ADAPTIVE REDUNDANCY-BASED TRANSMISSION FOR WIRELESS SENSOR NETWORKS

Jin Ren Ng[1*], Vik Tor Goh[1], Timothy Tzen Vun Yap[2], Mustaffa Kamal Shuib[3]

[1]*Faculty of Engineering, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia*
[2]*Faculty of Computing & Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Selangor, Malaysia*
[3]*Department of Geology, Faculty of Science, University of Malaya, 50603 Kuala Lumpur, Malaysia*

ABSTRACT

Wireless Sensor Networks (WSNs) are built upon tens to thousands of sensor nodes dispersed across a geographical area. Most sensor nodes have limited on-board resources, such as limited computing capabilities and limited power. These issues can reduce the reliability of the sensor nodes, which, in turn, affects the robustness of the WSN as a whole. One of the components that can be affected is the data transmission system of the sensor nodes. We propose a reliable transport layer protocol that uses a combination of redundant packets and probabilistic transmission to ensure reliable transmission of data while maintaining the efficiency of the network. The proposed protocol does not require acknowledgement packets, such as the transmission control protocol (TCP) and yet its efficiency is similar to that of the user datagram protocol (UDP). In this paper, we explain the proposed protocol and demonstrate how it can achieve 7% improvements in reliability while maintaining 77% efficiency compared to UDP.

Keywords: Efficiency; Redundancy-based; Reliability; Wireless sensor network

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a network system consisting of tens to thousands of wirelessly connected sensor nodes. These nodes collect data from the environment and send them to the receiver nodes. A receiver node is also known as a sink. It is used to receive and store the data collected from the sensor nodes. A typical WSN consists of multiple sensor nodes and one sink. The sensor nodes are dispersed across an area of interest, where the nodes will self-organize to form a wireless communication network. Since a single sensor node only contributes information about its immediate surroundings, multiple nodes collaborate with one another to provide better coverage over a large area.

Although WSNs can consist of only a few nodes (e.g., less than 10), their potential lies in scenarios where many nodes are deployed to monitor a large geographical area. This type of network is deployed to minimize manpower in monitoring a specific area. In certain cases, WSNs are deployed at ecologically sensitive or geographically restricted areas that are difficult for humans to access. For example, sensor nodes are deployed deep in forests, on top of mountains, and even on the slopes of hills. The remote locations and difficult operating conditions affect the

reliability of the sensor nodes. Ultimately, the reliability of the sensor nodes decreases, which, in turn, affects the effectiveness of the monitoring process. Thus, reliability is one of the main challenges faced by WSNs (Ali et al., 2018; Sumaryo et al., 2019). In this work, we look at how data transmission is affected and propose a transport layer protocol to mitigate the problem.

2. RELATED WORK

Multiple solutions have already been proposed, such as enhancing the hardware, creating new routing protocols, or designing new transport protocols. We focus on designing a transport layer protocol that ensures the reliability of the WSN when operating in a difficult environment. The proposed protocol is comparable to other transport layer protocols, such as the transmission control protocol (TCP) and the user datagram protocol (UDP), but with different properties and use cases. There are a few factors to consider when designing such a protocol. One example is the background noise when a network is deployed in a noisy radio environment or deep in the forest where the density of foliage could affect the communication link (Meng & Lee, 2010). In addition, the surrounding humidity and temperature are also parameters that can reduce the efficiency of the communication link and the reliability of the network.

The deployment topology and limitations of WSN make it susceptible to failures (Berawi et al., 2016). For example, network connectivity may fail due to battery failure, the nodes may become unresponsive because of a lack of processing power, or the communication link within the network could become unreliable due to interference from surrounding background noise. While commonly used transport protocols, such as TCP and UDP, can be used, they may not be optimized for WSN. For instance, although TCP guarantees the reliability of the network system, it uses more resources to do so. Specifically, TCP requires a three-way handshake for every new establishment of connection between the sensor nodes. It also needs acknowledgement (ACK) back from the sink for every packet sent. As a result of the additional ACK requirement and the properties of TCP, TCP packets require larger headers. Meanwhile, UDP is simple to implement and requires less resources for data transmission, but it does not guarantee reliability. Therefore, our research interest is in designing a transport protocol that offers reliability like TCP but without the need for TCP's connection setup and teardown, thus simplifying the protocol to be as straightforward as UDP.

