Volume 3, Issue 4, April 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Performance Analysis of SRTLD and BIOSARP Protocols in Wireless Sensor Networks

Mojtaba GhanaatPisheh Sanaei
Faculty of Computer Science and Information system
Universiti Teknologi Malaysia (UTM)
Johor 81310, Malaysia

Babak Emami Abarghouei
Faculty of Computer Science and Information system
Universiti Teknologi Malaysia (UTM)
Johor 81310, Malaysia

Hadi Zamani
Faculty of Computer Science and Information system
Universiti Teknologi Malaysia (UTM)
Johor 81310, Malaysia

Abstract— With the growing of wireless network technology researchers find that Wireless Sensor Network (WSN) is one the newest technology to make the life more comfortable and interesting. Security is needed to ensure the communication between the sensor node which is already a part from the same network and not outside intruder or attacker. To guarantee implementing the security in wireless sensor network, there are many protocols coming into the picture; this project selects the recent two protocols SRTLD and BIOSARP for critical analysis and investigation. After comparing the power consumption and delivery ratio to guarantee long life time for sensor node and to ensure the wireless senor network is working probably. According to what we reviewed there is an essential need to critical analyzes the recent security protocols in WSNs to determine which protocol is suitable for each network and application type. Two different security protocols for wireless sensor networks (WSN) will be analyzed to study the most effective protocol. After implementing BIOSARP and SRTLD using NS-2 simulator the project found that SRTLD is better energy consumption by 16.82%, but in delivery ratio BIOSARP is better by 4.21%.

Keywords— Secure Real-Time with Load Distribution, Biological Inspired Self-Organized Secure Autonomous Routing Protocol, Power Consumption, Wireless Sensor Network.

I. INTRODUCTION

Wireless sensor network is an infrastructure comprised of sensing, measuring, computing, and communication elements that give an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or information technology (IT) framework [1]. Wireless sensor network (WSN) has momentous applications like remote environment monitoring and target, these sensors are provided with wireless interface those wireless ports can combine a network by communicating to each other's. Sensor network one of the ad hoc mobile networks.

In wireless sensor networks there are several protocols, however this report will focus on analysis of two security protocols; (SRTLD) routing protocol that depends on the optimal forwarding (OF) decision which takes into account the link quality (LQ), packet delay time, remaining power of next hop sensor nodes and possesses built-in and an enhanced security measure. The other protocol is BIOSARP [2, 3, 4] which was developed from a conceptual design, taking into account the required features of having self-optimized routing and autonomous network security. WSN protocols are carried out every time when any node in WSN tries to send data to other nodes in WSN network and ensure the date is going to attended receiver. Different types of malicious attacks, such as impersonating, masquerading, interception for misleading because of the wireless connectivity, the absence of the physical protection and the unattended deployment. Therefore, security in sensor network is extremely important [5].

There is an essential need to analyze the recent protocols in WSN to determine which protocol is suitable for each network and application type. Two different protocols for wireless sensor networks (WSN) are analyzed to study the most effective protocol taking into account limitation of energy and delivery ratio to guarantee along live time for sensor nodes battery and to ensure our network is working in critical applications for example military field, industrial environment, health monitoring etc. There is an essential need to analyze the contemporary WSN protocols to determine the weakness, strength and the efficiency of those WSN protocol in term of packet delivery ratio. The aim of this papert is to identify the weakness, strength and the efficiency of wireless sensor network security protocols taking into account delivery ratio and energy consumption.

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. Wireless Sensor Network Security Protocols

WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, WSN may face various attacks. Probabilistic QoS(Quality of Service) guarantee in reliability and timeliness domains in wireless sensor networks (MM-SPEED) [6]. MM-SPEED designed to hold up multi-path forwarding, multiple communication speeds and to provide service differentiation and probabilistic QoS ensures in timeliness and reliability domains.

