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 06604
maalmasr@bridgeport.edu , elleithy@bridgeport.edu , abushnag@bridgeport.edu , ralshini@bridgeport.edu

***Abstract*—Recently, Wireless Sensor Networks (WSNs) have emerged to provide a variety of important applications with low cost sensors. The task of the sensors is to collect data and send it to the sink node which delivers the data to a task manager. However, these sensors have limited power and thus limited lifetime. Another important consideration in WSNs is the level of security. Transmitting data from node to another can risk the security of the data.**

In this paper, we propose a novel trusted and energy efficient routing protocol (TERP) based on the Destination Sequenced Distance Vector Protocol (DSDV). TERP helps to increase the security level in the network and thus avoid any malicious nodes or untrusted nodes. It also reduces the power consumption by using the trust factor. The higher the degree of trust, the less encryption is used which results in less energy. Other factors such as drop ratio, delivery ratio, average delay, and delay jitter are analyzed along a comparison of DSDV protocol with the proposed TERP routing protocol.

Keywords- Wireless Sensor Network (WSN); Destination Sequenced Distance Vector (DSDV); Trust; Trusted and Energy Efficient Routing Protocol (TERP).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have gained increased attention in the recent years due to its various useful applications such as healthcare field, traffic control, and military fields [1]. WSNs contain a large number of wireless sensor nodes that are designed to sense and collect important data in order to process them and then send them to the sink node [2]. A typical sensor network consists of many scattered sensor nodes that can communicate with each other. These scattered nodes collect data and route it to the sink node where the later communicates through satellite or Internet with the task manager. Sensors are designed limited supply of power which affects the transmission [3]. Fig. 1 illustrates the architecture of WSNs. In WSNs it is very difficult to recharge the battery used which has a limited energy. As a result, considering the energy consumption is a critical factor in WSNs [4]. To take the most advantage of wireless sensor network, the data transmitted over the network should be delivered and routed in a safe manner to ensure the validity and the efficiency of the network. Security is a crucial factor in WSN where the existence of secure routing protocols affects the WSN's security. There are several routing protocols that are deployed in Mobile Ad-Hoc Network and WSNs that are used for routing the packets between wireless devices. Wireless Routing protocols (WRP) are classified into three categories; proactive protocols such as DSDV, on Demand routing protocol (reactive), and Hybrid routing (combination of proactive and on demand) [6]. On Demand routing also known as Reactive routing is one of the important protocol types that helps in reducing the wireless traffic by generating path request on demand [7]. Proactive Routing is a table driven protocol where every node maintains a table to register the next hop entry and the number of hops needed to reach the destination [8]. Hybrid protocols use the characteristics of both proactive and reactive protocols to make routing smoother and scalable. Hybrid protocols try to overcome the deficiencies of the other two classes of routing protocols [9].

However, when applying such protocols many attacks could occur by malicious nodes which cause to disturb the efficient functionality of the network. As a result, in order to ensure that the network provides its services without any problem, a trust based protocol helps to resolve this issue. Based on the trust level, each node communicates with its neighbors [5]. Trust can help to sustain the stability of the network and enhance the communication process between nodes. In addition, trust can be implemented to reduce the size of the data sent from node to node and thus decrease the needed power consumption. As the trust level at each node increases, less encryption or cryptography is used.

In this paper, we propose a trusted and energy efficient routing protocol (TERP). Applying the trust concept to DSDV protocol helps to increase the security level of the network as it will avoid any misbehaving actions and denying malicious nodes. Trust also can be used to increase the life of the network as it reduces the power consumption by using less encryption with the trusted nodes.

The rest of this paper is structured as follows: section II presents the related work. Section III, introduces the trust concept with in-depth discussion. Section IV, proposes a new trusted and energy efficient routing protocol (TERP) to be deployed in WSN. Section V, discusses and analyzes the results. Finally, section VI, offers conclusions based on simulation results.

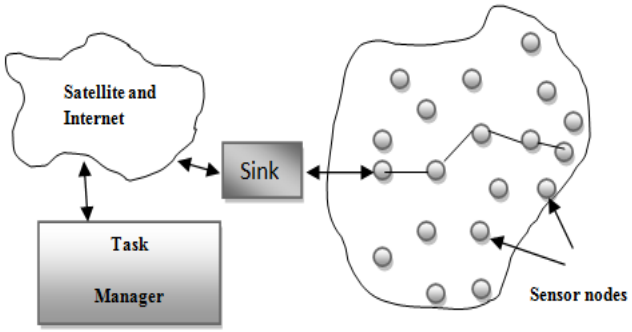

Figure 1. Architecture of WSNs

II. RELATED WORK

When dealing with WSNs, security and energy consumption are great aspects since both have direct impact on the authenticity, integrity, and functionality of the network. As a result, many researchers have paid attention to the need for improving the security level of the network to avoid the existence of misbehaving nodes. Authors in [13] have proposed a secure and energy efficient multipath routing protocol called SEER. SEER protocol uses the base station that discovers several paths to the source of the data where it finally selects one of them for communication purposes. This protocol updates each node with the remaining energy on a dynamic basis in order to select the appropriate path from the multipath chosen. The advantage of such protocol is to reduce the extra overhead needed for maintaining the route, and extend the sensor network's lifetime due to the efficiency of the level of energy consumption [13].