In general, transport layer protocols in a network are used to ensure the reliability of the packet transmission, reduce the packet loss, and perform fair bandwidth allocation (Chonggang et al., 2006). Whereas, the transport layer protocol in WSN should not only support a reliable message delivery, but it also needs to focus on the efficient use of scarce resources. Marchi et al. (2007), Raghavendra et al. (2004), and Kazem et al. (2007) concluded that transport layer protocols for WSNs should also simplify the connection setup to improve the throughput and reduce transmission delays, minimize packet transmission to avoid the wasting of resources, and guarantee fairness over all sensor nodes.

Muhammad et al. (2015) listed two approaches to solve the reliability issues, namely, using redundancy- and retransmission-based approaches. Redundancy-based approaches achieve the desired reliability by sending redundant packets or including error correction codes. These error correction codes can correct bit-level errors, while extra packets can replace the lost packets. Retransmission-based techniques emphasize guaranteed transmission by accounting for each packet and retransmitting any missing packets.

There are several types of redundancy-based techniques, such as those by Srouji et al. (2011) and Al-Awami and Hassanein (2012), where erasure coding is included, and those by Winston and Hwee (2006) and Budhaditya et al. (2003), where extra packets are sent through multiple

path routing. Bhisham and Trilok (2012) stored an extra cache of the packets in the intermediate nodes for redundancy.

For retransmission-based protocols, techniques, such as those of Celimuge et al. (2012), send multiple copies of each message to the receiver. As it is an adaptive protocol, it does not always send message copies twice. In order to prevent any unnecessary waste of resources, it only retransmits a message when the link quality has dropped below a threshold or if end-to-end delay is above a threshold, thus indicating congestion. Other researchers have focused on optimizing the frequency of retransmission so that the network will not be unnecessarily congested by multiple copies of the same message. In a study by Yogesh et al. (2003), the authors proposed a reliable transport protocol named Event-to-Sink Reliable Transport (ESRT), while Sunil et al. (2009) proposed an enhanced version of ESRT, named E2SRT. ESRT has its own congestion control scheme and tends to make the network operate in its optimal operating region (OOR) where the network is reliable and has no occurrence of congestion.

In this research, we focus on techniques that send multiple copies of each message, such as those proposed by Celimuge et al. (2012). However, sending multiple copies of messages will eventually decrease the efficiency of the network. Celimuge et al. (2012) did not consider the effect of their proposed technique on network efficiency. As such, this research aims to achieve the desired reliability through retransmission while maintaining the optimum efficiency.

3. METHODS

In this section, we present the design of two redundancy-based transport layer protocols, namely, the basic protocol and its extension, the probabilistic protocol. We have used OMNET++ (Varga, 2010) as the simulation tool to evaluate the performances of both redundancy-based protocols.

3.1. Design of a Basic Redundancy-based Protocol

As mentioned in Section 2, a redundancy-based protocol achieves the desired reliability through the usage of redundant data. In this basic protocol, a packet is duplicated and sent as a redundant packet. This is done for every packet sent. Therefore, two copies of each packet are sent from the sender to the receiver. The overall idea of this redundancy protocol is shown in Figure 1.
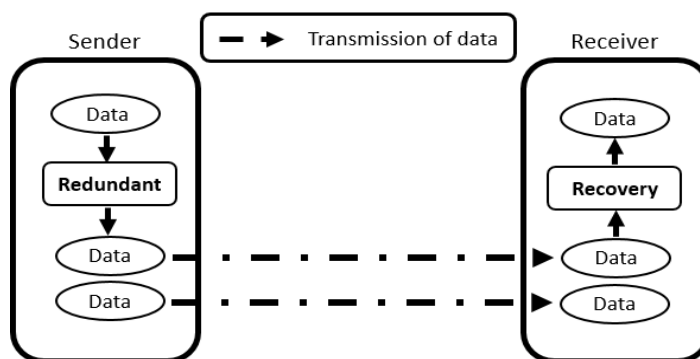

Figure 1 Basic redundancy-based protocol

As shown in Figure 1, the data sent from the sender will undergo a duplication process in which the original data is duplicated, two identical copies of data are obtained. Then, both copies of the data are transmitted to the receiver. Each original packet is given a unique identification (msgID), but every identical duplicated packet holds the same msgID as its original packet. Once both data copies have arrived at the receiver, the data will undergo a recovery process. Received packets that contain both the original and duplicated packets are recovered to only one packet.

