International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/207979 Volume 8, Issue 1, January – February (2021)

RESEARCH ARTICLE

Performance Evaluation of a MANET based Secure and Energy Optimized Communication Protocol (E^2S-AODV) for Underwater Disaster Response Network

Karan Singh
Department of Computer Science and Applications, M.M. Institute of Computer Technology and Business Management, MMDU, Mullana, India
karanola123@gmail.com

Rajeev Gupta
Department of Computer Science and Engineering, M.M. Engineering College, MMDU, Mullana, India
rajeev.gupta@mmumullana.org

Received: 10 December 2020 / Revised: 29 December 2020 / Accepted: 04 January 2021 / Published: 23 February 2021

Abstract – In recent years, the role of telecommunications in Under Water Mobile Ad-hoc Network (UWMANET) has emerged as a significant field during disaster prevention and rescue operations. Various disaster prevention and rescue supported applications are introduced in these years for flood, tsunamis, and underwater earthquakes. While communication in UWMANET, the existing communication system has some limitations like high energy utilization, tremendous packet loss rate, and delay. Sensor nodes can be deployed for data collection from the dense underwater environment. In UWMANET, security is another critical aspect of secure data transmission. In this paper, a new UWMANET based routing protocol, i.e., E^2S-AODV (Energy Efficient Secure Ad-hoc On-demand Distance Vector) is designed and tested for Under Water Disaster Response Network (UWDRN) in a controlled environment. The optimum route for data transmission is selected by Pigeons Swarm Optimization (PiSO). PiSO reduces the hop count in the chosen shortest path. Hello, messages are broadcasted to inform their neighbors that the connection to the host is active. LDW technique is used to authenticate these hello messages. For security purposes, original event message encrypted with CST (Ciphertext Stealing Technique) and qu-Vanstone ECC based public-key cryptography. To utilize energy efficiently, E^2S-AODV introduced two energy concepts drains rate finder and residual energy finder. Results that are compared with existing disaster-based protocols; are pro-motive and assure an improved quality of service (QoS) achievement in terms of many multipronged metrics like energy efficiency, reliability, security, scalability, delay, and Throughput, etc. E^2S-AODV achieved a 2% improvement in PDR, 5% enhancement in Throughput, 8% reduction in end-to-end delay, and 11% reduction in energy utilization compared to its near existing competent.

Index Terms – Energy Efficiency, End-to-End Delay, E^2S-AODV, MANET, PDR, QoS, Security, Throughput, UWDRN, UWMANET.

1. INTRODUCTION

The disaster prevention area has got great advancement in the research fields of MANET. MANET has many variants on behalf of its usage i.e., VANET (Vehicle Ad-hoc network), UWMANET (Under Water Mobile Ad-hoc Network), etc. An underwater acoustic mobile ad hoc network (UWMANET) is a significant research area in disaster prevention and rescue operations in the current era. UWMENT communication is much useful in disaster prevention applications. Traditional UWMANET has some limitations: high power utilization, high delay, and poor scalability [1]. Also, traditional UWMANET has less security due to inappropriate security modes in dense medium and more attackers in the network. These attackers may enter the network and engage with resources for a long time, leading to unnecessary delays in a network [2]. Therefore, underwater sensors are utilized for forwarding collated data to the surface station. The term Under Water Mobile Ad-hoc Network includes four various dedicated words: (i) Underwater means the dense medium where a network can be deployed (ii) Mobile, i.e., voyaging autonomously in nature, (iii) Ad-hoc implies minuscule time length, (iv) Network, i.e., a pool of a few hubs [3]. Thus, this network is defined as an underwater mobile ad-hoc network (UWMANET) [4, 5]. The UWMANET network has many supported devices for communication. The components involved in this type of network are as follows:

RESEARCH ARTICLE

- Sensor nodes (for sensing/collecting underwater information).
- Gateway nodes (connection to underwater route).
- Mobile/moving/floating nodes (AUVs)
- Portable sink node (node without underwater link like ship etc.)
- Onshore surface station (for broadcasting information to predict any decision, i.e., rain, high tides, etc.)