The security of information exchanged between two nodes is a strong factor especially in military fields. SAODV is a secure routing protocol that assures the information security as well as the energy efficiency. This protocol is based on the classic AODV protocol but several mechanisms are added to deal with security issues such as AES encryption standard, digital signature mechanism, and RSA public-key encryption [14]. In addition, many papers have discussed the importance of SAODV protocol and provided some enhancements. In [15], author has enhanced the existing SAODV protocol to deal with serious attacks from malicious nodes that are already have been authenticated by the network. This protocol is called SAODV-SDDO. In order to detect these malicious nodes, a cryptographic mechanism and a reactive approach have been used. he basically added Intrusion Detection Mechanism (IDM) and Trust Based Mechanism (TBM) to the SAODV protocol [15].

Moreover, the authors in [16] have discussed various issues regarding trust management in WSNs. They came up with a novel trust aware routing protocol that uses both direct and indirect trust. It has monitoring component with several trust metrics such as network-ACK, data confidentiality, reputation validation, data integrity, and remaining energy. The proposed routing protocol uses three control messages which are BEACON, REPREQ and REPRES. Each node calculates the trust value by using the trust metric and then a weighted trust value is computed as a direct trust value which indicates the level of trust in the network and thus avoids and detects many attacks [16]. In [17], a new trust scheme has been proposed which is based on cross-layer concept. This scheme is called Trust-Based Cross-Layer Model (TCLM). It uses the ACKs from data link layer and TCP layer in order to promote a trust model that avoids the malicious nods and ensures the trusted route from source to the sink [17].

Furthermore, authors in [18] have proposed a trust based secure data aggregation approach which is called Social Estrangement Trust Management model (SETM). They paired Order-Preserved Encryption Scheme (OPES) with Sigmoid trust Model. The advantages are as follow: using a secured and trusted data aggregation model, dealing with attacks, and providing a keyless behavioral observation. SETM is important in WSN since it allows nodes to adjust themselves and pay attention to their neighboring nodes and their trustworthiness level [18].

III. TRUST

The existing wireless routing protocols such as Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) and Zone Routing protocol (ZRP) are vulnerable to be broken and compromised since they do not have a mechanism to detect malicious nodes that misbehave [10]. Especially, if the attack is internally and comes from a node or more that are inside the network.

Misbehaving is not only caused by malicious nodes but also it can be done if the buffer of a node is fully occupied by packets and started to drop all new incoming packets [10]. Moreover, for instance if the node is running out of power, it could drop some packets or the node itself is broken.

By applying trust, malicious or misbehaving nodes can be avoided during the operation of routing between the sender and receiver which results in guaranteeing that routing data or data packets are delivered as expected. On the other hand, trust could also decrease the size of data or packets between the nodes. For example, if the trust factor is high, low cryptography can take place and this leads to reducing the amount of bandwidth.

Wireless sensor networks have a limitation on bandwidth, security and energy [11]. Therefore, applying the concept of trust improves these aspects which lead to a better overall performance of the network.

A. What is trust?

Trust in real life is simply when someone (node) acts as expected. Trust is a replacement of knowledge and also it is built on previous experience. In addition, trust might be used to shift risk from someone (node) to another. There are two types of trust; direct and indirect [11].

The direct relationship is when trust taking place between two nodes. However, the indirect relationship when node 1 trusts node 2, and node 2 trusts node 3. Therefore, node 1 should trust node 3 but this is not always working because the limitation of the scope is an issue in the existing reputation systems.

In the indirect relationship, since there is no trust between two nodes and at the same time, a third party trusts both of them. This third party which is a node could act as guarantor between the two nodes that have untrusted relationship between them which means moving the risk from node to another. But of course, the guarantor node gains some benefit in return. For example, the node that asked for the guarantor should act as a guarantor node itself for some time in future as a form of payback.

B. *How to calculate the trust factor?*

There are several ways to calculate the trust factor and this is based on the need of trust. Many aspects and matrices are involved. One of the most important aspects that play a serious role is the data value. In other words, how important is the data that is going to be sent from the sender to the receiver. For example node 1 wants to send location packets to node 2 and it has a trust factor of 10 for node 2.The scale used is from 0 to 10. Trust factor 10 means that node 2 is completely trusted by node 1 and the value of data is low. So node 1 can use no encryption as shown in Table I. However, if node 1 has a trust factor of 5 for node 2 and the value of data is medium, node 1 is going to use high encryption as shown in Table I.

Energy is another aspect that should be taken in account when trust factor is calculated because it indicates how many bits the node can send or forward before it is down. Also, previous experience between nodes is influential in trust factor calculation since it shows the general direction of trusting and if the trust factor is increasing or decreasing.