This process is done by checking the msgID, and, if two packets have the same msgID, one of the packets is kept and the other is dropped. In a very noisy environment, packets may be lost during transmission; hence, sending redundant packets can increase the packet receive rate.

However, the number of duplicates for each packet does not have to be constrained to just two packets. Instead, it can be adjusted according to the surrounding environment. In noisier environments, more duplicates of each packet are needed in order to increase the reliability of the transmission. Although constantly sending multiple copies of the same packet can increase reliability, the overall efficiency of the network will drop due to the duplicated packets created by the redundancy-based protocol.

3.2. Design of a Probabilistic Redundancy-based Protocol

Due to the drop in efficiency when the basic redundancy-based protocol is used, we propose an adaptive version instead. The adaptive version achieves an optimum level of reliability while maintaining the efficiency at a more acceptable level. The adaptive version is implemented using a probabilistic model in which the sender randomly decides to send duplicate packets or just the original packet. The decision is based on a uniform probability distribution. The sender sends duplicate packets based on a certain probability instead of constantly sending out redundant packets. The general idea of this probabilistic redundancy-based protocol is shown in Figure 2.
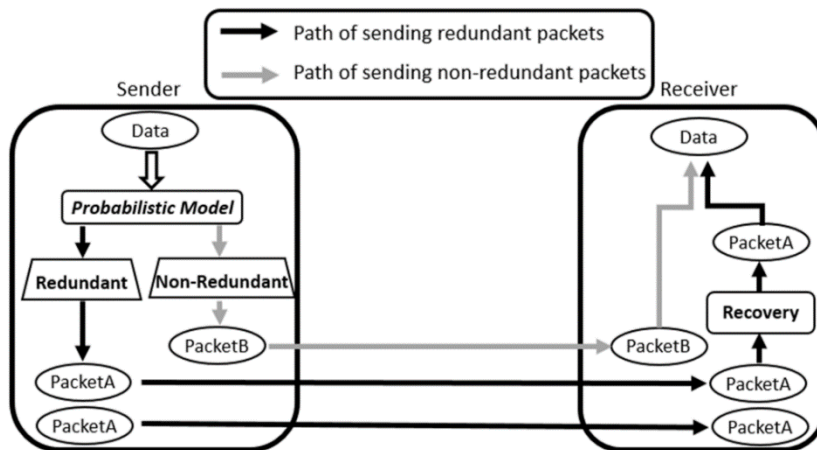

Figure 2 Probabilistic redundancy-based protocol

As shown in Figure 2, the data of this protocol undergoes a probabilistic model before sending duplicate packets. The probabilistic model configures the probability of sending duplicate packets based on the surrounding noise level. If the surrounding environment is very noisy, the probability of sending duplicate packets would be higher and, therefore, would result in higher reliability. If the data is chosen to be duplicated, the packet (PacketA) will be duplicated once, and both the packets will be transmitted to the receiver. Conversely, if the data is not chosen to be duplicated, only one packet (PacketB) will be transmitted to the receiver. Once the data have been successfully transmitted to the receiver, the packet from the non-redundant path will immediately be stored by the receiver. The packets from the redundant path will need to undergo a recovery process, in which only one packet is stored by the receiver and the other is dropped.

4. RESULTS AND DISCUSSION

To evaluate the proposed protocol, we simulated a basic wireless sensor network consisting of only two sensor nodes: a sender and a receiver. A straightforward topology was used in order to evaluate the genuine effects of the protocol, thus minimizing the effects of other factors related to the use of multiple nodes, such as network latencies or routing loops. We analyzed the performance of both the basic and probabilistic redundancy-based protocols at different noise

levels. In addition, we analyzed the relationship between the network's reliability and its efficiency in a noisy environment. We then found the optimum level for the probabilistic redundancy-based protocol based on the various noise levels.

