EXAMINATION AND APPLICATION OF AODV AND DVR PROTOCOLS IN WANETS

Randeep Kaur[1], Dr. Rajinder Singh[2]

[1]Research Scholar, Ph.D (Comp. Appl.), Guru Kashi University, Talwandi Sabo, Punjab, India.

[2]Assistant Professor, UCCA, Guru Kashi University, Talwandi Sabo, Punjab, India.

ABSTRACT

A wireless network is normally a decentralized network. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically. Since the ad-hoc network is a decentralized network it should detect any new nodes automatically and induct them seamlessly. The research paper primarily focuses on working of WANETs, elaborating its characteristics and its limitations. In addition of this, the two prominent routing protocols, AODV and DVR, has been discussed along with their implementation and working.

Keywords: AODV, DVR, wireless networks.

I. INTRODUCTION

WANETs are the distributed, dynamic, self-configuring, and decentralized wireless networks. Communication between nodes in these networks takes place with wireless links and without the help of a centralized trusted authority. This ad-hoc and decentralized working enabled them to be applied in the remote, hostile, and resource-constrained environments to perform mission critical tasks [1, 2]. An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other as shown in Fig. 1. In the Windows operating system, ad-hoc is a communication mode (setting) that allows computers to directly communicate with each other without a router [3, 4].

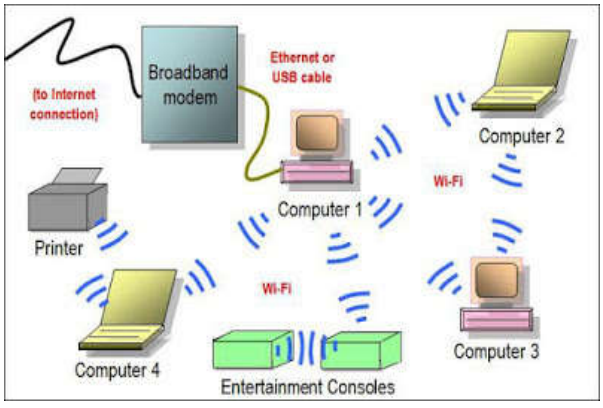

Fig. 1 The figure represents the basic structure of WANETs

Characteristics of WANETs

- Autonomous operations: Nodes communicate among them with inherent trust, cooperation, and without a central authority. Nodes act as the router to identify the path, and as the host to generate the data and control packets.
- Dynamically changing topology: Nodes arbitrarily move in the network with varying speed and direction. With this, nodes frequently enter and leave the communication range of other nodes. It causes a dynamic change in topology.
- Multi-hop routing: Each node consists of a fixed communication range and hence they tend to follow multi-hop routing to transmit the data between the source and the destination nodes.

Due to the characteristics and limitations of WANETs such as the absence of infrastructure, distributed network operations, and dynamic topological changes, the network performance directly depends on the nodes cooperation in the network operations. Furthermore, communication protocols in WANETs are designed with an assumption that nodes are cooperative and trustworthy. In this context, node cooperation and its operational efficacy cannot be guaranteed in the presence of adverse activities. This lack of coordination is said to be node misbehavior. The node misbehavior may occur in the following three ways mentioned as under [5, 6].

- Node malfunctioning: Nodes in the network malfunction due to hardware or software problems. These are not malicious nodes. Buffer overflow and route error due to mobility are the examples of this category.
- Passive attack behavior: Nodes in the network eavesdrop, impersonate, or creates a Denial of Service (DoS) on the communication between genuine nodes.
- Active attack behavior: In this, although nodes appear to be legitimate and valid, they are being compromised by an adversary. These attacks are termed as internal security attacks. Internal attacks cannot be identified by conventional cryptography security methods. Systematic observation and assessment of node behavior help in isolating these attacks [7, 8].

II. ROUTING PROTOCOLS IN WANETs

This section discusses the working and implementation of two prominent routing protocols used in WANETs, AODV and DVR.