1.1. Problem Statement

In UWMANET, researchers are focusing on some issues like power utilization, network load, transmission delay, and security. Additionally, various network performance parameters (QoS), i.e., packet delivery ratio (PDR), Throughput, end-to-end delay, scalability, and security, are challenging issues in a dense and sparse medium of UWMANET based applications. The traditional UWMANET network establishment process is based on three functions such as node finding, clustering (making subgroups), and data collection. UWMANET has various open issues. Some of them are as follows:-

- **Under Water Network Topology:** We can put this issue at the highest priority to be resolved. In traditional research work, 2D or 3D network topology is discussed for framing underwater topology [3, 5].
- **Under Water Node Distribution:** How to distribute the nodes in the underwater network is another major issue. Node distribution should cover all importation area which can generate the required information. Node distribution may adversely affect the network's energy utilization mechanism and packet delivery system.
- **Energy Utilization:** UWMANET has a critical issue named energy efficiency. UWAMNET's devices are battery operated. The energy of devices should be utilized efficiently to enhance network performance. The designed protocol should consume minimum battery power for data transmission. However, numerous traditional safe and power-aware routing protocols have been projected to improve data communication, but no new works have been implemented for reliable network transmission [2].
- **Under Water Connections:** Underwater node connection is essential and faces various issues like noise, path break, propagation delay, and bandwidth utilization, etc. Therefore, a UWMANET network should take care of the underwater connection establishment process.
- **Scalability:** If a network is efficient for a small topology (having few nodes), it must be suitable for large-scale topology. This is the scalable nature of any network. Scalability should be resolved in UWMANET [2, 3, 4].
- **Robustness:** Attacker nodes are efficiently recognized in the network, which must be removed to avoid the reason for any node breakdown. The network must run for a longer time without any involvement of malicious nodes.
- **Security:** Transmission between the initiator node and the target node must be secure. Security protocol must be easy and straightforward to employ in a controlled underwater environment. Many researchers utilize lightweight cryptography to deal with a security challenge.

1.2. Motivation

Underwater observation has a vital role in all the applications in current days as 70% area of our earth is occupied by ocean water. These days, UWMANET is utilized for various applications like ocean behavior monitoring, disaster prevention, rescue operations, wind, and pressure monitoring, ocean water level monitoring, underwater behavior monitoring, underwater navigation, and tactical monitoring for the navy, etc. Accordingly, these systems can be suitable and usable for understanding these kinds of circumstances in current patterns and the future. UWMANET is supported by many network components like sensors for data collection, modem for transmission devices, etc. UWMANET can be useful in various underwater applications like ocean behavior prediction, studying the underwater movement, navy tactical data transmission, etc [5].

1.3. Objective

A new scheme named E^2S-AODV (Energy Efficient Secured Ad-hoc On-demand Distance Vector) routing protocol is introduced for UWMANET to deal with the challenges mentioned above. The proposed protocol is an enhanced version of the traditional AODV (Ad Hoc On-Demand Distance Vector) protocol. AODV is used in such a network where high mobility, on-demand data transfer, and less control overhead is required. Therefore it is suitable for designing a new enhanced protocol based on AODV with adding some exciting features like security, energy-efficient route optimality, etc. Network deployment has many sensor nodes. The proposed secure network enhances PDR and diminishes power utilization and delay.

1.4. Foremost Contributions (Basic Approach)

An E^2S-AODV routing protocol is designed for underwater disaster response applications, and this can also cope with security, optimality, and energy efficiency. The proposed protocol is an enhanced version of traditional AODV with improved security, optimality, and energy consumption. During a data transfer, the node finds the optimum route. The basic concepts and methods which are applied in the proposed protocol are summarized here [2, 3, 4, 5]:-

- The shortest path is discovered by Pigeons Swarm Optimization (PiSO). PiSO also reduces the hop count in the fastest route.
- For event communication, Cipher-text Stealing Technique (CST) is utilized to change the last two squares of plain text and encoded using qV-ECC. CST takes care of the Ciphertext development issue.
- The qu-Vanstone based Elliptic Curve Cryptography (qV-ECC) found short-term public key method is used for node verification.
- For necessary information transmission, we utilize Lightweight Digital Watermarking (LDW) to secure and authenticate "hello" messages. At that point, the watermark bits are implanted into an original packet and are sent to the quick transfer hub. LDW works like a data hiding method that decreases computation cost over traditional cryptography methods.
- Energy utilization assessment is the central component of this research and performed by *energyEfficientRouteDiscovery()* module using two sub-modules, i.e. (i) Residual Energy Analyzer and (ii) Drain Rate Finder. For efficient utilization of battery power, two crucial attributes of energy named "residual energy" (RE) and "drain rate" (DR) are employed.