4.1. Reliability and Efficiency vs. Noise Levels

As shown in Figure 3 and Figure 4, *UDP* provides normal packet transmission, and only a single packet is sent to the receiver. *Redundant-Basic* refers to the basic redundancy-based protocol in which two packets are sent (i.e., original and duplicate packets), and *Redundant-Probabilistic* refers to the probabilistic redundancy-based protocol for which the probability of sending a duplicate is set to 50%. Finally, *TCP* is the traditional retransmission protocol, which is able to achieve very high reliability.
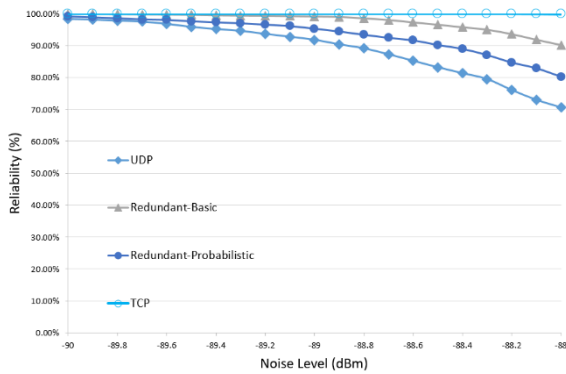

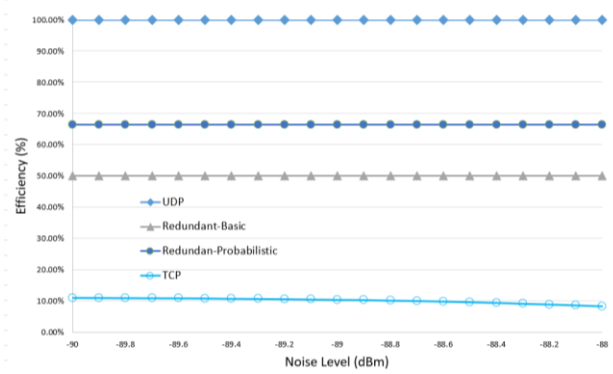Figure 3 Reliability vs. noise level   Figure 4 Efficiency vs. noise level

Using both graphs, we compared the results under two conditions: the minimum noise environment (-90 dBm) and the maximum noise environment (-88 dBm). Depicted in Figure 3, reliability is defined as the ratio of received packets over sent packets, as shown in Equation 1.

$$\text{Reliability} = \frac{Received\ Packets}{Sent\ Packets} \qquad (1)$$

In the case of the -90 dBm noise level, all four protocols had similar performances, and all of them achieved a reliability rate of more than 98%. However, for the -88 dBm noise level, *UDP* achieved the lowest reliability rate of 70%, followed by *Redundant-Probabilistic,* which achieved a reliability rate of 80%, *Redundant-Basic,* which achieved a reliability rate of 90%, and *TCP,* which achieved the highest reliability rate (100%). *TCP* was able to maintain the reliability throughout different noise levels due to the working principle of *TCP,* which includes the transmission of Acknowledgement (ACK) and the retransmission of the same packet, if the packet is not successfully received. This proves that sending redundant packets increases the reliability rate, but the trade-off is a decline in the efficiency of the network, as shown in Figure 4.

Depicted in Figure 4, efficiency is defined as the ratio of original packets over total packets sent (original packets and redundant packets), as shown in Equation 2.

$$\text{Efficiency} = \frac{Sent\ Packets\ (Original)}{Total\ Sent\ Packets\ (Original+Redundant)} \qquad (2)$$

The efficiency of all four protocols shows a constant straight line across the graph. While *TCP* achieved the highest reliability (100%) at the highest noise level of -88 dBm, as shown in Figure 3, it produced the lowest efficiency rate (only 10%), as shown in Figure 4. Meanwhile, *Redundant-Basic,* which achieved the second highest reliability in Figure 3, achieved only 50% efficiency in Figure 4. This is consistent with Equation 2 because, for every original packet that has to be sent, another packet is generated and transmitted together, resulting in an efficiency of

only 50%. Although *UDP* had the lowest reliability of 70%, the efficiency rate was the highest at 100%. Finally, *Redundant-Probabilistic* had an efficiency rate of 68%, falling between the efficiency rates of *Redundant-Basic* and *UDP*. Thus, in the maximum noise environment, the proposed *Redundant-Probabilistic* protocol improved the reliability rate by 10% when compared to *UDP*. It also improved the efficiency rate by 18% when compared to *Redundant-Basic* and by 58% when compared to *TCP*.

All four protocols provided similar reliability rates of more than 98% when the noise level was at its minimum (i.e., -90 dBm). However, *TCP*, *Redundant-Basic* and *Redundant-Probabilistic* could only do so at the cost of lower efficiency rates of 10%, 50%, and 68%, respectively. In comparison, the *UDP* protocol was able to achieve the highest reliability at a 100% efficiency rate.

