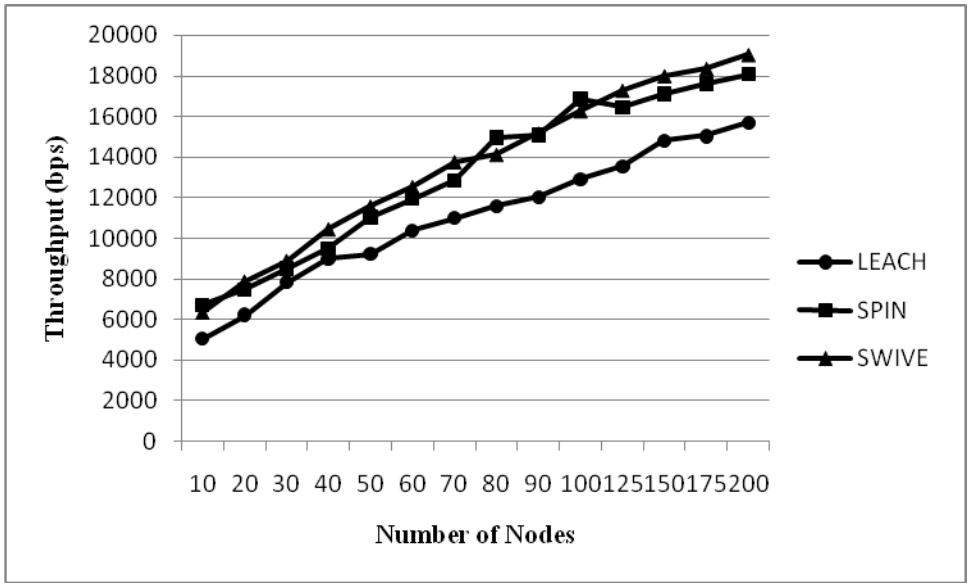

Fig. 9 Throughput observed over varying nodes

SWIVE demonstrates throughput based on node mobility and route establishment time. The traffic intensity generated between the nodes discusses on the packet loss and congestion control mechanisms to improve throughput.

7.0 CONCLUSION

Major research challenges exist on providing Quality of services over WSN networks. Though numerous research works discuss on providing QoS over variant intervals of time, the phenomenon of supporting consistent quality over numerous nodes is not supported. This research work SWIVE designed as an opportunistic QoS routing scheme for supporting vehicular safety scenario over Wireless Sensor Network works on an buffer based handoff management and scheduling approach.

Performance of SWIVE in terms of quality of service metrics such as throughput, packet delivery ratio, and delay observed. SWIVE performs better than compared to SPIN and LEACH which are adopted in industry terms. SWIVE also performs well for 200 nodes taken for testing as simulation over OPNet simulator, while compared other schemes which shows its performance only for minimal nodes on mobility.

References

[1] Achlioptas, D. Database-friendly random projections: Johnson-Lindenstrauss with binary coins, J. Comput. Syst. Sci.66, 671– 687, 2003
[2] O Akan, I Akyildiz, Event-to-sink reliable transport in wireless sensor network. IEEE/ACM Trans. on Networking 13(5), 1003–1016, 2005
[3] Baris Yuce, Michael S. Packianather, Ernesto Mastrocinque, Duc Truong Pham. Alfredo Lambiase , Honey Bees Inspired Optimization Method: The Bees Algorithm, Insects, 4, 646-662, 2013
[4] Cetisli, B.; Barkana, A. Speeding up the scaled conjugate gradient algorithm and its application in neuro-fuzzy classifier training. Soft Computing. 14, 365–378, 2009
[5] M.W. Chiang, Z. Zilic, K. Radecka, J. S.Chenard, "Architectures of Increased Availability Wireless Sensor Network Nodes," ITC International Test Conference, Vol. 43, No. 2, pp. 1232-1241, 2004
[6] E. Felemban; Chang-Gun Lee, Ekici, E. MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and Timeliness in wireless sensor networks, Mobile Computing, IEEE Transactions on Volume 5, Issue 6, pages 738-754, June 2006.
[7] Gagandeep Singh, Amandeep Kaur, Evaluating Wireless Sensor Network on Quality of Services Using Mobile Sink Nodes, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013
[8] M. Z. Hasan and T. C. Wan, "Optimized Quality of Service for Real-Time Wireless Sensor Networks Using a Partitioning Multipath Routing Approach," Journal of Computer Networks and Communications, Vol. 2013, 18 p, 2013
[9] T. He, J. Stankovic, L. Chenyang, and T. Abdelzaher. SPEED: A stateless protocol for realtime communication in sensor networks. In Proceedings of 23rd International Conference on Distributed Computing Systems, pages 46–55, May 2003.
[10] Koc, E. The Bees Algorithm Theory, Improvements and Applications. Ph.D Thesis, Cardiff University, Cardiff, UK, 2010
[11] B. Kosko, Neural Networks and Fuzzy System, Prentice Hall of India, 1997.
[12] Kulik J., Heinzelman W., Balakrishnan H. Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks. Wirel. Netw. pp 8:169–185, 2002
[13] Mainwaring, A., "Wireless Sensor Networks for Habitat Monitoring", in ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02), 2002
[14] P. Mahapatra, J. Li, and C. Gui. QoS in mobile ad hoc networks, IEEE Wireless Communication, vol. 10, no. 3, pp. 44–52, 2003
[15] Perrig, A. "SPINS: Security protocols for sensor networks", Proceedings of MOBICOM, 2002
[16] Rabiner W., Kulik J., Balakrishnan H. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks. Proceedings of the Fifth Annual International Conference on Mobile Computing and Networking (MOBICOM); Seattle, WA, USA. August, 1999; pp. 174–185.
[17] F Ren, S Das, Traffic-aware dynamic routing to alleviate congestion in wireless sensor networks. IEEE Transactions on Parallel and Distributed and Distributed Systems 22(9), 1585–1599 (2011)
[18] Rubén Braojos, Ivan Beretta, Giovanni Ansaloni and David Atienza, Early Classification of Pathological Heartbeats on Wireless Body Sensor Nodes, Sensors 2014, 14, 22532-22551
[19] Sameh H. Ghwanmeh, Wireless Network Performance Optimization using OPNET Modeler, Information Technology Journal, Vol-5, No-1, pp-18-24, 2006
[20] Tsai, P.-W.; Khan, M.K.; Pan, J.-S.; Liao, B.-Y. Interactive artificial bee colony supported passive continuous authentication system. IEEE Syst. J. 2012
[21] X. Wang, W. Gu, K. Schosek, S. Chellappan and D. Xuan, "Sensor Network Configuration under Physical Attacks," Technical Report Technical Report (OSU-CISRC-7/04- TR45), The Ohio-State University, Columbus, 2004.
[22] Y Yao, Q Cao, V Vasilakos, EDAL: an energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks. IEEE/ACM Trans. on Networking 23(3), 810–823, 2015
[23] Yang Dondkai and Liu Wenli, ―The Wireless Channel Modeling for RFID System with OPNET, the Proceedings of the IEEE communications society, 5th International Conference on Wireless communications, networking and mobile computing, Beijing, China, pp. 3803-3805, September 2009.