IV. 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.

Delay is the time duration that packet need to be received at the destination. Delay can be divided into three types. The first one is called queuing delay which is the time duration that any packet has to wait inside a node to be transmitted. Second, propagation delay is the time duration that the first bit of a packet needs to be transmitted at receiver. Finally, transmission delay is the time taken for the whole packet to be transmitted at the receiver. The sum of the three delays is called total delay or latency [12].

Packet loss takes place when a packet cannot reach its destination for any reason such as network connection problems, lack of bandwidth, link failure or human interference. It can be a combination of these reasons [12]. Fig. 2, demonstrates a scenario where there are trusted and untrusted nodes in the network. In this scenario, packets are delivered using the shortest route to the destination if the nodes in this route are trusted. Otherwise, the second best trusted route is used. In Fig. 2, node 3 is avoided because it is not trusted by the network regardless it has a shorter route to the receiver compared to node 4.

A. *The First Simulation Scenario*

This simulation judges the power consumption of sensor nodes such as sender, receiver and middle nodes in a wireless network that consists of 11 nodes using CSMA/CA protocol on its MAC layer. Packets are transmitted from N0 to N4 for 400 seconds and each node has an initial energy of 120 mw as shown in Fig. 3. Based on what route the packets will follow, the nodes of this route are going to use energy when they send, receive, or forward packets as represented in Fig. 4. At the end of the simulation, there will be an indicator (remaining energy) that presents information of which nodes will have more traffic compared to others as shown in Table II. Table II, shows the power consumption level of each node using the untrusted DSDV routing protocol. This implementation was conducted using the DSDV and the proposed protocol TERP which has three levels of trust: high, medium and low.

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	-	-	-

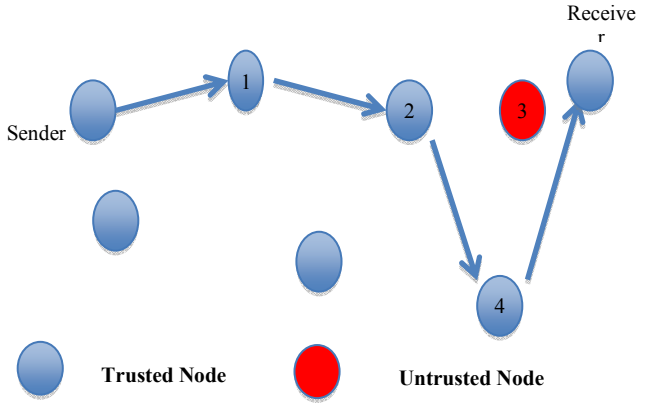

Figure 2. A scenario of trusted and untrusted nodes in the network

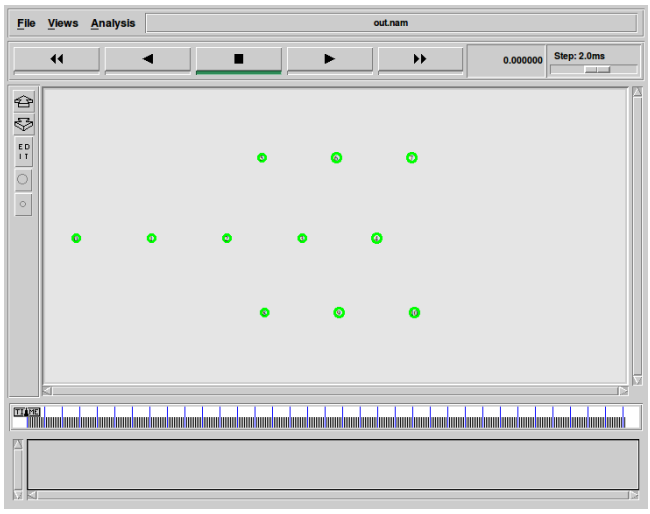

Figure 3. The first simulation scenario

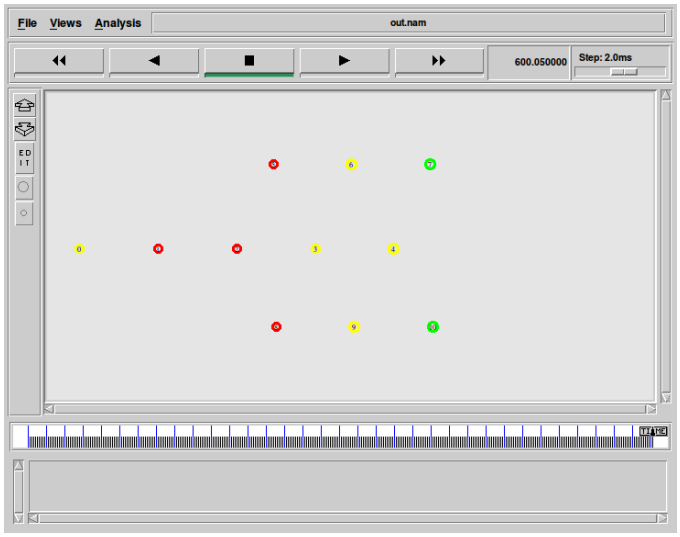

Figure 4. Energy level for different nodes

Using different levels of trust help to compare the power consumption of each node for TERP routing protocol versus untrusted DSDV routing protocol. Table III shows the power consumption when TERP routing protocol is used with low trust level. As shown in Fig. 5, the power consumption of untrusted DSDV protocol is a little bit higher than the power consumption of TERP routing protocol with low trust level.