In Figure 3 and Figure 4, the *Redundant-Probabilistic* protocol has its probability of sending a duplicate set to 50%. This parameter was not adaptable and did not change despite the varying levels of noise. Therefore, in order to identify the most optimum probability, the relationship between the various parameters (i.e., probability, reliability, and efficiency) will be examined below.

4.2. Effects of Probability on Reliability and Efficiency

We plotted the reliability rate for different probabilities while maintaining the noise at a constant level. This was also done for the efficiency rate. We set the noise level at -88 dBm and plotted both results, as shown in Figure 5. In the figure, we can observe that, while reliability increased with increasing probabilities, the efficiency dropped. This is consistent with the observations made regarding Figure 3 and Figure 4.

In order to identify the optimum probability for a given noise level, we identified the intersection point of the reliability and efficiency plots. This intersection point represents the optimum value of probability to send duplicate packets, and it guarantees the transmission reliability while providing the best efficiency. As shown in Figure 5, the optimum probability of sending redundant packets at the -88 dBm noise level was 32%. It provided 77% of reliability, as well as an equivalent level of efficiency. When compared with the results of *Redundant-Probabilistic* in Figure 3 and Figure 4, which provided a reliability of 80% and an efficiency of 68%, the current solution provided a 9% improvement in efficiency with only a 3% trade-off in reliability.
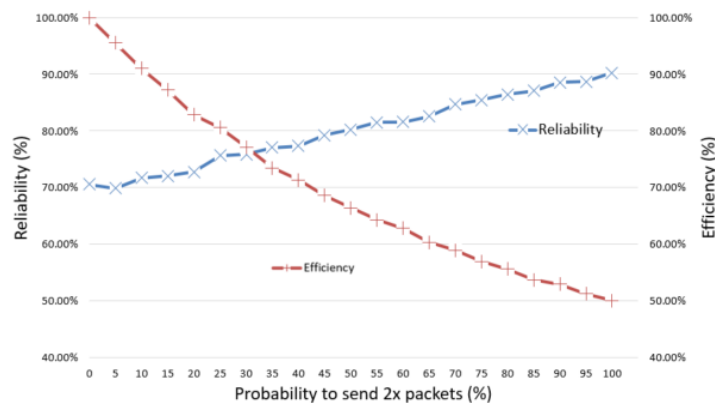

Figure 5 Relationship of reliability and efficiency for various probabilities of sending 2× packets at the -88 dBm noise level

Based on the methods used to obtain the plots in Figure 5, we also plotted the results for different noise levels, specifically for -88.5 dBm, -89.5 dBm, and -90 dBm. These plots are shown in Figure 6.
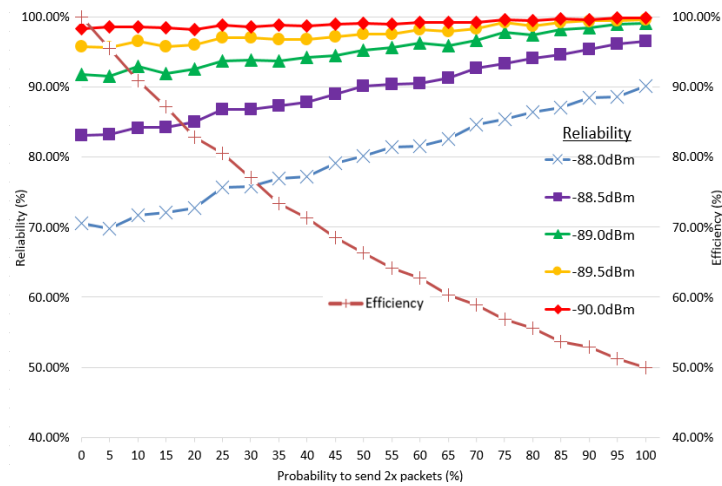
Figure 6 Relationship of reliability and efficiency for various probabilities of sending 2× packets at various noise levels

As shown in Figure 6, the "+" line refers to the efficiency of the probabilistic redundancy-based protocol. The efficiency is the same for all of the noise levels; thus, only one line is shown on the graph. The diamond line is the reliability achieved by the protocol at the -90 dBm noise level. It had an optimum value of 2% probability to send redundant packets, and it was able to achieve 99% reliability and efficiency. The -90 dBm noise level represents a nearly ideal environment, which contains very little noise. Therefore, less redundant packets are needed to achieve the desired reliability. This, in turn, results in significantly better efficiency. For other cases with higher noise levels, the probability of sending redundant packets will be increased in order to obtain the optimum levels of reliability and efficiency.