Reactive Protocol - AODV

Adhoc On-demand Distance Vector (AODV) is the currently most popular routing protocol for MANETs. In this protocol, a node discovers a route on demand, i.e., only when it is needed, and caches it. Network wide flooding is used to discover the routes. This protocol requires that nodes maintain local connectivity information by sending periodic local (1-hop) broadcast messages known as hello messages. Through these hello messages a node becomes aware of its neighbors or nodes in its radio range. When a source node wants to send a message to a destination node and a route to the destination is not available in the cache, it initiates a path discovery process by broadcasting a route request (RREQ) packet. When a node receives a RREQ packet it checks whether it has received the same packet before, if it has then it discards the packet. The node then determines whether it has a route to the destination node in its cache. If it cannot satisfy the route request of the source then it rebroadcasts the packet after setting up a reverse path to the source. To

set up a reverse path, a node records the address of the neighbor from which it received the first copy of RREQ as the next hop to the source. Eventually a RREQ arrives at a node (possibly the destination itself) that possesses a current route to the destination. Then node unicasts a route reply (RREP) packet back to the source. As the RREP travels back to the source, each node along the path sets up a forward pointer to the node from which the RREP was received as the next hop to the destination and updates its timeout information for the route entries to the source and destination. Nodes that are not part of the path determined by the RREP, timeout after ACTIVE_ROUTE_TIMEOUT and delete the reverse path to the source. When a node detects that a destination node is unreachable (a link failure is detected either by failure to receive hello messages or a link-layer acknowledgement), it propagates to all the active neighbors a route error (RERR) packet for the failed routes for which the node was the next hop [9, 10].

For each route entry a list of active neighbors is also maintained. A neighbor is considered active if it originates or relays at least one packet for that destination within the most recent ACTIVE_TIMEOUT period. All routes in the route table cache are tagged with destination sequence numbers which guarantees that no routing loops can form, even under extreme conditions of out-of-order packet delivery and high node mobility. The sequence number also helps in checking the freshness of a route, the greater the sequence number the more fresh a route is.

Several extensions have been proposed to the basic AODV routing protocol [11, 12]. Some of the most prominent ones have been accepted as part of standard AODV. One such modification is use of link layer feedback to maintain neighborhood information instead of periodic hello messages [13]. Another modification is the use of expanding ring search for route request packets. Instead of sending a network wide broadcast for a RREQ, the source node starts out by sending a limited broadcast (done by setting the TTL (time to live) field in the packet to TTL_START). If this broadcast fails (indicated by a timeout) to find a route to the destination then the source increases the previous TTL value by TTL_INCREMENT and sends out another broadcast with the higher TTL value. This process is repeated till the TTL value reaches TTL_THRESHOLD after which the source sends out a broadcast with TTL equal to NETWORK_DIAMETER. If this broadcast also fails to discover a route to the destination then such broadcasts are sent again upto RREQ_RETRIES. If still a route cannot be found then all the packets queued for that destination are dropped. When RREQ_RETRIES is 0, the timeout for each RREQ is calculated as

$$\text{Timeout} = \text{Min}\,(2.0 * \text{TTL} * \text{LINK\_TRAVERSAL\_TIME}, \text{MAX\_RREQ\_TIMEOUT})\ .$$

Here LINK_TRAVERSAL_TIME is the time taken to traverse a link and MAX_RREQ_TIMEOUT is the maximum possible value of the timeout. When RREQ_RETRIES is greater than 0 then the timeout of each RREQ is calculated as

$$\text{Timeout} = \text{Min}\,(2.0 * \text{TTL} * \text{LINK\_TRAVERSAL\_TIME} * \text{RREQ\_RETRIES}, \text{MAX\_RREQ\_TIMEOUT})\ .$$

Fig. 2 show the entered values in the text boxes in order to construct the working scenario. The values on which the current scenario would operate are mentioned on the right side of Fig. 2.