E^2S-AODV can be a multipronged solution for many disasters like situations like a flood, drought, fire in the forest, tsunamis, underwater movements in oceans, emergency rescue operations, disaster prevention operations, weather forecasting, tracking of wild animals, traffic controlling, and vehicle movement tracking and message passing from one moving vehicle to other on highways, etc. [2, 3, 5]. For implementation, the proposed protocol is used for Underwater Disaster Response Network (UWDRNs). The results are compared with existing protocols, i.e., AODV, E2-SCRP, HAMA, ABSR, GA-CRAP, and SO-AODV, within a controlled environment using a simulation tool named network Simulator Version 2 (NS2) [4, 5]. NS2 uses TCL based scripting language. NS2 is specially designed for simulation purposes for analyzing and study the research area of the communication network.

The paper organization flow: - Section 2 deals with various former literature works related to underwater DRAs in recent years and finds knowledge (research) gaps. Segment 3 follows a line of investigation (research methodology) to be accompanied while complete the research journey. Section 4 discover the problem, originate it, and proposed a protocol for UWMANET based disaster response network. This section also offers a logical pseudo code for the proposed protocol. Section 5 offers the logical architecture and flow chart of an underwater disaster based network. Section 6 depicts a mock-up (simulation) setup. Section 7 involved outcomes and performance assessment of the anticipated solution in respect of underwater DRA. This section also judges the results of existing underwater DRAs and compares with the proposed E^2S-AODV. Section 8 wrap up concerning overall hard work made in the formulation of the research. Finally, segment 9 offers some future directions and some more relatable employ of the proposed solution.

2. LITERATURE REVIEW AND KNOWLEDGE GAP

This section addresses communication issues, challenges, and achieved solutions in terms of protocols, algorithms. The previous study pretends that these efforts are useful in MANET based disaster response applications, i.e., in communicating restricted environment (in simulation), flood based disasters, underwater sudden movements.

Singh and Gupta in [2020] [3] presented a solution for DRA based issues named SO-AODV. The proposed solution is a secure and optimized Ad-hoc on-demand distance vector routing protocol over AODV with QoS for Disaster Response Applications (DRA). The shortest path is discovered by Pigeons Swarm Optimization (PiSO). PiSO also reduces the hop count in the preferred shortest route. "Hello" packets are authenticated by the LDW technique. We are using the Ciphertext Stealing Technique (CST) with encryption qu-Vanstone Elliptic Curve Cryptography (qV-ECC) based public key for the security of event messages cryptography. The qV-ECC generates the public key. NS2 found experimental are evaluated and compared over AODV for several metrics, i.e., PDR, Throughput, end-to-end delay, etc.

Singh and Gupta in [2020] [4] investigated a power-aware AODV protocol for DRA-based applications, i.e., "An Energy-Efficient Multipronged Reliable Strategy ensuring Secure and Scalable QoS over Disaster Response Applications". The authors presented a solution for energy efficiency and security in MANET. The presented method is an enhanced version of traditional AODV with added features like security and energy efficiency (through residual energy concept). Proposed technique achieve authentication of "hello" message via LDW and security encryption of event messages by CST (Ciphertext Stealing Technique) with a key generation technique, i.e., qu-Vanstone ECC based public-key cryptography. The procedure named Energy_Efficient_routeDiscovery() will calculate the residual energy of nodes that will decide which node has sufficient power to take part in communication. Many multipronged features like reliability, scalability, secured route with QoS, minimum control overhead, and energy consumption will be simulated. Further, the proposed method can also be tested with any UWMANET.

Yadav and Kush in [2019] [5] recommended a new secure and power-aware protocol for underwater MANET named E^2-SCRP and implemented it in a three-dimensional ad-hoc network, i.e., UWMANET. UWMANET is a unique network environment into the water called 3D Under-Water acoustic MANET (UWMANET). Environment activity capturing device/sensors are set up in three dimensions in the depth of water for monitoring underwater movements. Type two fuzzy-based multilayered techniques are used for energy efficiency, and CST is implemented for fulfilling the security parameters. Various metrics like PDR, power utilization, security, end-to-end delay, Throughput, etc., are examined under a simulator environment for authenticating the proposed protocol.

Yu et al. in [2016] [6] introduced a lopsided cluster organization technique dependent on a layered system for occasion inclusion. The power utilization during data transfer at various profundities of the submerged organization is examined. The organization is divided into different levels, and the organization is framed with inconsistent bunches. Under this arrangement, the system builds start to finish deferral and expands energy utilization.