The features of MM-SPEED are decrease WSN lifetime due to load distribution is not studied. The problem of MM-SPEED the Power consumption is not taken into account. Another protocol is Research on Wireless Sensor Networks Routing Protocol for Wetland Water Environment Monitoring (LQER) [7], main advantage of this protocol It proposes a link quality estimation based routing protocol (LQER) to meet the high reliability of transmitting data in water environment. But the drawbacks of (LQER) are divided into two; first Packet deadline is not considered and second the Link quality is based on network layer which waste time and power. In High-throughput Path Metric for Multi-hop Wireless Routing By [8] main feature it decreases WSN lifetime due to load distribution is not studied. And drawbacks are Packet deadline is not considered and Link quality is based on network layer which waste time and power. In [9] proposed QoS and energy aware routing for real-time traffic in wireless sensor networks. The main feature of this protocol is to balances node energy utilization to increase the network lifetime, takes network congestion into account to reduce the routing delay across the network and increases the reliability of the packets reaching the destination by introducing minimal data redundancy, but the drawback that it increases power consumption because packet always forwarded to the nearest neighbour. It maximizes the number of hops between the source and destination that increases end to end delay. SPINS is a security mechanism for wireless sensor networks it is made of the SNEP protocol which is used to provide confidentiality in the network and μTESLA protocol which is used to authenticate data before broadcasting, however we will focus on the negotiation protocol [10, 11]. BROSK Compared to SPINS can be considered a more recent Ad-hoc key negotiation protocol. In this scheme, there is no trusted party or server and each node directly negotiates a session key with its neighbors by broadcasting a key negotiation message. Once a node receives this message, it can construct the shared session key by generating the MAC of two nodes [12]. For BROSK proposal there is no mention is found about what is done with the master key once the broadcasting process has finished, so it is assumed that the master key is not erased or processed in a special way. If this assumption is true, the scheme would be vulnerable to physical intrusion, and the same drawback is to SPINS [11]. However, a stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. Though, weak security protocols can be broken easily by attackers. In the next section this project will explain about BIOSARP and SRTLD protocols [5]. The wireless sensor network modeling and routing strategies are receiving much preference, the security challenges do not receive extensive center of attention. It is very important that the security concerns be addressed from the beginning of the system design [13]. It is easier to suffer all kinds of attacks, if the sensor nodes are deployed in the environment that is unprotected or hostile because of resource limitation and vulnerabilities of wireless communication. As reported by [14], these attacks occupy signal jamming and spoofing, sinkhole attacks, selective forwarding, eavesdropping, tempering, resource exhaustion, altered or replayed routing information, Sybil attacks, wormhole attacks, flooding attacks and the rest.

Though, the reactive measures based on encryption and authentication can reduce interruption to some extent but cannot eradicate them at all. An uncomplicated example is that these two measures take no effect on these attacks caused by these compromised nodes with legal keys. In this case, the second secure defense of WSN to further reduce attacks and insulate attackers can be Intrusion Detection System (IDS). In conventional networks, traffic and computation are typically monitored and analyzed for anomalies at different concentration points. Conversely, this is often expensive in terms of energy and networks memory consumption and also its naturally limited bandwidth. Wireless sensor networks require a solution that is distributed and reasonably priced in terms of energy, memory requirements and communication. Consequently, new techniques must be developed to make intrusion detection perform efficiently or otherwise the IDS traditional techniques must be improved for WSN.

A. Secure Real-Time with Load Distribution (SRTLD)

Provides secure real-time data transfer and less energy consumption usage in WSN. The SRTLD routing protocol ensures high packet throughput and reduced packet overhead. It has been effectively studied and verified through simulation and real time experiment implementation [15]. Secure real-time with load distribution (SRTLD) routing protocol that depends on optimal forwarding (OF) choice that that uses the link quality (LQ), packet delay time, and the unconsumed power of next hop sensor nodes. It owns built-in and an improved security measure. The random chosen of a next hop node using multi-path forwarding and location aided routing will enhance to build-insecurity measure. The encryption and decryption with authentication of the packet header additional enhancement secure packet transfer. The SRTLD routing protocol in WSN has been effectively studied and confirmed by simulation and real-time implementation [15].