4.3. Performance Analysis of the Optimized Model
Using the optimum values obtained in Figure 6, we plotted the line labelled *Redundant-Probabilistic-Optimized* in Figure 7.
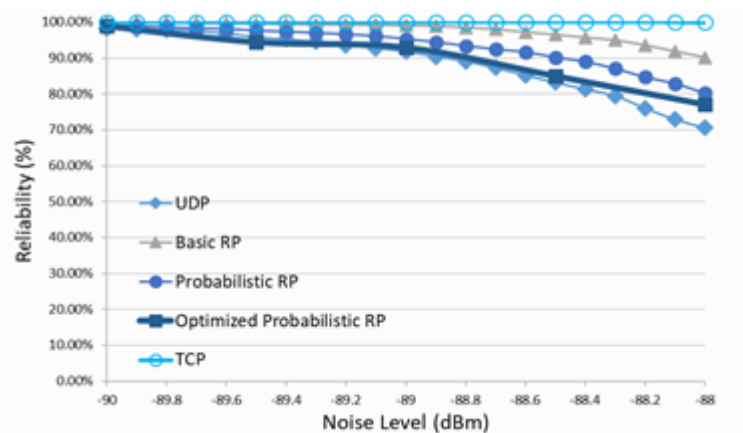

Figure 7 Graph of reliability vs. noise level

This line shows the attainable reliability at any given noise level when the probability of a duplicating packet was optimized. We also plotted earlier lines in Figure 7 for comparison.

As shown in Figure 7, we measured the reliability of the various protocols for the noise levels between -90 dBm (least noisy) and -88 dBm (most noisy). In the least noisy environment, all five protocols had identical performances and achieved reliability rates of more than 98%. Whereas, for the noisiest environment, the reliability rate of *Redundant-Probabilistic-Optimized*

was 77%. It outperformed *UDP* by 7% but was 3% lower than the reliability rate of *Redundant-Probabilistic*, 13% lower than *Redundant-Basic,* and 23% lower than *TCP*.

Despite not performing as well as the other, more basic, protocols in term of reliability, *Redundant-Probabilistic-Optimized* did have better efficiency. Although *Redundant-Probabilistic-Optimized* also sends duplicate packets like *Redundant-Probabilistic* and *TCP*, it does so by adaptively optimizing the probability of sending duplicate packets based on its surrounding noise level. Therefore, the trade-off in efficiency would also be different when compared to *Redundant-Probabilistic, Redundant-Basic,* and *TCP*.
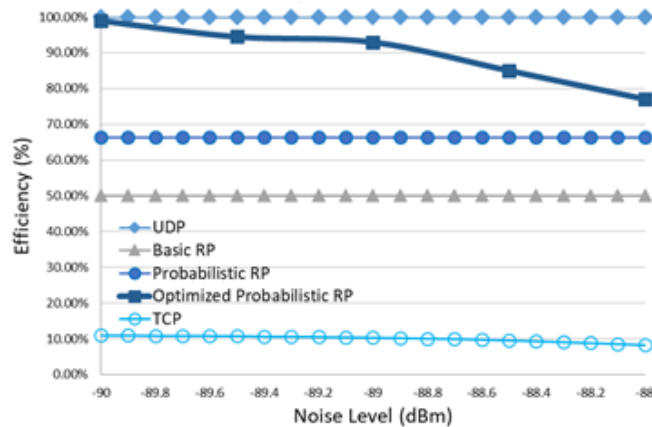