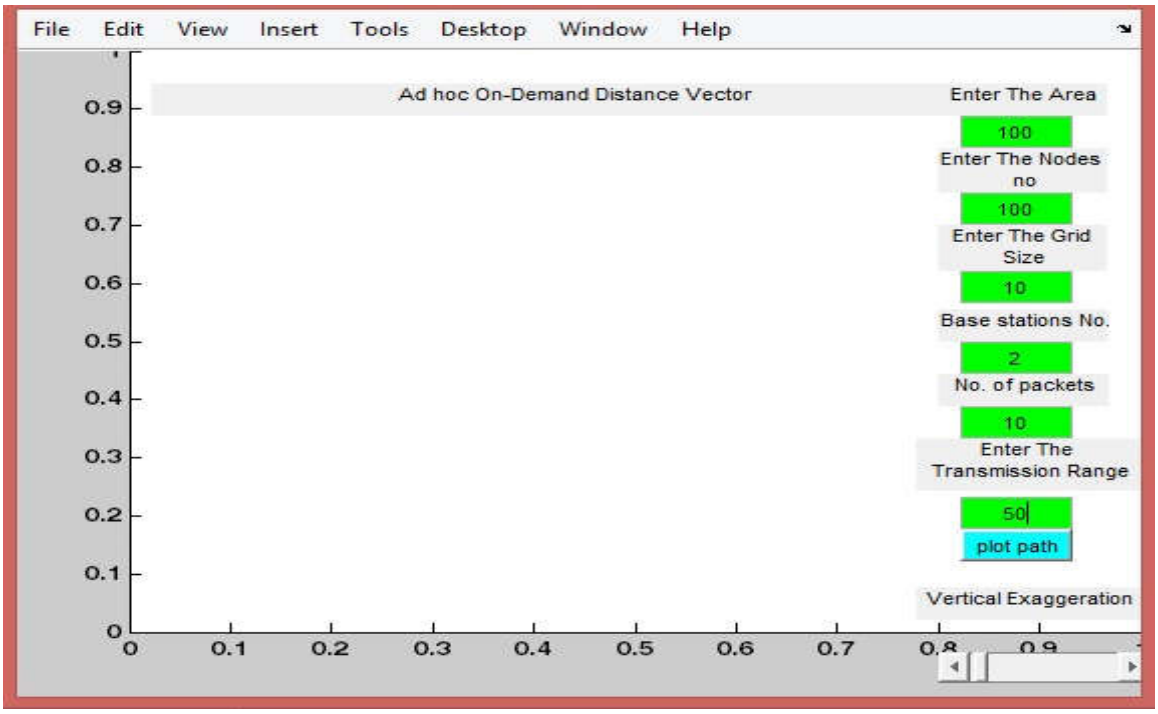

Fig. 2 The figure shows the entered values in the appropriate text boxes which would be used to construct the scenario under study

Fig. 3 shows the created scenario based on the values shown in Fig. 2. Fig. 3 shows the creation of two base stations. The first base station is targeted by three packets whereas second base station in targeted by seven packets.