B. Biological Inspired Self-Organized Secure Autonomous Routing Protocol (BIOSARP)

IEEE 802.15.4 is the one of the most famous development establishing the possible deployment of WSN systems. In physical (PHY) and Medium Access Control (MAC) layer devoted for Low-Rate Wireless Personal Area Network (LR-WPAN) IEEE 802.15.4 is specified. IEEE 802.15.4 is important in developing a standard, and that should not rely on existing technologies like Bluetooth or WLAN, so that to guarantee low complexity with energy efficient operations. IEEE 802.15.4 offers low-cost solution, energy efficient and it is simple compared to a wide multiplicity of applications. [16] State that IEEE 802.15.4 standard supports one hop star network and multi-hop peer-to-peer network.

III. SIMULATION PARAMETERS

This chapter starts by implementation and specifically declares our network parameters to simulate SRTLD and BIOSARP in network simulator -2. After that it goes down to the network model used for implementing of the two protocols. Tow evaluation metrics are employed to compare two of the contemporary wireless sensor network protocols, one of them is SRTLD which is designed by [10] another one is BIOSARP which is designed by [3] as a current using protocols in wireless sensor network. First parameter in comparison is delivery ration and after will address power consumption results.

TABLE I
SIMULATION PARAMETER VALUE

Simulation Parameters	*Value*
Propagation Model	Shadowing
Application traffic	CBR
path loss exponent	2.45
shadowing deviation	4.0 db
reference distance	1.0 m
Operation mode	Non Beacon (unslotted)
Transport layer	UDP
Power transmission	1 mW
Initial Energy	3.6 Joule
Number of malicious nodes	4,8,12, 16
Pause time	10 s
Simulation Time	500 s
Simulation area (m2)	80*80
Number of Node	120

IV. RESULTS AND DISCUSSIONS

In this part the study will go to explain the comparison between SRTLD and BIOSARP protocol in terms of packet delivery ratio and power consumption.

A. Packet Delivery Ratio

Packet Delivery Ratio (PDR): The PDR can be estimated as the ratio of the number of delivered data packet to the destination and the number of data packets that are sent by the source. Figure 3 shows as the count of node increase it gets better because contingency of route breakage decrease. For calculating the PDR the following formula can be used:

$$PRD = \frac{\sum \text{ Count of packet receive}}{\sum \text{ Count of packet send}} \quad (1)$$

Figure 1 below show that SRTLD performance is good than BIOSARP in case of using four malicious nodes attack implemented wireless sensor network.

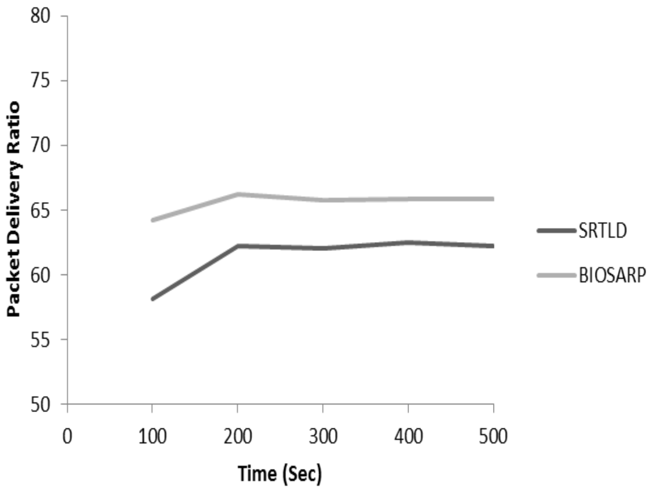

Fig. 1 Delivery ratio comparisons between SRTLD and BIOSARP in (4) malicious nodes