Figure 8 Graph of efficiency vs. noise level

As shown in Figure 8, when it was most noisy, the efficiency of *Redundant-Probabilistic-Optimized* (77%) was better than *Redundant-Probabilistic*, *Redundant-Basic,* and *TCP* by 9%, 27%, and 68%, respectively. As discussed earlier, the drops in reliability of 3%, 13%, and 23% shown Figure 8 were traded for improvements in efficiency. In environments where the noise level was at its lowest, the *Redundant-Probabilistic-Optimized* protocol had an efficiency rate of 99% compared to those of *TCP* (10%), *Redundant-Probabilistic* (68%), and *Redundant-Basic* (50%).
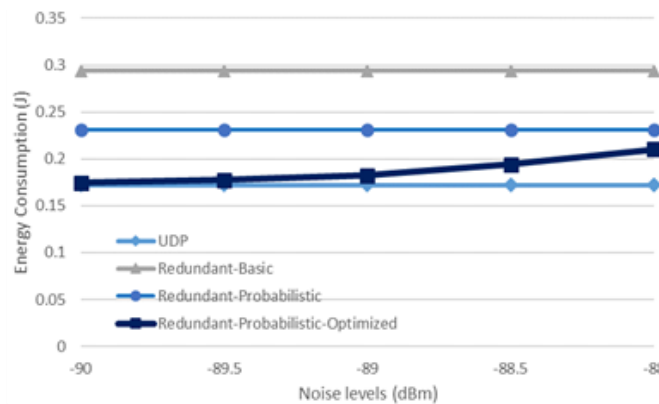

Figure 9 Graph of energy consumption vs. noise level (without TCP)

Next, the energy consumption obtained by each of these protocols under various noise levels were compared. Energy consumption is dependent on the usage of redundant packets; as more redundant packets are sent, energy consumption increases. As shown in Figure 9, *UDP,* which does not utilize redundancy techniques, consumed the least energy, while *Redundant-Basic,* which sends the most redundant packets, consumed the most energy. Based on Figure 9, *UDP*, *Redundant-Basic*, and *Redundant-Probabilistic* had constant energy consumption levels across various noise levels, as the number of packets sent was fixed. Ideally, in a low noise

environment, lower energy is needed, as the number of redundant packets sent to achieve the desired reliability is less. Figure 9 shows that our optimized protocol (*Redundant-Probabilistic-Optimized*) is the only protocol that provides non-fixed energy consumption. It is able to consume less energy in a lower noise environment. Hence, this proves that the proposed protocol provides better adaptability when compared to other protocols.
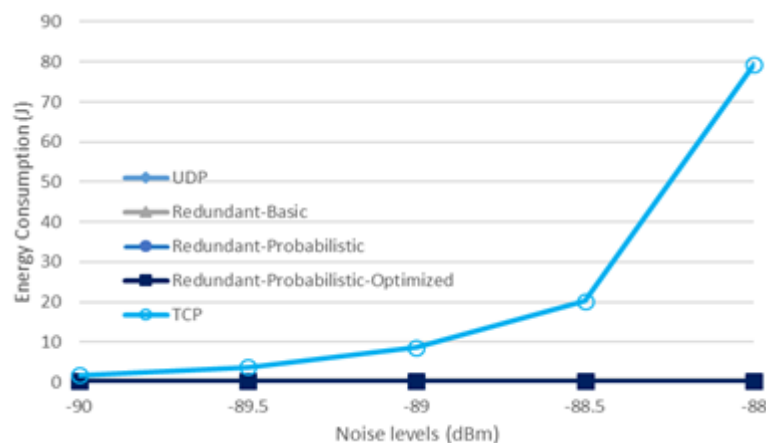

Figure 10 Graph of energy consumption vs. noise level

In Figure 10, the energy consumption of *TCP* across various noise levels is depicted. The results obtained by *TCP* were significantly higher than those of the rest of the protocols. This is due to the working principle of *TCP,* which is that it must successfully complete one transmission cycle before starting a new cycle. The same packet will be retransmitted until that specific packet is successfully received by the receiver. The high energy consumption of *TCP* shown in Figure 10 indicates that more redundant packets were sent in order to maintain its perfect reliability.

5.   CONCLUSION

We have proposed a probabilistic redundancy-based protocol (*Redundant-Probabilistic-Optimized*) that is adaptive to one of the dynamic behaviors of WSN: varying noise levels. The proposed protocol would be able to choose the proper probability of sending duplicate copies of each packet according to the surrounding noise level. The usage of redundant packets would eventually improve the reliability, but it also reduces the overall efficiency of the protocol. In our proposed *Redundant-Probabilistic-Optimized* protocol, we can achieve the optimum result for both reliability and efficiency as compared to other protocols. In addition, our proposed *Redundant-Probabilistic-Optimized* protocol has been proven to be adaptable to the variation of noise levels in terms of energy consumption. In the future, we plan to study other dynamic behaviors of WSN and include more parameters in the creation of the probabilistic redundancy-based protocol, such as the surrounding temperature. Additionally, we will also evaluate the protocol in a larger network and consider sending more than two copies of a packet for increased reliability.

