TERP: A Trusted and Energy Efficient Routing Protocol for Wireless Sensor Networks (WSNs)

Marwah Almasri, Khaled Elleithy; IEEE Senior Memebr, Anas Bushang, and Remah Alshinina
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Recently, Wireless Sensor Networks (WSNs) have got researchers attention due to its various useful and helpful applications in the real world with low cost sensors. The task of the sensors is to collect data from the environment and send it to the central node (sink node). However, the power is limited in these sensors and therefore it has a limited lifetime which is a big deal in WSNs. Another important issue in WSNs is the level of security. Since these sensor nodes exchange and transmit data among the network, the security of the data can be at risk. Hence, In this poster, we propose a novel trusted and energy efficient routing protocol (TERP), which is based on the Destination Sequenced Distance Vector Protocol (DSDV). TERP can avoid any malicious nodes (untrusted nodes) and thus increase the security level in the network, and decrease the power consumption level.

Introduction

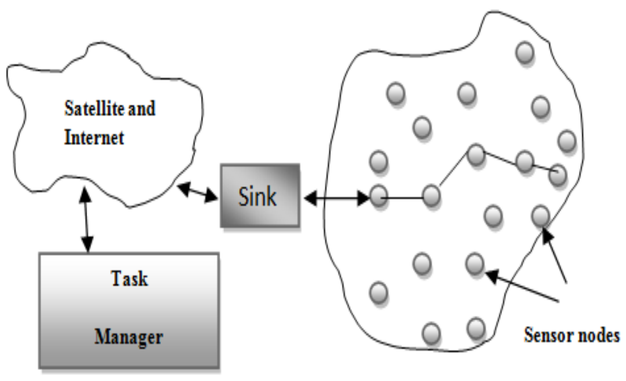

Fig. 1. Architecture of WSNs

Wireless Sensor Network (WSN) composed of a huge number of scattered sensor nodes that can communicate with each other as shown in Figure 1. These sensors collect data from the environment and then route it to the sink node where it communicates through satellite or Internet with the task manager. However, it is essential to deliver and route these data over the network in an efficient and secure manner. There are several routing protocols that are used in WSNs such as Destination Sequenced Distance Vector (DSDV).

Trust

Many wireless routing protocols such as Destination Sequenced Distance Vector (DSDV) can not detect malicious nodes that misbehave in the network. Therefore, trust is needed to avoid these malicious nodes during the operation of routing between nodes and thus guarantees data packets are delivered as expected .

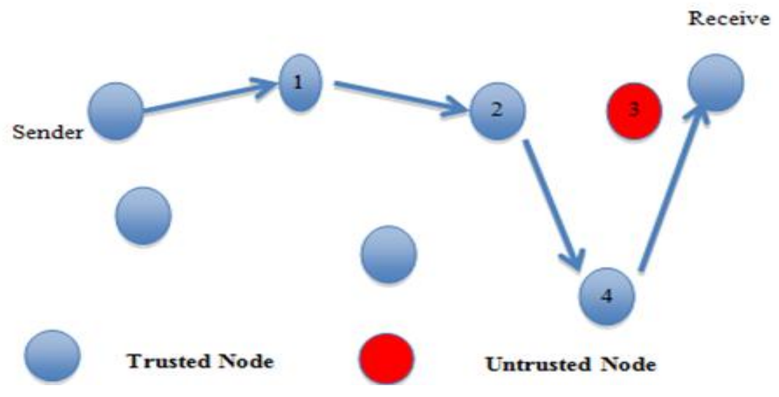

Fig. 2. A scenario of trusted and untrusted nodes in the network

Proposed work

The Proposed work provides information of how the analysis was achieved and how the results were calculated by comparing the performance of the existing DSDV and the proposed trusted and energy efficient routing protocol (TERP). The proposed work is evaluated based on power consumption, drop ratio, delivery ratio, average delay, and delay jitter. The simulation scenarios are conducted by using NS-2 simulator.