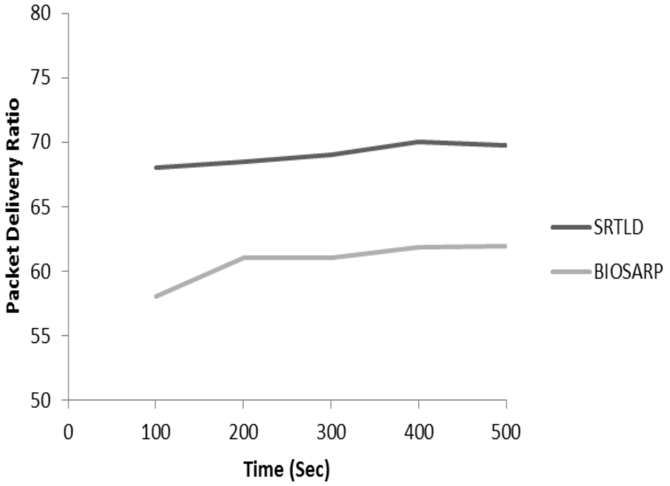

Fig. 2 Delivery ratio comparisons between SRTLD and BIOSARP in (8) malicious nodes

As showed in Figure 1 above shown that SRTLD delivery ratio performance is decreased by increasing the number of malicious node to eight nodes, but still it’s better than BIOSARP in small number of malicious nodes attack.

Figure 3 below show that SRTLD delivery ratio performance is better than BIOSARP at the beginning simulation time of the scenario used 12 malicious nodes to attack our wireless sensor network; nevertheless BIOSARP performance is better in higher simulation time. In contrast SRTLD delivery ratio will become lower than BIOSARP after mentioned simulation time.

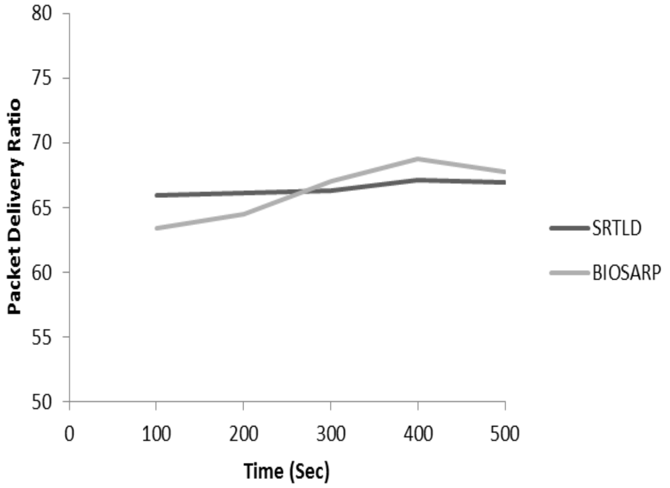

Fig. 3 Delivery ratio comparisons between SRTLD and BIOSARP in (12) malicious nodes

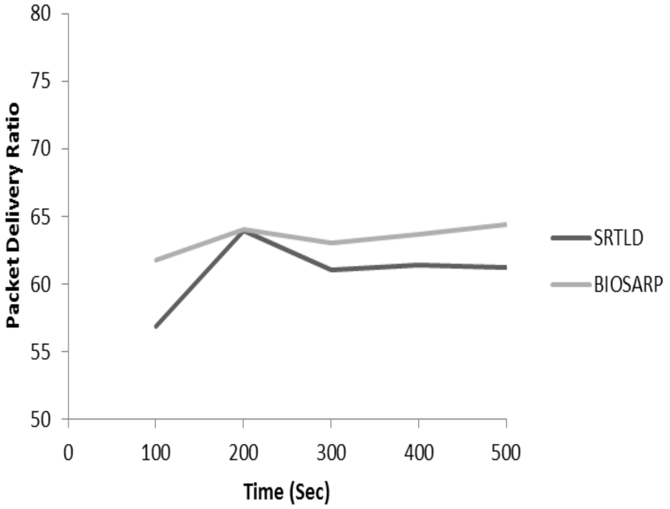

Fig. 4 Delivery ratio comparisons between SRTLD and BIOSARP in (16) malicious nodes

In Figure 4 above shown that BIOSARP delivery ratio performance is better than SRTLD at in scenario used (16) malicious nodes to attack implemented wireless sensor network, consequently BIOSARP performance is better in environments facing a lot of number of attacks (e.g.: selective forwarding; spoofed or altered, sinkhole attacks, acknowledgement spoofing Sybil attacks, replayed routing information, wormholes and HELLO flood attacks).