TABLE II. The energy remaining and power consumption level of each node using the untrusted DSDV

Nodes	Energy Remaining	Power Consumption%
n0	32.3371	73.05%
n1	10.6083	91.16%
n2	7.5801	93.68%
n3	32.3371	73.05%
n4	59.541	50.38%
n5	7.8786	93.43%
n6	32.3371	73.05%
n7	61.0557	49.12%
n8	7.8042	93.50%
n9	32.3371	73.05%
n10	60.4639	49.61%

TABLE III. The energy remaining and power consumption level of each node using TERP with low trust level

Nodes	Energy Remaining	Power Consumption %
n0	39.6778	66.94%
n1	13.5479	88.71%
n2	10.5215	91.23%
n3	33.6805	71.93%
n4	59.2806	50.60%
n5	10.9727	90.86%
n6	33.6805	71.93%
n7	63.4389	47.13%
n8	10.5924	91.17%
n9	33.6805	71.93%
n10	61.0394	49.13%

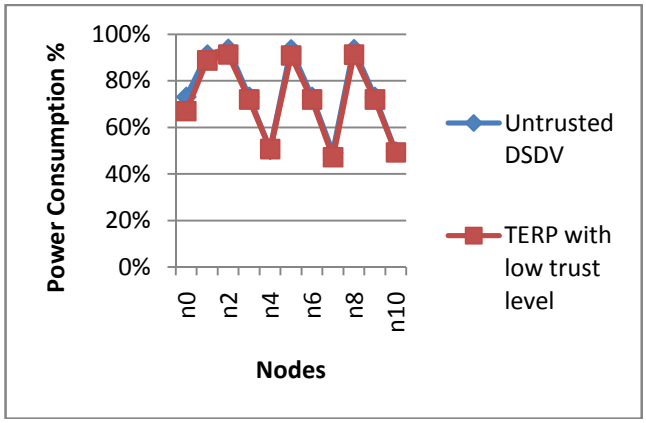

Figure 5. Comparison of the power consumption level between the untrusted DSDV and TERP routing protocols with low trust level

Table IV, shows the energy remaining at each node using TERP routing protocol with a medium trust level and also shows the power consumption percentage used at each node. The power consumption in this case is better than using TERP with low trust which is much better than using the untrusted DSDV. Similarly, increasing the level of trust saves power and reduces the consumption level at each node as shown in Fig. 6. TERP with high trust level can reduce the power consumption and save energy for a longer network life. As shown in Fig. 7.

TABLE IV. Energy remaining and power consumption level of each node using TERP with medium trust level

Nodes	Energy Remaining	Power Consumption%
n0	48.8860	59.26%
n1	24.7283	79.39%
n2	22.0858	81.60%
n3	43.6494	63.63%
n4	67.6472	43.63%
n5	22.1591	81.53%
n6	43.6494	63.63%
n7	68.4782	42.93%
n8	22.1493	81.54%
n9	43.6494	63.63%
n10	68.3341	43.05%

TERP shows a better performance in terms of saving energy as it reduces the power consumption percentage compared to the untrusted DSDV. Table V, summarizes the energy remaining at every node along with the percentage of power consumed.

As shown in Fig. 8, TERP with high trust level consumes less power compared to untrusted DSDV and low trusted TERP. Therefore, using TERP with high or medium level of trust can defiantly save a lot of energy and enhance the life of the whole network.

TABLE V. summarizes the energy remaining and power consumption level of each node using TERP with a high trust level

Nodes	Energy Remaining	Power Consumption%
n0	53.1161	55.74%
n1	29.3538	75.54%
n2	24.9656	79.20%
n3	44.9139	62.57%
n4	67.3131	43.91%
n5	26.0615	78.28%
n6	44.9139	62.57%
n7	68.592	42.84%
n8	25.7538	78.54%
n9	44.9139	62.57%
n10	68.1101	43.24%

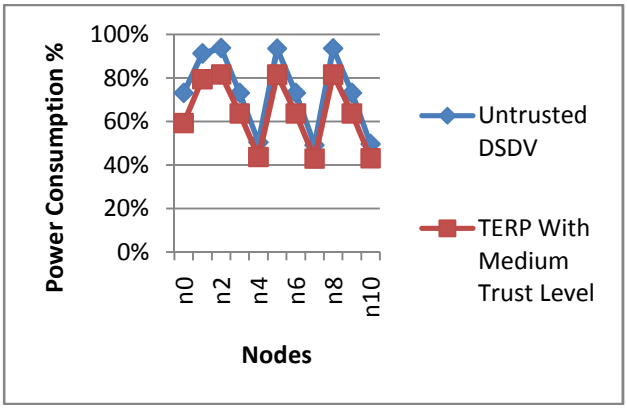

Figure 6. Comparison between the power consumption level between the untrusted DSDV and TERP routing protocols with a medium trust level

