A Combinatorial Multi-Objective Trust Model for Efficient and Secured Routing in UWSN

U D Prasan[1], Dr. S Murugappan[2]

[1]Research Scholar, Dept. of CSE, SCSVMV University, Associate Professor, AITAM, Tekkali, Andhra Pradesh
[2]Department of Computer science & Engineering, Annamalai University, Chennai, Tamilnadu

Abstract*— Wireless Sensor Networks (WSN) play an important role in applications both in the civilian as well as in the defence sector. WSNs are autonomous, distributed, self-organized networks consisting of multiple sensor nodes. Usually, limited radio range of the nodes, arising from energy constraints and trust value amongst the nodes, is overcome with the cooperation between nodes. Attention in the domain of Underwater Wireless Sensor Networks (UWSN) is increasing because of its realistic applications and necessity of communication through mobile devices. A mobile ad hoc network consists of mobile self configuring wireless nodes and these nodes communicate amongst themselves without any centralized management system. Dynamic characteristics of UWSN, has made it fairly demanding to uphold connectivity and guarantee Quality of Service (QoS). Trust based routing is one way to develop cooperation among nodes for performing efficient routing between nodes. A trust based AODV is presented where nodes are selected for routing based on their trust values. A threshold value is defined dynamically and nodes are preferred for routing only if the trust levels are higher than the threshold. Energy levels of nodes are also considered to make routing still more efficient. Nodes which are selected for routing are also considered based on high energy levels. In addition, all data transmission is secured using MD5 algorithm. Simulation results show good improvement on QoS metrics like Packet Delivery Ratio, Throughput, Delay, Packet Received, Packet Loss and energy consumption when compared with traditional AODV and DSR.

***Keywords*— Wireless Sensor Network, Threshold value, Data transmission, Secured, Throughput, Delay.**

I. INTRODUCTION

Underwater communications are becoming increasingly important, with numerous applications emerging in environmental monitoring, exploration of the oceans and military missions. Until the mid-nineties, research was focused on hardware and on communication transmitters and receivers for the transmission of raw bits. In network terminology, this is known as the physical layer. Reasons for the rapidly increasing efforts into research on underwater networks are various. The ongoing exploration of the oceans calls for sensor networks to support wide-area environmental monitoring. Military applications are also emerging, especially in the areas of autonomous sensor networks for mine countermeasures (MCM) and anti-submarine warfare (ASW). Autonomous underwater vehicles (AUVs) play an important role in such networks as they may replace traditional platforms for tasks in mine hunting or detection, classification, localization and tracking of a target. The advantages of AUVs include covertness, cost effectiveness and a reduced risk for personnel. Academia involved in the development of radio frequency (RF) sensor networks[1] are now discovering the underwater world and corresponding challenges and opportunities.

Routing is a fundamental network primitive in any wireless network. Given typical transmitted power constraints, it is very unlikely that all nodes in a network are within the range of receiving from one another. For this reason, many messages may have to be relayed through multiple hops to reach their destination. This strategy brings about in terms of connectivity among far nodes, multi-hop routing generates two types of overhead: on one hand the messages get replicated throughout the network, as multiple nodes relay the original transmission; on the other hand, the decisions about which node should be a relay, requires some sort of signalling before routing actually takes place.

Nodes can join and leave the network at anytime and are free to move arbitrarily and organize themselves randomly. The simplicity of deployment and the infrastructure less feature of UWSN makes it extremely attractive for the present day scenarios. Dynamic topological changes are caused by quick and random node mobility that makes routing difficult in UWSN. Routing protocols in UWSNs are generally classified as proactive and reactive. Reactive routing protocols start to establish routes only when required or only if there is a demand. There are many reactive routing protocols, such as AODV, DSR, TORA, ABR, SSA and RDMAR. The other classification of routing protocol is table-driven or pro-active routing protocols. Each node maintains one or more routing information table of all the participating nodes and updates their routing information regularly to maintain most up-to-date analysis of the network. There are many proactive routing protocols, such as DSDV, WRP, CGSR and FSR. Traditional routing protocols [2] in UWSN assume a collaborating environment inside the network. However, this suggestion is not always true and an aggressive or vulnerable environment can seriously affect network performance. UWSN is a cooperation based network [12] that expects each participating node to forward packets. This nature of UWSN leads to the possibility that there could be some malicious nodes that try negotiating the routing protocol functionality and make UWSN vulnerable. Due to vibrant nature of UWSN, there are many issues which need to be dealt with and one of the areas for perfection is Quality of Service (QoS). When it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met. A few challenges faced in providing QoS are, steadily changing environment, unobstructed mobility which causes recurring path breaks and also make the link-specific and state-specific information in the nodes to be inexact.