The simulation results show that the delivery ratio of BIOSARP is higher up to 4.21% as compared to the SRTLD protocols. Delivery ratio is increased because the data packets are processed in very short time duration. The reduction in processing time ultimately helps in decreasing the delay while transferring data packets from source to destination securely. SRTLD has better delivery ratio than BIOSARP when number of source nodes is increased to four from one and make the network under attacking from different eight malicious nodes, so the of delivery ratio SRTLD will be better by 2.19% than BIOSARP.

B. Power Consumption

In this part the study will go to explain the comparison between SRTLD and BIOSARP protocol in term of power consumption.

Power Consumption: energy consumption is defined as the consumption, using and spending of energy or power [17]. The result gained after run the NS-2 simulator with 120 nodes to check the performance of SRTLD and BIOSARP regards to power consumption parameter.

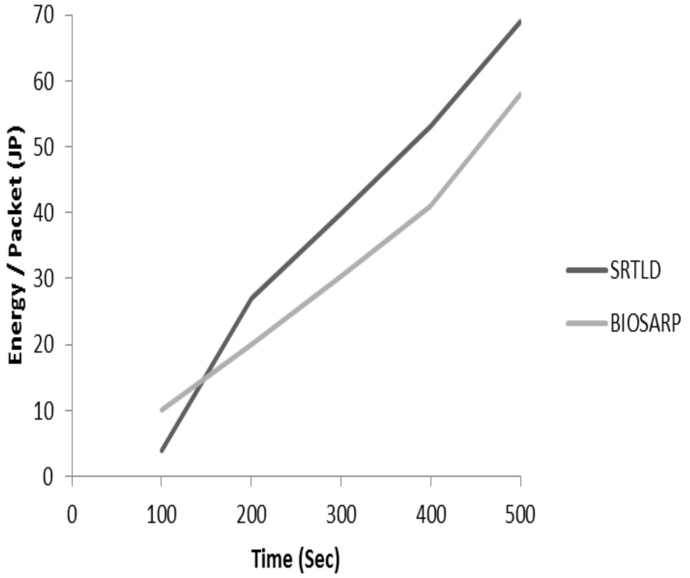

Fig. 1 Energy consumption comparisons between SRTLD and BIOSARP protocols with 4 malicious nodes

In Figure 1 above shown that SRTLD energy consumption is better than BIOSARP. SRTLD energy consumption is better than BIOSARP as show In Figure 2 below. The result clearly show view the power consumption is increasing with increasing the simulation time for both BIOSARP and SRTLD protocols.

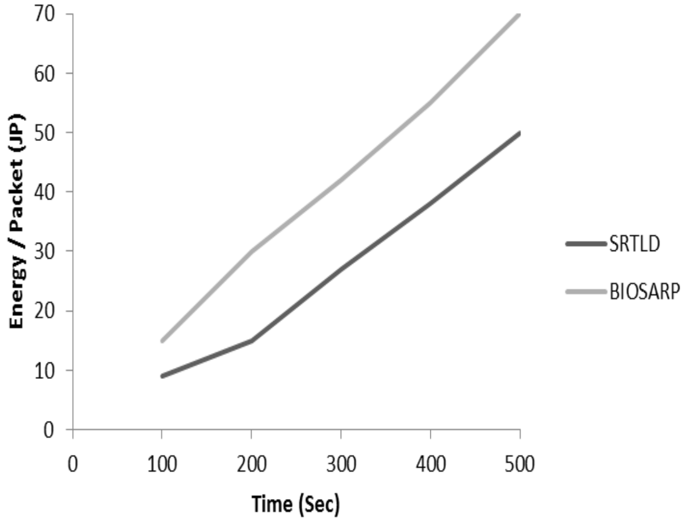

Fig. 2 Energy consumption comparisons between SRTLD and BIOSARP protocols with 8 malicious nodes