Ghoreyshi et al. in [2016] [7] recommended a hop-constrained clustering method in underwater sensor organizations, in which portable hubs are utilized for information assortment. This methodology is actualized for thick underwater sensor condition. The essential interests are center around lessening information collection delay and power utilization. Information assortment is executed utilizing clustering measure. Sensor's gathering information is further forward it to moving underwater utility vehicles. After clusters are framed, moving utility vehicles go for an optimal path to move near to sensor nodes, collect information, and forward it to the onshore surface sink station. Ideal sensor data collection and forward plans are noteworthy. This paper explored these Issues but not much reason for massive scope networks.

Cai et al. in [2019] [8] presented versatile edge components for genuine portability replica. Here, utility vehicle's speed and versatility two parameters are significant boundaries while gathering information from the depth of ocean water. Auditory and magnetic connections are coordinated for factual data communication. It limits information assortment time. Power utilization is adjusted in the whole organization and other execution measurements, such as network lifetime, PDR, and Throughput. The proposed solution is not suitable for long-range communication, which prompts high information assortment time utility vehicles, and this is also not well suited for scalable well for checking adversity situations. Information transmission time is much higher when the data load is heavy on the network.

Zhu and Wei in [2018] [9] exposed layers supported inconsistent groups for network dependent on sensing devices, further utilizing a power-aware routing scheme. Three different phases are combined in this article, i.e., (i) asymmetrical group creation, (ii) communication Routing, and (iii) revision and maintenance of cluster. The presented report highlights the hotspot issue and looks up the information communication and compilation execution. A novel optimization practice is introduced in a multipronged manner to handle the cost and incentive for cluster head (multi incoming link point). This method measured two features for sensing nodes, i.e., (i) forward ratio and (ii) remaining power of sensing nodes. Inconsistent clustering is a decent answer for the hotspot issue, yet it isn't reasonable to relieve all grouping issues.

Khan and Dwivedi in [2018] [10] investigated a technique named ADAN-BC, where nodes can make large holes in the operation area. Mobility metrics of the network can be a solution for sensor arrangement in the proposed method. The organization of portable sensor hubs is performed haphazardly for better organization inclusion. Groups are created dependent on space among mobile sensing nodes and their remaining power (residual).

Wang and Bang in [2017] [11] examined the idea of the node tumbling method in undersea sensing organizations. It tends to the issue of organization setup, i.e., connectivity within the network and coverage area. The organization is made out of anchored hubs. The sensor hubs are conveyed haphazardly on the sea surface. Three issues are addressed; first, proficient three-dimensional circle pressing example to pick the principal cluster of sink hubs. Second, sink hub availability is checked and third; fix inclusion openings by as of now sink hubs. Hub sinking calculation isn't compelling for enormous scope 3D underwater networks.

Khosravi and Rostami in [2018] [12] presented a fusion technique called SDV. This communicational method has come for information sending, and it highlights two issues of water depth based sensing network (UWSN). These are as follows: (i) path/link safety, (ii) correspondence traffic. Efficient working in thick underwater systems, power utilization, better reliability, and enhanced data delivery ratio is aimed by this article. The routing process is improved by the vector forwarding method. Scalability is a significant drawback in this technique.

Gomathi and Manickam in [2017] [13] addressed a multilayered directing convention to enhance the general working of the delay, lifetime of the implemented network, and compelling power usage. A joining technique is introduced for effective information transmission through an

RESEARCH ARTICLE

optimal path (shortest). The join work decides the whole of power relating to an associated hub, and furthermore, the path having the best power is opted to launch information from sensing device to surface sink station. It is reasonable for a specific number of hubs in an organization, for example, in an inadequate organization. Delay is high because discovering the path with the most excellent conceivable power with the least distance must be considered for information transmission.

Gomathi and Manickam in [2018] [14] investigated a technology named three-dimensional ZOR. ZOR is supported by "time differential on arrival." Both ZOR and TDOA are combined to solve the disaster based situations in under level water sensing network. In the ZOR region, submerged data is gathered and sent to a utility vehicle. When a fixed node is energy drained, then the hub with the most leftover power is selected for information broadcast. A probability model GMM (Gauss Markov Model) is useful for process hub power and portability in UWAN. This article also explores more power consumption reasons while working with fixed nodes.

Lal et al. in [2017] [15] recommended a hybrid MANET architecture. This model works for many qualities like hub/node mutual aid, context understanding, communication medium-security, i.e., physical layer protection, and cognition. When the network level is different, and the deployment area is changed, this model updates itself and protects the system from various attacks.