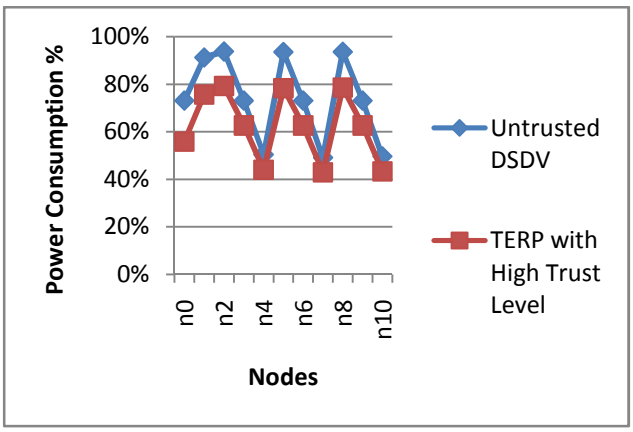

Figure 7. Comparison of power consumption level between untrusted DSDV and TERP routing protocols with a high trust level

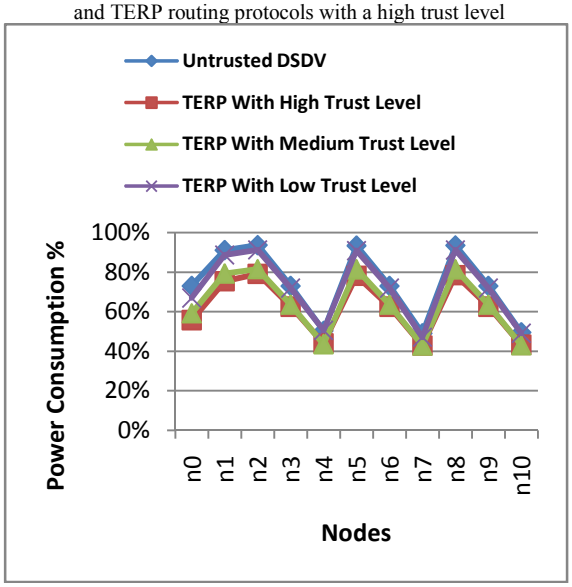

Figure 8. Comparison of the consumption of different levels of trust along with the untrusted DSDV

B. The Second Simulation Scenario

This simulation scenario is used to examine the performance of the number of dropped packets, dropped ratio, delivery ratio, average end-to-end delay, and delay jitter. There are 11 nodes that are created in this scenario. The nodes act as sensor nodes in a wireless network that are using CSMA/CA protocol. The sender node, which is n0, is going to transmit packets to the receiver node n4 at time 100 seconds and it will stop transmitting at time 500 seconds as shown in Fig. 9. Also, node n3 at time 300 seconds starts misbehaving by dropping packets. The number of packets sent per second is increased to calculate the performance metrics in different environment situations. This implementation was applied using the existing DSDV and the proposed protocol TERP. Results of both protocols were collected and compared to each other to know which one is performing better.

1) Drop Ratio:

The drop ratio indicates how often packets are dropped in the network during the simulation time. Table VI shows the number of sent packets which are 8000, 16001, 32001, 64000, and 128000 packets and it also summarizes the number of received packets and dropped packets, and the drop ratio of untrusted DSDV in each case. The drop ratio is calculated using (1).

$$Drop\ Ratio = \frac{\text{Number of Dropped Packets}}{\text{Number of Sent Packets}} \text{ X } 100 \qquad (1).$$

As shown in Table VI when sending 8000 packets, half of the packets are received and the other half is dropped which leads to a 50% drop ratio. As the number of sent packets increases, the drop ratio of using untrusted DSDV increases as well. On

the other hand, when sending the same number of packets using TERP protocol, 7321 packets are received whereas 679 packets are dropped leading to 8.49% drop ratio as represented in Table VII. Again as the number of sent packets increases, the drop ratio increases as well. However, comparing TERP with DSDV, TERP has much better drop ratios as it happens to drop less number of packets as shown in Fig. 10.

2) Delivery Ratio

Delivery ratio indicates how many packets are received compared with the number of sent packets during the simulation. Using untrusted DSDV and TERP protocols lead have different delivery ratios. The delivery ratio is calculated using (2).

$$Delivery\ Ratio = \frac{\text{Number of Received Packets}}{\text{Number of Sent Packets}} \text{ X } 100 \qquad (2).$$

Table VIII provides the delivery ratios for both DSDV and TERP routing protocols. Sending 8000 packets has a delivery ratio of 50%, where it is 91.51% using TERP protocol. As the number of sent packets increases, the delivery ratio decreases. However, with TERP, the delivery ratio is much better compared with DSDV protocol. For example, sending 16001 has resulted in 47.65% and 82.71% for DSDV and TERP respectively. Therefore, using the proposed TERP helps to maximize the number of received packets and thus increases the delivery ratio as shown in Fig. 11. Fig. 11, compares the delivery ratio of untrusted DSDV and TERP protocols where it highlights the difference in the performance of both protocols. TERP has a higher delivery ratio than DSDV and reaches about the same level when sending a large number of packets such as 128000 packets.