How to calculate the trust factor?

TABLE I. The relationship between data value and trust factor.

	High	Medium	Low
9 & 10	Medium Encryption	No Encryption	NO Encryption
6,7 & 8	High Encryption	Medium Encryption	No Encryption
2,3,4 & 5	High Encryption	High Encryption	No Encryption
0 & 1	-	-	-

The First Simulation Scenario

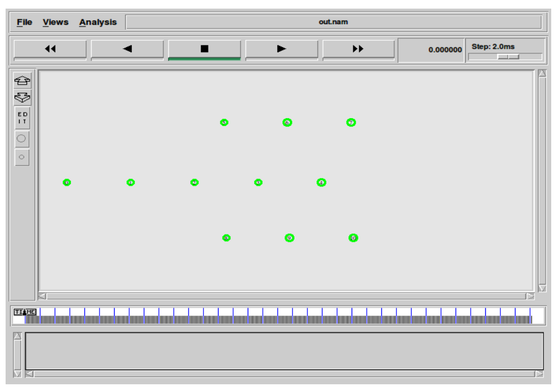

Fig. 3. The first simulation scenario

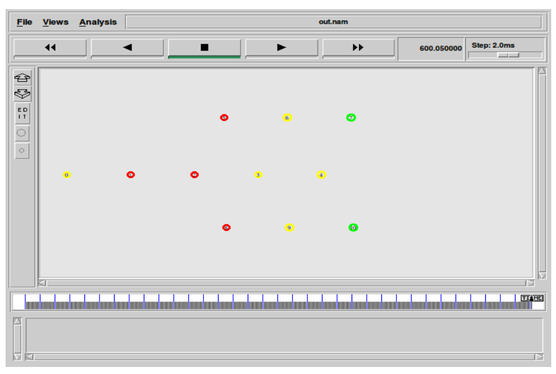

Fig. 4. Energy level for different nodes

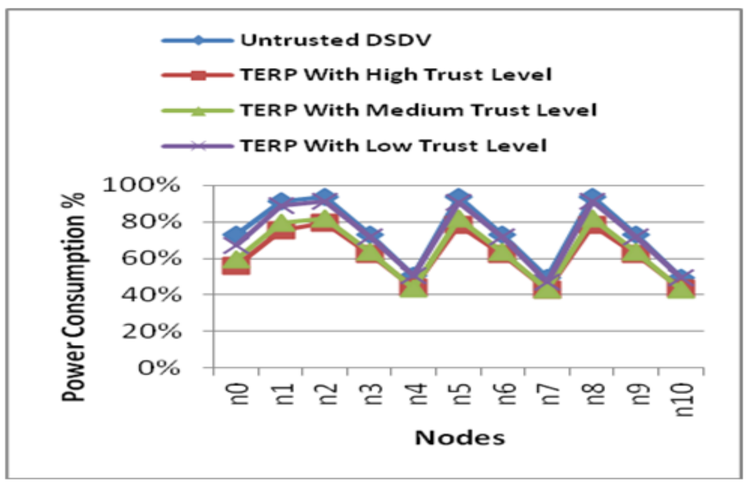

Fig. 5. Comparison of the consumption of different levels of trust along with the untrusted DSDV

The Second Simulation Scenario

A. Drop Ratio

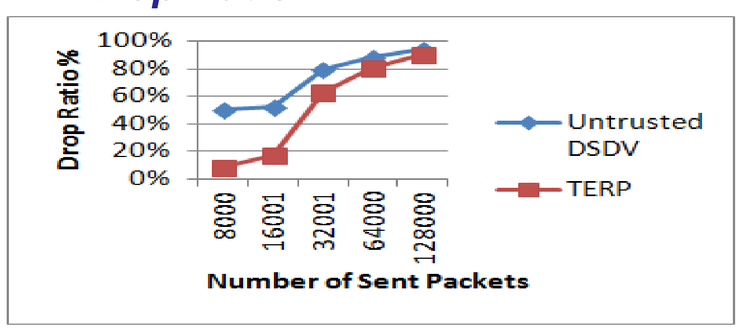

Fig. 6 Comparison of the drop ratio for both untrusted DSDV and TERP routing protocols