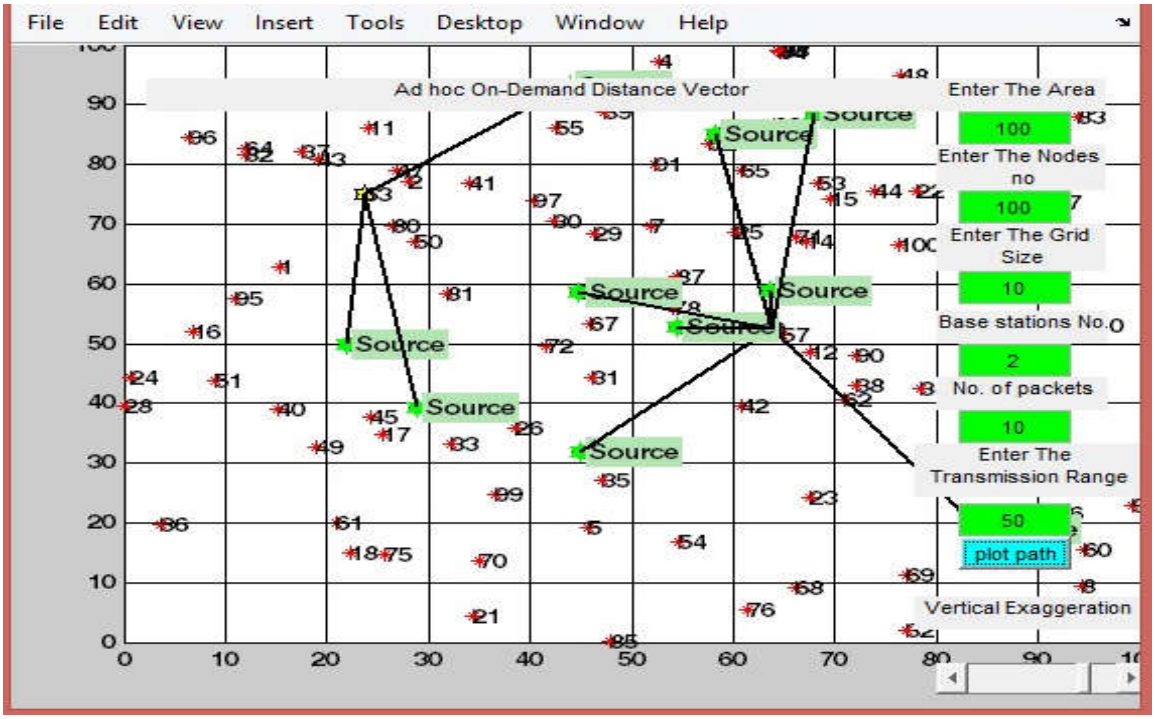

Fig. 3 The figure shows the constructed scenario based on AODV

Distance Vector Routing Protocol

DVR (Distance Vector routing) protocols are the simplest among Routing Protocols [14, 15]. Distance vector routing protocols use the distance and direction (vector) to find paths to destinations. A router which is running a Distance Vector routing protocol informs its neighbors about the network topology changes periodically, using limited broadcasts using destination IP address 255.255.255.255. Distance Vector protocols use the Bellman-Ford algorithm for finding best paths to destinations. Routers running Distance Vector protocols learn who their neighbors are by listening for routing broadcasts on their interfaces. Distance Vector protocols periodically send local limited broadcasts (255.255.255.255) to share routing information. Distance Vector algorithms pass routing table updates to their immediate neighbors in all directions [16, 17]. At each exchange, the router increments the distance value received for a route, thereby applying its own distance value to it. The router who received this update again pass the updated table further outward, where receiving routers repeat the process. The Distance Vector protocols do not check who is listening to the updates which they sent and Distance Vector protocols broadcast the updates periodically even if there is no change in the network topology. These are easy to set-up and troubleshoot. These require less router resources. These receive the routing update, increment the metric, compare the result to the routes in the routing table, and update the routing table if necessary. Examples of DVR are RIP, IGRP, and EIGRP [18, 19].

Fig. 4 to Fig. 8 shows the working of distance vector protocol in an environment having five nodes.

Fig. 4 shows the biograph view of the created scenario having five dynamically positioned nodes connected to each other with appropriate weights been displayed on each edge.

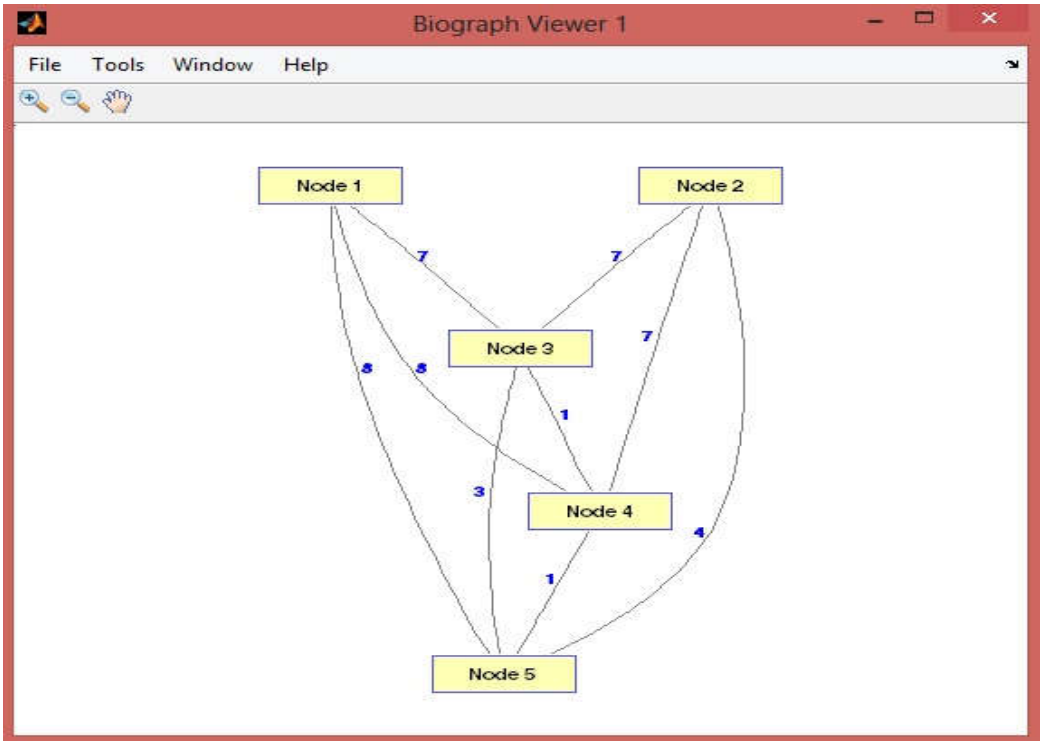

Fig. 4 The figure shows the created scenario comprising five nodes

After the scenario is created, the source node and the destination node needs to be entered. In this case under study, the entered source node in node 1 and the entered destination node is node 5 as shown in Fig. 5.

```
Enter the source node: 1
Enter the destination node: 5
     1     5
```