Zhao et al. in [2017] [16] projected ECPM (Elliptic Curve Point Multiplication) method. ECPM diminishes the computational load. It can manage the session and event authentication by maintaining key generation and key management. The projected key arrangement plot neutralizes different security attacks, for example, replay assaults, replication attacks, Sybil assaults, spoofing, etc.

Yan et al. in [2018] [17] planned a new security solution named ultra-lightweight scheme (UAN) for undersea acoustic ad-hoc networks is advised. 8-round slab cipher is proposed instead of using S-box slab encryption. The chaotic hypothesis is assumed for this, which leads to enhancement in the keyspace by tailored iteration rounds. Anticipated encryption scheme opposes brute force security assail. UAN decrypts only if the message is authenticated by the node and stops a malicious person from injecting a fake note.

Bisen and Sharma in [2017] [18] suggested a security solution for MANET named AB-SEP (Agent Based-Secure Enhanced Performance). Some features, i.e., reliability, energy level (residual), distance, node mobility, optimality, etc., are used for selecting the agent. Selected agent nodes are used for spiteful activities recognition. These behaviors are figure out by "Fuzzy-Based Secure Architecture (FBSA)." FBSA model enhanced some complexity and communication overhead.

Vamsi et al. in [2019] [19] planned a secure short digital signature scheme and this leads to verification between source and sink. The trapdoor technique achieves the routing procedure. An increase in Ciphertext issues can arise, leading to communication overhead, but the proposed solution created a digital signature and affixed it to the original data packet.

Sathiamoorthy et al. in [2017] [20] addressed a competent fuzzy approach in cluster formation. The proposed method has two steps, one formulates of fuzzy clusters and the other brings in a 3-level filtering method. Fuzzy technique assigns membership to each node; while filtering system is used for identify the malicious nodes. This helps is determining the identity and authenticity of the cluster members'. This also helps in improving the packet transmission in ad hoc networks like MANETs.

Sathiamoorthy et al. in [2018] [21] recommended a fuzzy dynamic cluster routing protocol (FDCRP). FDCRP has a trusted waterfall system to compete with MANETs issues. The proposed scheme will reduce the requirement of finding a new path from the source to the destination. New path is established whenever the packet travels towards the destination node by using a peer group of clusters. Energy consumption model is helped by ant colony optimization involving fuzzy rules. ACO-fussy combination reduces the time and energy. The FDCRP protocol can help in improving the network performance when compared to the previous network scenario. Table 1 depicts a comparative analysis of various underwater methods proposed by eminent researchers based on issues resolved and limitations.

2.1. Knowledge Gap

Various existing UWMANET protocols are studied and analyzed for making a ground for further enhancement and improvement. SO-AODV, E^2-SCRP, HAMA, and GA-CRAP are investigated. However, AODV performed better when on-demand nature was encountered. In AODV, protocol nodes are highly mobile, easily adaptable to new features, but on the other hand, it lacks security and optimality [22]. Many fact-finding previous work and attempts in these directions are elaborated in the above paragraphs. Here, two critical issues are identified (i) optimality through energy efficiency in data transmission, (ii) secure communication of messages/data. Both problems can be picked up to study over AODV (an on-demand based traditionally) protocol. While designing a protocol for UWMANET, an energy efficiency scheme and secure method can be applied. Energy can be achieved through residual energy, and security can be accomplished by using any block altered technique with public key generation technique. Various multipronged network metrics like PDR, Throughput, delay, scalability, etc., can be achieved in a novel, secure and energy-efficient method. Thus, a new safe and energy-efficient protocol named will fulfill these critical research gaps.