Underwater networks are not different from other kinds of wireless networks in this regard. For many scenarios, including harbour patrol, coastline environmental monitoring, etc., the area of operations of the network may span several square kilometres, making single-hop networking impossible. In addition, specific features of underwater propagation [10] make multi-hop topologies more convenient: it has been shown that absorption losses (due to the resonance of pressure waves with salt particles in water) cause a significant attenuation phenomenon, whose entity grows exponentially with distance. This comes in addition to the usual spreading loss factor, which depends on distance according to a power law and is found in terrestrial radio transmissions as well. Such attenuation requires that very high power is used at the transmitter side, in order to cover a long-distance hop while achieving a sufficient Signal-to-Noise Ratio (SNR), and thereby correct reception.

A perfect trust model is introduced in the network layer to establish a secure route between source and destination without any intruders or malicious nodes. Continuous evaluation of node's performance and collection of neighbour node's opinion value about the node is used to calculate the trust relationship of this node with other nodes. This work has shown good improvement in QoS metrics. A routing algorithm which adds a field in request packet which stores trust value indicating node trust on neighbour is proposed. Based on level of trust factor, the routing information [11] will be transmitted depending upon the highest trust value amongst all. This not only saves the node's power by avoiding unnecessary transmission of control information resulting in effective of bandwidth (channel utilization), which is very important in UWSN. Here, a trusted path irrespective of shortest or longest path which can be used for communication in the network is proposed. A security-enhanced AODV routing protocol called R-AODV (Reliant Ad hoc On-demand Distance Vector Routing) is implemented by a modified trust mechanism known as direct and recommendation trust model and then incorporated inside AODV which will allow AODV to not just find the shortest path, but instead to find a short path that can be trusted. This enhances security by ensuring that data does not go through malicious nodes that have been known to misbehave. The R-AODV protocol does provide a more reliable data transfer mechanism compared with the normal AODV if there are malicious nodes in the UWSN. This has shown good improvement in QoS metrics.

II. TRUST MODEL

The idea of using trust to moderate security threats has been an important area of research. The concept of “Trust” is defined as the degree of subjective belief about the behaviour of a particular entity. The trust based routing is one way to build cooperation among nodes for establishing an efficient routing path. Trust value plays a crucial role in all of the network activities [3]. Continuous evaluation of node's performance is used to calculate the trust value of the node. Basically Mobile ad hoc networks are designed for a cooperative environment but in hostile environments trust-based routing should be used. Instead of establishing the shortest route as done in traditional routing protocols, trusted routes are established to make it a trustworthy and efficient routing.

A trust based work is designed and implemented in the network layer. All nodes transmit and receive packets [9] to all other nodes in the network. Not all transmissions are successful. Some packets reach destination successfully and some may be lost or dropped. Thus, based on this concern a trust model is defined here which takes into account the success and failure rate of transmission of the node. Trust value is calculated based on success and failure rate and trust values for nodes are stored separately for each node during simulation. When network starts, all nodes are trusted nodes and the initial trust value is 1 for all nodes. This value either increases or decreases based on nodes success or failure rate.

The trust level value calculation [4] is based on the parameters shown at Table 1. The count field describes two criteria, success rate (packets delivered successfully) and failure rate (packets lost or not delivered). RREQ and RREP are the route request and route reply respectively which are exchanged between nodes in the network. Data refers to the payload transmitted by the node in the routing path.

TABLE 1
TRUST VALUE CALCULATION PARAMETERS

Count Type	RREQ	RREP	Data
Success	qrs	qps	qds
Failure	qrf	qpf	qdf

The parameter qrs is defined as the query request success rate and is calculated based on number of neighbouring nodes which have successfully received (RREQ) from the source node which has broadcasted it, qrf defined as the query request failure rate which is calculated based on number of neighbouring nodes which have not received the query request, qps is defined as the query reply success rate which is calculated as successful replies (RREP) received by the source node which has sent the RREQ and qpf is defined as the query reply failure rate which is calculated based on the number of replies not received by the source node for which RREQ was sent. qds is defined as the data success rate calculated based on successful transmitted data and Qdf is defined as data failure rate calculated based on data which has failed to reach destination.

$$Qr = \frac{q_{rs} - q_{rf}}{q_{rs} + q_{rf}}$$

$$Qp = \frac{q_{ps} - q_{pf}}{q_{ps} + q_{pf}}$$

$$Qd = \frac{q_{ds} - q_{df}}{q_{ds} + q_{df}}$$

TL=T(RREQ) * Qr + T(RREP) * Qp + T(DATA) * Qd

Where Qr, Qp and Qd are intermediate values that are used to calculate the nodes Request rate, Reply rate and Data transmission rate. TL is the trust level value and T(RREQ), T(RREP) and T(DATA) are time factorial at which route request , route reply and data are sent by the node respectively.