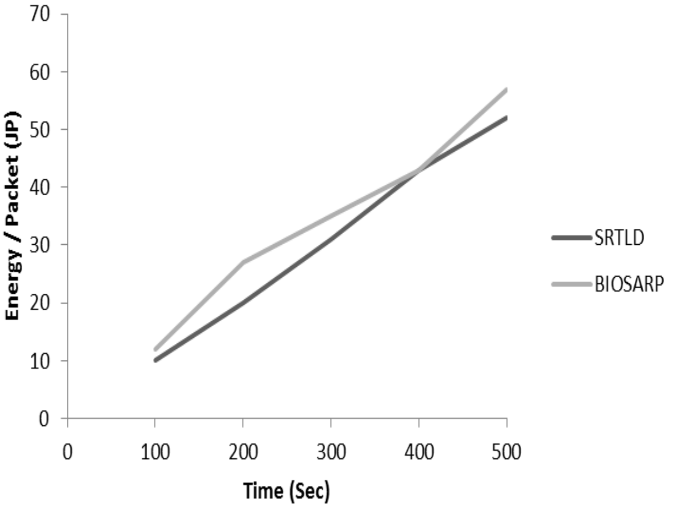

Fig. 3 Energy consumption comparisons between SRTLD and BIOSARP protocols with 12 malicious nodes

BIOSARP energy consumption is higher than SRTLD as show In Figure 3 above. The result shown the energy consumed by SRTLD is higher compared with previous result; because of increased number of malicious nodes. And completely contrary to BIOSARP it is power consumption coming better compared with previous result.

In Figure 4 below BIOSARP energy consumption is still higher than SRTLD. The Comparison using sixteen malicious nodes, only one source node and sink node.

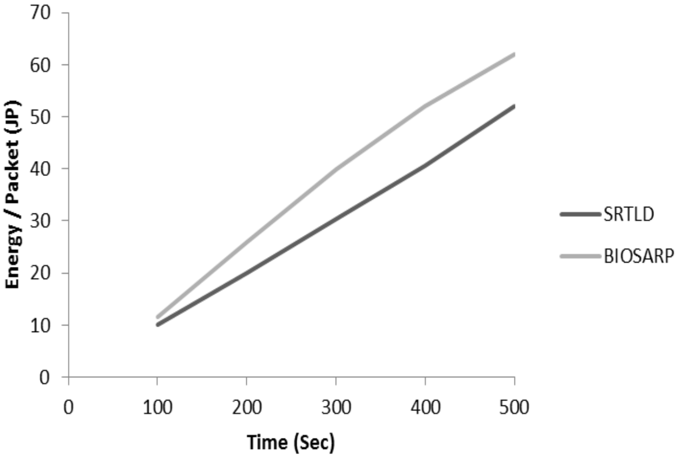

Fig. 4 Energy consumption comparisons between SRTLD and BIOSARP protocols with 16 malicious nodes

SRTLD reduce the processing delays and hence the battery power consumption. As shown in result also SRTLD consumes up to 16.82% less power in front of BIOSARP protocols. The reduced power consumption helps in increasing life of WSN. BIOSARP is consuming less power than SRTLD when number of source nodes is increased to four from one and make the network under attacking from different eight malicious nodes, so the total power consumption of BIOSARP in this case will be 11.7%.