Fig. 5 The figure displays the entered node and the destination node

Fig. 6 shows the biograph view of the most appropriate path between node 1 and node 5. The node 1 (green color) represents the source node and the node 5 (red color) represents the destination node. Some of the possible paths connecting node 1 and node 5 along with their individual total weights are mentioned as under.

Node1 – Node 3 – Node 4 – Node 5 = 9

Node1 – – Node 4 – Node 5 = 9

Node1 – Node 5 = 8

Node1 – Node 3 – Node 5 = 10

Node1 – Node 3 – Node 2 – Node 5 = 18

Node1 – Node 4 – Node 2 – Node 5 = 19

Node1 – Node 4 – Node 3 – Node 2 - Node 5 = 20

The red colored edge having weight 8 directly connecting Node 1 to Node 5 shows the best path connecting the two nodes.

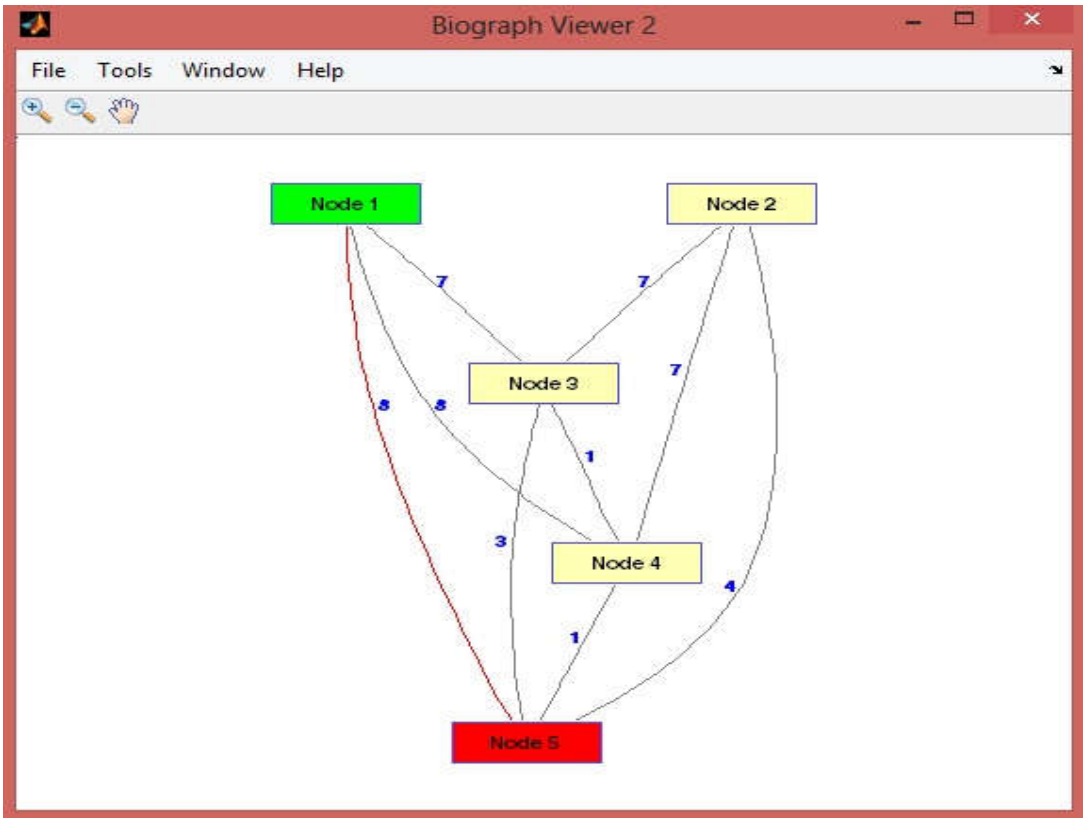

Fig. 6 The figure shows the biograph view

III. CONCLUSION

Due to the dynamic nature of MANETs, designing communications and networking protocols for these networks is a challenging process. One of the most important aspects of the communication process is design of the routing protocols which are used to establish and maintain multi-hop routes to allow the data communication between nodes. A considerable amount of research has been done in this area, and many multi-hop routing protocols have been developed. The research paper elaborated the working of AODV and DVR under dynamic circumstances. Both the implementations were done using Matlab as a simulation tool.