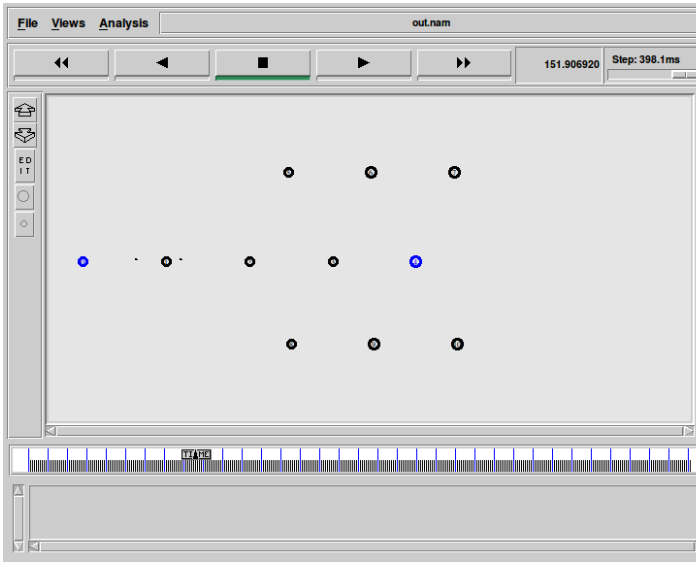

Figure 9. The second simulation scenario

TABLE VI: The drop ratio of untrusted DSDV routing protocol

Number of Sent Packets	Number of Received Packets	Number of Dropped Packets	DSDV Drop Ratio%
8000	4000	4000	50%
16001	7624	8377	52.35%
32001	6665	25363	79.26%
64000	7656	56345	88.03%
128000	7656	120344	94.02%

TABLE VII: The drop ratio of TERP routing protocol

Number of Sent Packets	Number of Received Packets	Number of Dropped Packets	TERP Drop Ratio%
8000	7321	679	8.49%
16001	13235	2766	17.29%
32001	11941	20060	62.69%
64000	12245	51755	80.87%
128000	12380	115620	90.33%

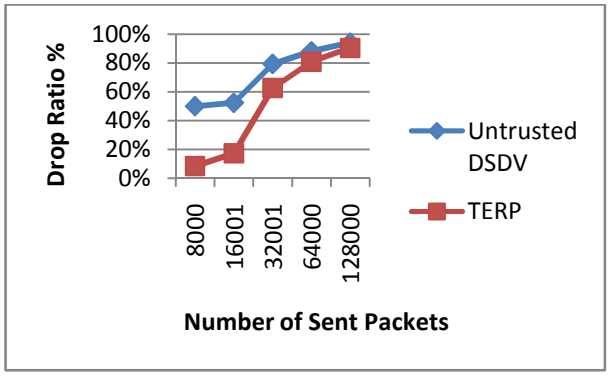

Figure 10. Comparison of the drop ratio for both untrusted DSDV and TERP routing protocols

Table VIII provides the delivery ratios for both DSDV and TERP routing protocols. Sending 8000 packets has a delivery ratio of 50%, where it is 91.51% using TERP protocol. As the number of sent packets increases, the delivery ratio decreases. However, with TERP, the delivery ratio is much better compared with DSDV protocol. For example, sending 16001 has resulted in 47.65% and 82.71% for DSDV and TERP respectively. Therefore, using the proposed TERP helps to maximize the number of received packets and thus increases the delivery ratio as shown in Fig. 11. Fig. 11, compares the delivery ratio of untrusted DSDV and TERP protocols where it highlights the difference in the performance of both protocols. TERP has a higher delivery ratio than DSDV and reaches about the same level when sending a large number of packets such as 128000 packets.

TABLE VIII: Summary of the delivery ratio of DSDV and TERP routing protocols

Number of Sent Packet	DSDV Delivery Ratio%	TERP Delivery Ratio%
8000	50.0%	91.51%
16001	47.65%	82.71%
32001	20.83%	37.31%
64000	11.96%	19.13%
128000	5.98%	9.67%

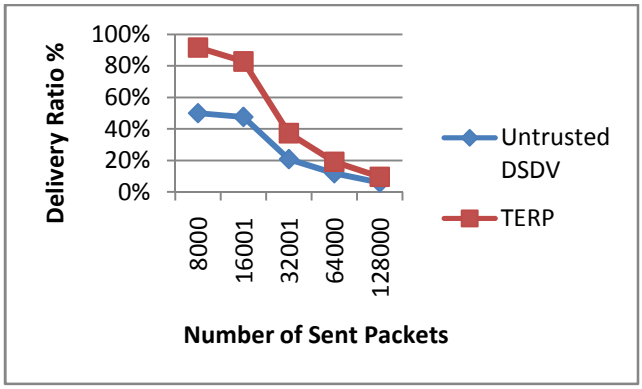

Figure 11. Compares the delivery ratio for both untrusted DSDV and TERP routing protocols

3) Average End-to-End Delay

Table IX gives the average delay for both DSDV and the proposed TERP protocol. As shown in Fig. 12, the average delay values for the TERP are higher than those for the untrusted DSDV over an interval. When the interval is 0.05, the average delay of DSDV is 0.0249 seconds while it is 0.0274 seconds using TERP. This is due to more information is sent to the trusted nodes without encryption which takes longer delays to process. However, in the case of untrusted nodes, only relevant encrypted information is sent and hence it is processed faster. Also as shown Fig.12, as the interval decreases, the average delay increases as well.