The next hop node is selected based on the trust value. To select the next hop node the trust value of all neighbouring nodes from current source node are calculated and finally a node which has highest value and greater than the threshold is selected as next hop node for the current routing [5]. For example, Route starts from node N1 and next hop node N2 is selected. Now to select next hop node for N2 its neighbours are identified and their trust values are calculated. If N3, N4, N5, N6, N7 are the neighbouring nodes of N2 then trust value for all these nodes is collected and an average of this is identified and this value is set as threshold value for selecting the next hop node for N2 only. The node which has the highest trust value than the threshold will be selected as next hop node. Threshold value is calculated dynamically for every next hop node selection in each run. The nodes which are not selected for the current transmission [6] based on their trust value cannot be tagged as unfit node because it can serve as best trusted node for another transmission based on the scenario. The tables 2 and 3 show the comparison of QoS metrics values of Trust based AODV and Traditional AODV. QoS metrics have improved when compared with traditional AODV.

TABLE 2
COMPARISON OF AODV AND TRUSTED AODV ON QOS METRICS PACKET DELIVERY RATIO AND THROUGHPUT

Node size	Packet Delivery Ratio (PDR)		Throughput	
	AODV	Trusted AODV	AODV	Trusted AODV
25	29.99	33.78	40	56
50	31.50	67.94	130	257
100	56.78	72.68	3175	7485
200	62.45	75.52	6350	14970
300	66.82	81.56	9525	22455

TABLE 3
COMPARISON OF AODV AND TRUSTED AODV ON QOS METRICS DELAY, PACKET RECEIVED AND PACKET LOSS

Node size	Delay		Packet Received		Packet Loss	
	AODV	Trusted AODV	AODV	Trusted AODV	AODV	Trusted AODV
25	0.235	0.004	42	67	23	18
50	1.415	0.065	132	247	37	28
100	8.799	2.647	3235	7364	58	42
200	17.598	7.058	6460	14728	116	84
300	26.388	9.852	9695	22092	174	135

III. ENERGY AND SECURITY

In UWSN, nodes energy also plays a key role. Node should have a good energy level to complete the transmission successfully. Though the node is said to be a reliable node and has a good success rate of transmission, it fails if it does not have energy. Therefore energy becomes vital for all nodes to perform a efficient transmission.

One of the related works proposes and investigates a power-aware ad hoc on-demand distance vector routing protocol (PAW-AODV) for efficient power routing. PAW-AODV could use the limited power resources efficiently as it routes based on a power-based cost function. Both AODV and PAW-AODV are simulated under various mobile situations. Another similar work based on energy proposes a enhanced AODV routing protocol, modified to improve the networks lifetime in UWSN. One improvement for the AODV protocol is to maximize the networks lifetime by applying an Energy Mean Value algorithm [7] which considers node energy of each node.

This paper proposes an energy model where a node is selected for routing only if its energy level is greater than the threshold value (average of energy values of the neighboring nodes). Energy calculation is based on nodes sending and receiving signal strength. Energy level the nodes are evaluated where sender to increase transmission power to identify best nodes with more energy levels. Current Energy level of node can be calculated by the initial energy level and the consumed energy level of a node. During simulation scenario energy values are displayed on top of each node. For every transmission the transmission power and reception power gets subtracted from its initial value of 100 Joules (initialized during simulation).

Thus, the consideration of node's energy value makes the routing more efficient compared with traditional AODV. During simulation, communication messages (RREQ and RREP) are exchanged between nodes in the network. RREP contains energy values. Therefore, energy for nodes needs to be considered while routing since nodes energy levels may be lowered due to drain. Though a node is providing its complete support for routing it can perform well only if it has sufficient energy.