6.   ACKNOWLEDGEMENT

7. REFERENCES

Al-Awami, L., Hassanein, H., 2012. Energy Efficient Data Survivability for WSNs via Decentralized Erasure Codes. *In:* Proceedings of 37th Annual IEEE Conference on Local Computer Networks, pp. 577–584

Ali, S., Al-Balushi, T., Nadir, Z., Hussain, O.K., 2018. Improving the Resilience of Wireless Sensor Networks Against Security Threats: A Survey and Open Research Issues. *International Journal of Technology*, Volume 9(4), pp. 828–839

Berawi, M.A., Suwartha, N., Kusrini, E., Kartohardjono, S., Suryanegara, M., Putra, N., Zagloel, T.Y., 2016. Accelerating Technology Development: Engaging Stakeholders and International Networking. *International Journal of Technology*, Volume 7(7), pp. 1128–1131

Bhisham, S., Trilok, C.A., 2012. A Comparative Analysis of Reliable and Congestion-aware Transport Layer Protocols for Wireless Sensor Networks. *ISRN Sensor Networks*, Volume 2012, pp. 52–57

Budhaditya, D., Sudeept, B., Badri, N., 2003. ReInForM: Reliable Information Forwarding using Multiple Paths in Sensor Networks. *In:* Proceedings of 28th Annual IEEE International Conference on Local Computer Networks, pp. 406–415

Celimuge, W., Satoshi, O., Toshihiko, K., 2012. An Adaptive Redundancy-based Mechanism for Fast and Reliable Data Collection in WSNs. *In:* Proceedings of 8th IEEE International Conference on Distributed Computing in Sensor Systems, pp. 347–352

Chonggang, W., Kazem, S., Bo, L., Mahmoud, D., Yueming, H., 2006. A Survey of Transport Protocols for Wireless Sensor Networks. *IEEE Network*, Volume 20(3), pp. 34–40

Kazem, S., Daniel, M., Taieb, Z., 2007. *Wireless Sensor Networks Technology, Protocols and Applications*. USA:John Wiley & Sons, Hoboken, NJ

Marchi, B., Grilo, A., Munes, M., 2007. DTSN: Distributed Transport for Sensor Networks. *In:* Proceedings of 12th IEEE Symposium on Computers and Communications, pp. 165–172

Meng, Y.S., Lee, Y.H., 2010. Investigations of Foliage Effect on Modern Wireless Communication Systems: A Review. *Progress in Electromagnetics Research*, Volume 105, pp. 313–332

Muhammad, A.M., Winston, K.G.S., Ian, W., 2015. Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead. *Computer Networks*, Volume 79, pp. 166–187

Raghavendra, C.S., Krishna, M.S., Taieb, Z., 2004. *Wireless Sensor Network. Springer, United States of America.* Switzerland: Springer

Srouji, M.S., Zhonglei, W., Jorg, H., 2011. RDTS: A Reliable Erasure Coding Based Data Transfer Scheme for Wireless Sensor Networks. *In:* Proceedings of 17th International Conference on Parallel and Distributed Systems, pp. 481–488

Sumaryo, S., Halim, A., Ramli, K., Joelianto, E., 2019. A Model for Accelerating Discharge of Lane Traffic to Facilitate Intersection Access by EVs. *International Journal of Technology*, Volume 10(1), pp. 116–125

Sunil, K., Zhenhua, F., Yang, X., 2009. E2SRT: Enhanced Event-to-Sink Reliable Transport for Wireless Sensor Networks. *Wireless Communications and Mobile Computing*, Volume 9(10), pp. 1301–1311

Varga, A., 2010. *Modeling and Tools for Network Simulation.* Berlin, Heidelberg: Springer

Winston, K.G.S., Hwee, X.T., 2006. Multipath Virtual Sink Architecture for Wireless Sensor Networks in Harsh Environments. *In:* Proceedings of the 1st International Conference on Integrated Internet Ad-hoc and Sensor Networks, p. 19

Yogesh, S., Ozgur, B.A., Ian, F.A., 2003. ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks. *In:* Proceedings of the 4th ACM International Symposium on Mobile Ad-hoc Networking & Computing, pp. 177–188