B. Delivery Ratio

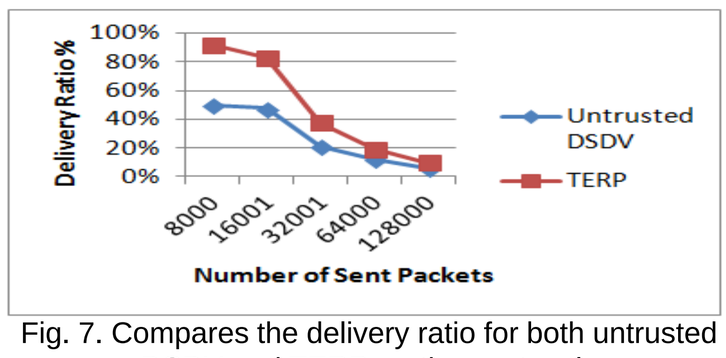

Fig. 7. Compares the delivery ratio for both untrusted DSDV and TERP routing protocols

C. Average End-to-End Delay

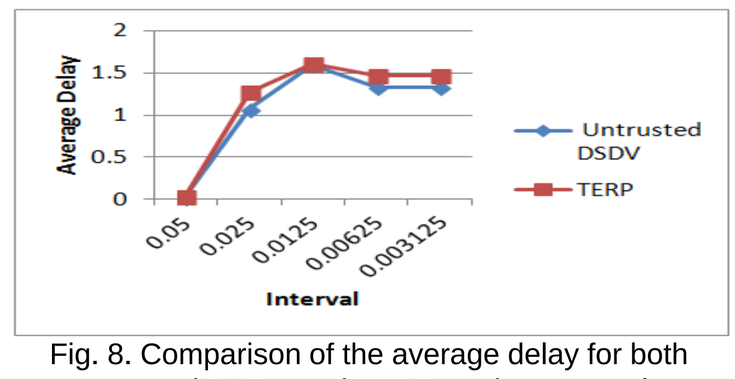

Fig. 8. Comparison of the average delay for both untrusted DSDV and TERP routing protocols

D. Delay Jitter

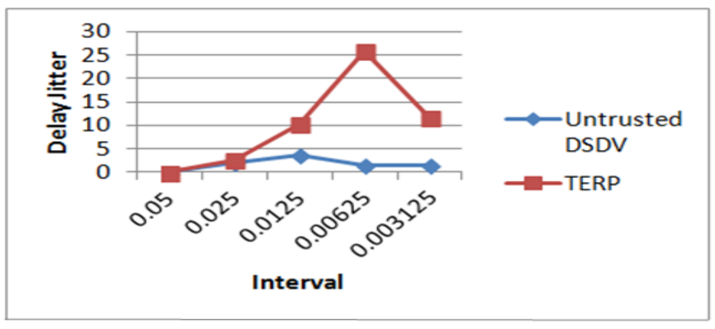

Fig. 9. The jitter delay for both untrusted DSDV and TERP routing protocols

Conclusion

In wireless sensor networks (WSNs), saving the energy is a challenging task. Since these sensors have limited power, we need to recharge or replace the sensors which is a costly and an inefficient process. This poster proposes a trusted and an energy efficient protocol called TERP that helps to maximize the network life. Based on the simulation results, TERP decreases the power consumption compared to the DSDV protocol using the trust concept which leads to less encryption applied. Three levels of trust are presented and compared to DSDV in terms of power consumption. Other factors such as drop ratio, delivery ratio, average delay, and delay jitter are also analyzed. TERP has less drop ratio and more delivery ratio than DSDV which enhances the overall performance of the network.