4) Delay Jitter:

In order to calculate the delay jitter, the maximum and minimum delays for a packet at each interval are needed as in Table X. Fig. 13 shows the delay jitter for both DSDV and TERP protocols. As expected, the trusted nodes take longer time than the untrusted nodes because of the amount of information sent to each node. When the interval is 0.003125 the delay jitter for DSDV is 1.4375 seconds where it is 11.668 seconds for TERP as provided in Table XI. As a result, as the interval decreases, the delay jitter increases.

TABLE IX: Comparison of the average delay of DSDV and TERP routing protocols

Interval	Average Delay of DSDV	Average Delay of TERP
0.05	0.0249	0.0274
0.025	1.0709	1.2739
0.0125	1.5989	1.6033
0.00625	1.3294	1.4685
0.003125	1.332	1.465

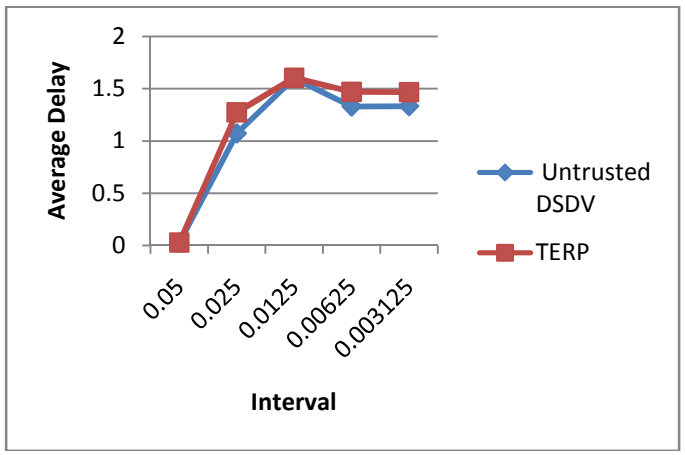

Figure 12. Comparison of the average delay for both untrusted DSDV and TERP routing protocols

TABLE X: The maximum and the minimum average delays for a packet.

Interval	Maximum Delay for a Packet	Minimum Delay for a Packet
0.05	0.0447	0.0225
0.025	2.1478	0.0448
0.0125	3.8029	0.0506
0.00625	1.9283	0.4098
0.003125	1.9283	0.4908

TABLE XI: The delay jitter of DSDV and TERP protocols.

Interval	Delay Jitter of DSDV	Delay Jitter of TERP
0.05	0.0222	0.0222
0.025	2.1029	2.6773
0.0125	3.7522	10.3763
0.00625	1.5185	25.9951
0.003125	1.4375	11.668

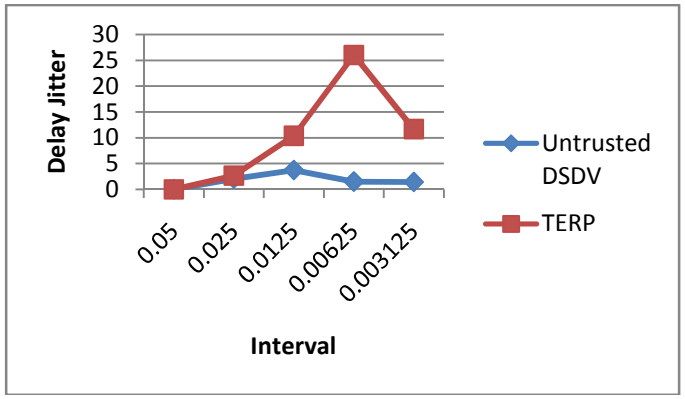

Figure 13. The jitter delay for both untrusted DSDV and TERP routing protocols

V. ANALYSIS OF RESULTS

Results show that TERP which is based on is performing better than the existing DSDV. The remaining energy in nodes after the simulation is higher than those used DSDV without trust. In other words, trust saves more power. The main reason why trust improves the power consumption is that it reduces or even removes cryptography in case of high trust from transmitted packets which results in that nodes need to transmit fewer bits for each packet than usual. This leads to less energy consumed in nodes. For instance, the sender node n0 saved 17.31% of its energy in case of using high trust. Also the receiver node n4 saved about 6.47% of its power and the energy that being saved in middle nodes was up to 15.62% as shown in Table II, and Table V. These results demonstrate that trust can improve the lifetime of a sensor network.