The transaction made by nodes in UWSN should be a secured transaction. To provide security for all transactions Message digest algorithm is introduced during transmission. All transmissions are secured using MD5 Algorithm. MD5 algorithm is also introduced to secure transmissions and increase the reliability in routing. These algorithms operate on a message 512 bit at a time. Pad the message to a multiple of 512 bits. Digest calculation begins with digest value initialized to a constant. This value is combined with first 512 bits of message to produce a new value for the digest; using a complex transformation [8]. New value is combined with next 512 bits of message using same transformation and so on until final value of digest is produced. The main ingredient of MD5 algorithm is the transform that takes input as current value of the 128 bit digest, plus 512 bits of message and outputs a new 128-bit digest. MD5 operates on 32 bit quantities. Current digest value can be thought of as four 32-bit words(d0, d1, d2, d3) and piece of message currently being digested (512) as sixteen 32 bit words (M0 through M15). Traditional AODV do consider the energy levels of nodes before routing. Energy is announced by the proposed AODV protocol which checks for energy levels of nodes before taking part in routing and transmissions are secured using MD5 algorithm in order to make the UWSN routing efficient and effective and ensure QoS. The following table-4 and table-5 show the QoS metrics for traditional AODV and proposed AODV respectively.

TABLE 4
QOS METRICS FOR ENERGY BASED TRADITIONAL AODV

Node Size	Traditional AODV		
	PDR	Delay	Throughput
25	54.45	0.33567	757771.43
50	66.36	0.22496	120032.60
100	72.35	0.18624	115783.25

TABLE 5
QOS METRICS FOR ENERGY BASED PROPOSED AODV

Node Size	Proposed AODV		
	PDR	Delay	Throughput
25	76.78	0.18567	846472.68
50	81.93	0.12404	248723.74
100	88.36	0.13993	272375.46

IV. TRUST, ENERGY AND SECURITY

Two separate works one based on trust model and another based on Energy and security were proposed and simulated. Results show that they perform well compared with traditional AODV [13]. To achieve better results we combine these two models together. A new work where routing between nodes is done considering the nodes trust and energy values in addition transmission is secured with MD5 algorithm.

Related works which combine trust and energy have also shown good improvement over QoS metrics. A reliable routing algorithm is proposed where three parameters are determined: trust value, energy value and reliability value which are used for finding a stable route from source to destination. During route discovery, every node records its trust value and energy capacity in RREQ packet .In the destination ,based on reliability value , is decided which route is selected .The path with more reliability value [8] is selected to route data packets from source to destination. The proposed method has significant reliability improvement in comparison with AODV.

Another related work shows an energy consumption model to calculate the energy-factor of the nodes is considered and then a trust based protocol for energy-efficient routing is proposed. A trust module to track the value of routing metric is adopted. Simulation results show that the proposed protocol reduces delay and increases packet delivery ratio by consuming less energy compared to AODV and DSR. Thus, a new enhanced AODV which implements Trust model and energy model for efficient routing in UWSN where each transmission is secure using MD5 algorithm is proposed in this work.

V. RESULTS

Performance of proposed AODV protocol is analysed using NS-2 simulator. The network is designed using network simulator with 25, 50, 100, 200 and 300 nodes. General AODV & DSR are simulated initially and its QoS metrics is observed. Enhanced Trust based AODV is simulated and its results are also observed. Results are compared in terms of Packet delivery ratio, Packet received, Packet loss, Throughput, Delay and Energy consumption ratio. The proposed Trust based AODV shows good improvement in QoS metrics. PDR and Throughput are higher, Packet loss and delay are reduced, and energy consumption is also less compared with general AODV and DSR. Following tables 6, 7,8,9,10 and 11 show the comparison of general AODV, DSR and proposed AODV on QoS metrics such as Packet Delivery Ratio (PDR), Packet Received, Packet loss, Throughput, Delay and Energy respectively.

TABLE 6
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC PACKET DELIVERY RATIO WITH DIFFERENT NODE SIZES.

Node size	Packet Delivery Ratio		
	AODV	DSR	Trusted AODV
25	29.99	31.89	35.35
50	31.50	44.64	69.47
100	56.64	54.23	76.25
200	62.84	58.43	80.27
300	68.72	61.63	85.81

TABLE 7
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC PACKET RECEIVED WITH DIFFERENT NODE SIZES.

Node size	Packet Received		
	AODV	DSR	Trusted AODV
25	40	49	64
50	132	323	367
100	3235	956	8316
200	6460	1912	16632
300	9695	2868	24948

TABLE 8
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC PACKET LOSS WITH DIFFERENT NODE SIZES.

Node size	Packet Loss		
	AODV	DSR	Trusted AODV
25	00	08	00
50	03	22	02
100	58	83	39
200	116	166	72
300	174	249	111

TABLE 9
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC THROUGHPUT WITH DIFFERENT NODE SIZES.