V. Conclusions

After finding, the study achieved its objective by simulating results in an attacked WSN environment situation of sixteen malicious nodes and one source node and less network load. SRTLD consumes less energy by 16.82% than BIOSARP and less delivery ratio by 4.21%. In an attacked WSN environment situation with eight malicious nodes , four source nodes and heavy network load, BIOSARP consumes less energy by 11.7% than SRTLD, while BIOSARP provides better and high delivery ratio by 2.19%. In the case of SRTLD the delivery ratio decreases soon due to massive broadcast at every hop. Hence, this report finally concludes that BIOSARP performs better in heavily loaded and attacked real time WSN due to its autonomous and self-optimized functionality.

References

[1] Sohraby, Kazem, Daniel Minoli, and Taieb Znati. Wireless sensor networks: technology, protocols, and applications. Wiley-Interscience, 2007.

[2] Saleem, Kashif, Norsheial Fisal, and Sharifah Hafizah. "BIOSARP: biological inspired self-organized secure autonomous routing protocol for wireless sensor network." In Proceedings of the 11th WSEAS international

conference on applied computer science, pp. 158-165. World Scientific and Engineering Academy and Society (WSEAS), 2011.

[3] Saleem, Kashif, Norsheila Fisal, Muhammad Sharil Abdullah, and Sharifah Hafizah Syed Ariffin. "Biological inspired secure autonomous routing mechanism for wireless sensor networks." International Journal of Intelligent Information and Database Systems 5, no. 4 (2011): 313-337..

[4] Saleem, Kashif, Norsheila Fisal, Sharifah Hafizah, and Rozeha Rashid. "An intelligent information security mechanism for the network layer of WSN: BIOSARP." Computational Intelligence in Security for Information Systems (2011): 118-126.

[5] Zhang, Junqi, and Vijay Varadharajan. "Wireless sensor network key management survey and taxonomy." Journal of Network and Computer Applications 33, no. 2 (2010): 63-75.

[6] Felemban, Emad, C-G. Lee, Eylem Ekici, Ryan Boder, and Serdar Vural. "Probabilistic QoS guarantee in reliability and timeliness domains in wireless sensor networks." In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 4, pp. 2646-2657. IEEE, 2005.

[7] Jiang, Peng, Qingbo Huang, Jianzhong Wang, Xiaohua Dai, and Ruizhong Lin. "Research on wireless sensor networks routing protocol for wetland water environment monitoring." In Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on, vol. 3, pp. 251-254. IEEE, 2006.

[8] Couto, Douglas SJ De, Daniel Aguayo, John Bicket, and Robert Morris. "A high-throughput path metric for multi-hop wireless routing." Wireless Networks 11, no. 4 (2005): 419-434.

[9] Mahapatra, Abinash, Kumar Anand, and Dharma P. Agrawal. "QoS and energy aware routing for real-time traffic in wireless sensor networks." Computer Communications 29, no. 4 (2006): 437-445.

[10] Baronti, Paolo, Prashant Pillai, Vince WC Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu. "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards." Computer communications 30, no. 7 (2007): 1655-1695.

[11] Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9, no. 5 (2011): 727-735.

[12] Lai, Bocheng, Sungha Kim, and Ingrid Verbauwhede. "Scalable session key construction protocol for wireless sensor networks." In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), p. 7. 2002.

[13] Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing (2007): 367.

[14] Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, vol. 2, pp. 6-pp. IEEE, 2006.

[15] Ali, A., and Norsheila Fisal. "Security enhancement for real-time routing protocol in wireless sensor networks." In Wireless and Optical Communications Networks, 2008. WOCN'08. 5th IFIP International Conference on, pp. 1-5. IEEE, 2008.

[16] Koubaa, Anis, Andre Cunha, and Mario Alves. "A time division beacon scheduling mechanism for IEEE 802.15. 4/Zigbee cluster-tree wireless sensor networks." In Real-Time Systems, 2007. ECRTS'07. 19th Euromicro Conference on, pp. 125-135. IEEE, 2007.

[17] Lai, Bocheng, Sungha Kim, and Ingrid Verbauwhede. "Scalable session key construction protocol for wireless sensor networks." In IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), p. 7. 2002.