Moreover, based on our findings, TERP is performing much better than DSDV without trust. For example, when node n3 starts misbehaving and dropping packets, the existing DSDV does not have the mechanism to detect weather n3 is misbehaving or not. Therefore, DSDV without trust will think n3 is still acting in a good way and will continue to transmit packets to it while n3 is misbehaving. However, the proposed protocol TERP detects that n3 is not acting as expected. So, n3 is removed from the trusted nodes and added to the untrusted nodes. Furthermore, the proposed solution recalculates the route to the destination using only the route that all its nodes are trusted. Delivery ratio can be improved up to almost the double in the trusted scenario as shown in Fig. 11. However, the average end-to-end delay and delay jitter are increased in TERP due to more packets are and time duration needed to recalculating routes to the destination that does not have untrusted nodes as shown in Fig. 12.

VI. CONCLUSION

In wireless sensor networks (WSNs), saving energy is challenging as it is hard to recharge or replace the sensors used. This paper proposes a trusted and an energy efficient protocol called TERP that helps to maximize the network life. Simulation results show that TERP reduces the power consumption compared to the existing routing protocol DSDV using the trust concept. The more the level of trust is, the less encryption is needed. Three levels of trust are discussed in depth 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 and discussed. TERP has less drop ratio and more delivery ratio than DSDV.

REFERENCES

[1] Zahariadis, T.; Trakadas, P.; Leligou, H.; Karkazis, P.; Voliotis, S., "Implementing a Trust-Aware Routing Protocol in Wireless Sensor Nodes," *Developments in E-systems Engineering (DESE), 2010* pp.47,52, 6-8 Sept. 2010.

[2] García Villalba LJ, Sandoval Orozco AL, Triviño Cabrera A, Barenco Abbas CJ. " Routing Protocols in Wireless Sensor Networks," *Sensors*.9, No. 11, 2009.

[3] Praveena, A.; Devasena, S.; Chelvan, K.M.A., "Achieving energy efficient and secure communication in wireless sensor networks," *Wireless and Optical Communications Networks, IFIP International Conference, 2006.*

[4] Kulkarni, N.; Prasad, R.; Cornean, H.; Gupta, N., "Performance Evaluation of AODV, DSDV & DSR for Quasi Random Deployment of Sensor Nodes in Wireless Sensor Networks," *Devices and Communications (ICDeCom), 2011 International Conference on* , vol., no., pp.1,5, 24-25 Feb. 2011.

[5] Pushpa, A.M., "Trust based secure routing in AODV routing protocol," *Internet Multimedia Services Architecture and Applications (IMSAA), 2009 IEEE International Conference on* , vol., no., pp.1,6, 9-11 Dec. 2009.

[6] Pandey, A. K., & Fujinoki, H. (2005). Study of MANET routing protocols by GloMoSim simulator. *International Journal of Network Management , 15*, 393-410.

[7] Koliousis, A., & Sventek, j. (n.d.). Proactive vs Reactive Routing for Wireless Sensor Network. 7-8.

[8] Tyagi, S. S., & Chauhan, R. K. (2010). Performance Analysis of Proactive and Reactive Routning Protocol for Ad hoc Networkds. *International Journal of Computer Applications , 1*, 27-28.

[9] Sharma, m., & Singh, G. (2011). Evaluation of proactive, Reactive and Hybrid Adhoc Routing. *International Journal of Smart Sensors and Ad Hoc Networks , 1* (2), 65-66.

[10] Arif, M. Z., & Shrivastava, G. (2012). Trusted Destination Sequenced Distance Vector Routing Protocol for Mobile Ad-hoc Network. *International Journal of Computer Application , 15*, 0975-887.

[11] Gordon, R. L.; Dawoud, D. S., "Direct and indirect trust establishment in ad hoc networks by certificate distribution and verification," *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on* , vol., no., pp.624,629, 17-20 May 2009.

[12] Peterson, L. & Davie, B. Computer Networks Edition 4, San Francisco: Morgan Kaufmann, 2007.

[13] N. Nasser and Y. Chen, "SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2401–2412, 2007.

[14] Li Wei, Chen Ming, Li Mlingming. "Information Security Routing Protocol in the WSN". *The Fifth International Conference on Information Assurance and Securit*y. Xi'an, 2009. 651-656.

[15] F.De Rango, "Improving SAODV Protocol with Trust levels management, IDM and Incentive Cooperation in MANET," *in Wireless Telecommunication Symposium (WTS'09*), Prague, Czech Republic, 22-24 Apr.2009.

[16] Theodore Zahariadis, Panagiotis Trakadas, Helen Leligou, Panagiotis Karkazis, "Implementing a Trust-Aware Routing Protocol in Wireless Sensor Nodes", *DeSE 2010*, London UK, 6-8 September 2010.

[17] Rahhal, H.A.; Ali, I.A.; Shaheen, S.I., "A novel Trust-Based Cross-Layer Model for Wireless Sensor Networks," *Radio Science Conference (NRSC), 2011 28th National* , vol., no., pp.1,10, 26-28 April 2011.

[18] Poolsappasit, N.; Busby, M.; Madria, S.K., "Trust Management of Encrypted Data Aggregation in a Sensor Network Environment," *Mobile Data Management (MDM), 2012 IEEE 13th International Conference on* , vol., no., pp.157,166, 23-26 July 2012.