Node size	Throughput		
	AODV	DSR	Trusted AODV
25	40	44	64
50	130	299	367
100	3175	873	8276
200	6350	1746	16552
300	9525	2619	24828

TABLE 10
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC DELAY WITH DIFFERENT NODE SIZES.

Node size	Delay		
	AODV	DSR	Trusted AODV
25	0.235	0.875	0.001
50	1.415	3.923	0.006
100	8.799	17.292	1.516
200	17.598	34.584	3.032
300	26.388	51.976	4.548

TABLE 11
COMPARISON OF GENERAL AODV, DSR AND PROPOSED AODV ON QOS METRIC ENERGY WITH DIFFERENT NODE SIZES.

Simulation Time	Energy		
	AODV	DSR	Trusted AODV
5	96.098	96.557	97.067
10	92.273	93.182	94.192
15	87.748	88.907	90.617
20	84.000	85.600	87.799
25	80.155	82.427	83.324

VI. CONCLUSION

Nodes in UWSN may misbehave or drop packets during routing which affects the QoS parameters and brings down the performance of the Network. Many approaches have been proposed for identifying these misbehaving or malicious nodes. A trust model is proposed which identifies misbehaving nodes, the routing path and isolates those nodes from routing and selects an alternate path for efficient routing and also improves the QoS performance. The trust factor is calculated based on the nodes success rate and failure rate of transmission. Though node is trusted if it does not have enough energy in it becomes ineffective for routing. Therefore Energy is also considered for routing where in node should have sufficient energy for taking part in routing. Finally, a trust and energy based model is proposed. All data transmissions are secured with MD5 algorithm and provide security for transmission. Simulation results show significant improvement in QoS metrics. Results of the proposed AODV protocol are compared with traditional AODV and DSR protocol. In proposed AODV protocol, Packet delivery ratio is increased, throughput is increased, Packet loss is reduced and Delay is also reduced. Energy consumption is reduced in the proposed protocol.

REFERENCES

[1] A. Abraham, A. Hassanien, and V. Snasel, “Computational social network analysis: trends, tools and research advances”, Springer-Verlag New York Inc, 2009.

[2] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, Reputation and Trust- based systems for Ad Hoc and Sensor Networks," Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, 2006.

[3] A. Kellner, K. Behrends, and D. Hogrefe, \Simulation Environments for Wireless Sensor Networks," Institute of Computer Science, Georg-August-Universit • at G • ottingen, Germany, Technical Report No. IFI-TB-2010-04, June 2010, ISSN 1611-1044. [Online]. Available: http://_lepool.informatik.uni-goettingen.de/ publication/tmg/2010/AK KB 2010 01.pdf

[4] D. Angus and C. Woodward, \Multiple objective ant colony optimisation," Swarm intelligence, vol.3, no. 1, pp. 69 - 85, 2009.

[5] M. Hempstead, M. Lyons, D. Brooks, and G. Wei, “Survey of hardware systems for wireless sensor networks," Journal of Low Power Electronics, vol. 4, no. 1, p. 11, 2008.

[6] K. Pister, J. Kahn, B. Boser et al., “Smart dust: Wireless networks of millimeter-scale sensor nodes”, Highlight Article in, p. 2, 1999.

[7] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security: A survey”, Security in distributed, grid, mobile, and pervasive computing, p. 367, 2007.

[8] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks”, IEEE Communications Surveys and Tutorials, vol. 8, no. 2, pp. 2 - 23, 2006.

[9] J. Zhang, P. Orlik, Z. Sahinoglu, A. Molisch, and P. Kinney, “UWB systems for wireless sensor networks," Proceedings of the IEEE, vol. 97, no. 2, pp. 313 - 331, 2009.

[10] L. Rasmusson and S. Jansson, “Simulated social control for secure Internet commerce," in Proceedings of the 1996 workshop on New security paradigms. ACM New York, NY, USA, 1996, pp. 18 - 25.

[11] A. J_sang and S. Pope, “Semantic constraints for trust transitivity," in Proceedings of the 2nd Asia-Pacific conference on Conceptual modeling, Vol. 43. Australian Computer Society, Inc., 2005, pp. 59-68.

[12] P. Dasgupta, “Trust as a Commodity”, Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, pp. 49 - 72, 2000.

[13] R. Lewicki and B. Bunker, “Trust in relationships: A model of development and decline," Conict, cooperation, and justice: Essays inspired by the work of Morton Deutsch, pp. 133 - 173, 1995.