REFERENCES

[1] Gupta, S.K. and Saket, R.K., "Routing Protocols in Mobile Ad-hoc Networks", The International Conference on Electronics, Information and Communication Engineering; Jodhpur (Rajasthan), 2011, pp. 1-5.

[2] Singh, R. et al., "Ant Colony Optimization—Computational swarm intelligence technique", *Computing for Sustainable Global Development (INDIACom), 2016,* pp. 1493-1499.

[3] Zungeru, A. M., Ang, L. M., & Seng, K. P., "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison", *Journal of Network and Computer Applications*, *35*(5), 2012, pp. 1508-1536.

[4] Geetha, R., & Srikanth, G. U., "Ant Colony optimization based Routing in various Networking Domains–A Survey", *International Research Journal of Mobile and Wireless Communications*, *3*(01), 2012, 424-428.

[5] Batth KK, Singh R; **"**Performance Evaluation of Ant Colony Optimization Based Routing Algorithms for Mobile Ad Hoc Networks", International Journal of Advancements in Technology, DOI: 10.4172/0976-4860.1000181, March 2017.

[6] Prasad S., Zaheeruddin; **"**A Review and Comparison of Quality of Service Routing In Wireless Ad Hoc Networks", *International Journal of Wireless & Mobile Networks (IJWMN)*, DOI : 10.5121/ijwmn.2011.3115 172, Vol. 3, No. 1, February 2011.

[7] Goswami S., Das CB., "Reactive and Proactive Routing Protocols Performance Metric Comparison in Mobile Ad Hoc Networks NS 2", *International Journal of Advanced Research in Computer and Communication Engineering ,* ISSN (Online) : 2278-1021, ISSN (Print) : 2319-5940, Vol. 3, Issue 1, January 2014, pp. 4908 – 4914.

[8] K. Devi1, S. Rinesh; "Energy Efficient Path Determination in WANET", International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 3, Issue 2, February 2015, pp. 740 – 744.

[9] Sharma SK, "An Approach in Optimization of Ad-Hoc Routing Algorithms", International Journal of Distributed and Parallel Systems (IJDPS), DOI : 10.5121/ijdps.2012.3310, Vol.3, No.3, May 2012, pp. 101-110.

[10] Singh, R. et al., "A Comprehensive Review of Simulation Tools for Wireless Sensor Networks (WSNs)", *Journal of Wireless Networking and Communications*, *5*(1), 2015, 19-47.

[11] Sharma, S. et al., "A Survey on Coverage and Connectivity Issues Surrounding Wireless Sensor Network", *IJRCCT*, *3*(1), 2014, pp. 111-118.

[12] Goyal, D., & Tripathy, M. R., "Routing protocols in wireless sensor networks: A survey", *Second International Conference on Advanced Computing & Communication Technologies, 2012,* (pp. 474-480).

[13] Keerthi, S., Ashwini, K., & Vijaykumar, M. V. (2015). Survey Paper on Swarm Intelligence. International Journal of Computer Applications, 115(5).

[14] Di Caro, G. A. (2014). Principles of swarm intelligence for adaptive routing telecommunication networks. *Sistemi intelligenti*, *26*(3), 443-464.

[15] Zheng, J., & Jamalipour, A. (2009). *Wireless sensor networks: a networking perspective*. John Wiley & Sons.

[16] Misra, S., Zhang, I., & Misra, S. C. (Eds.). (2009). *Guide to wireless sensor networks*. Springer Science & Business Media.

[17] Saleem, M., Di Caro, G. A., & Farooq, M. (2011). Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions. *Information Sciences*, *181*(20), 4597-4624.

[18] Zengin, A., & Tuncel, S. (2010). A survey on swarm intelligence based routing protocols in wireless sensor networks. *International Journal of Physical Sciences*, *5*(14), 2118-2126.

[19] Ali, Z., & Shahzad, W. (2011, July). Critical analysis of swarm intelligence based routing protocols in adhoc and sensor wireless networks. In *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on* (pp. 287-292).