RESEARCH ARTICLE

Papers	Method Proposed	Tool Used	Issues Resolved			Limitations
			Energy Efficiency	Security	QoS Improvement	
Singh and Gupta [3]	• SO-AODV • Pigeons Swarm Optimization • Ciphertext Stealing Technique (CST) • qu-Vanstone Elliptic Curve Cryptography (qV-ECC)	NS-2	X	✓	✓	The proposed method is suitable for large scale network due to high power utilization.
Singh and Gupta [4]	• power-aware AODV protocol • Energy_Efficient_routeDiscovery() • Optimality through Minimum hop count	NS-2	✓	X	✓	The proposed method is suitable for sensitive networks due to security reasons.
Yadav and Kush [5]	• E^2-SCRP • 3D Under-Water acoustic MANET (UWMANET). • CST • Type two fuzzy-based multilayered techniques	NS-2	✓	✓	✓	System complexity
Yu et al. [6]	• lopsided cluster organization	MATLAB	X	✓	✓	The method is not suitable for long connections.
Ghoreyshi et al. [7]	• hop-constrained clustering method • underwater sensor organizations	NS-2	X	X	✓	The method is designed for underwater networks.
Cai et al. [8]	• versatile edge components	NS-2	X	X	X	Not suitable for long range communication. Not well suited for scalable
Zhu and Wei [9]	• exposed layers supported inconsistent groups • power-aware routing	NS-2	✓	X	✓	Hotspot issue, It isn't reasonable to relieve all grouping issues.
Khan and Dwivedi [10]	• ADAN-BC • nodes can make large holes	NS-2	X	✓	X	Less secure in dense network
Wang and Bang [11]	• the node tumbling method in undersea sensing organizations • for enormous scope 3D underwater	NS-2 & MATLAB	✓	X	X	Hub sinking calculation issue in large scale network.

RESEARCH ARTICLE

Khosravi and Rostami [12]	• fusion technique called SDV • water depth based sensing network	NS-2	X	X	✓	Scalability is a significant drawback in this technique.
Gomathi and Manickam [13]	• multilayered directing convention • joining technique is introduced	NS-2	✓	X	✓	Delay is high
Gomathi and Manickam [14]	• three-dimensional ZOR • under level water sensing network • Gauss Markov Model	NS-2 & MATALB	✓	X	✓	Consume more power while working with fixed nodes.
Zhao et al. in [16]	• ECPM (Elliptic Curve Point Multiplication)	NS-2	X	✓	✓	Diminishes the computational load.
Yan et al. [17]	• ultra-lightweight scheme (UAN) • undersea acoustic ad-hoc networks • 8-round slab cipher is proposed	NS-2	X	✓	✓	Unbalanced energy consumption in heavy network load.
Bisen and Sharma [18]	• AB-SEP (Agent Based-Secure Enhanced Performance) • Fuzzy-Based Secure Architecture (FBSA)	NS-2	X	✓	✓	FBSA model enhanced some complexity, communication overhead
Vamsi et al. [19]	• A secure short digital signature scheme	NS-2 & MATLAB	X	✓	✓	Energy efficiency issues.

Table 1 Comparative Analysis of Various UWMANET based Existing Methods

3. RESEARCH METHODOLOGY

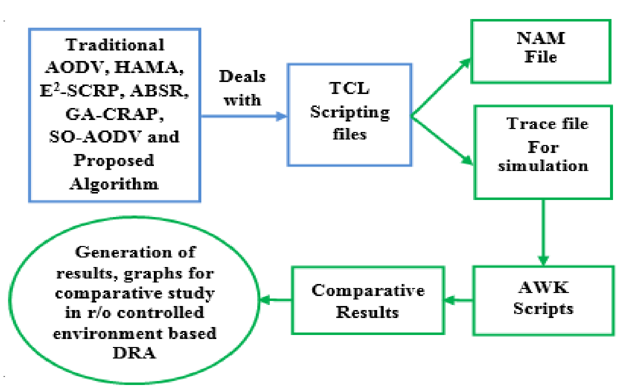


Figure 1 Research Methodology for Proposed E^2S-AODV Protocol

Figure 1 gives an idea about the methodology followed in the proposed E^2S-AODV protocol and how various metrics, i.e., security, energy efficiency. The results are analyzed using a network simulator (NS-2) [23]. A TCL script is created that will take care of traffic and wireless network conditions of mobile devices. TCL script will run on the network simulator. The simulation process of TCL will generate a "trace file" and the "NAMfile." Trace files will further develop an "AWK script" to create results and analyze the proposed protocol [24].

Figure 2 depicts the overall efforts and presents a state-of-art approach to how this article is designed and written. Firstly, current research trends are studied, and movements are captured in MANET-based DRAs then investigated in the related literature survey to identify the problem and need exploration. Research gaps are identified and formulate then using the problem identification phase. Next step is crucial where we designed the actual solution and proposed a new energy efficient secure protocol named E^2S-AODV (Energy Efficient Secure Ad-hoc On-demand Distance Vector) Routing Protocol. Proposed protocol is tested using a network simulator (NS2); figure 1 depicts this step in detailed. In last, proposed solution can be implemented in a controlled environment for any disaster response application (DRA).

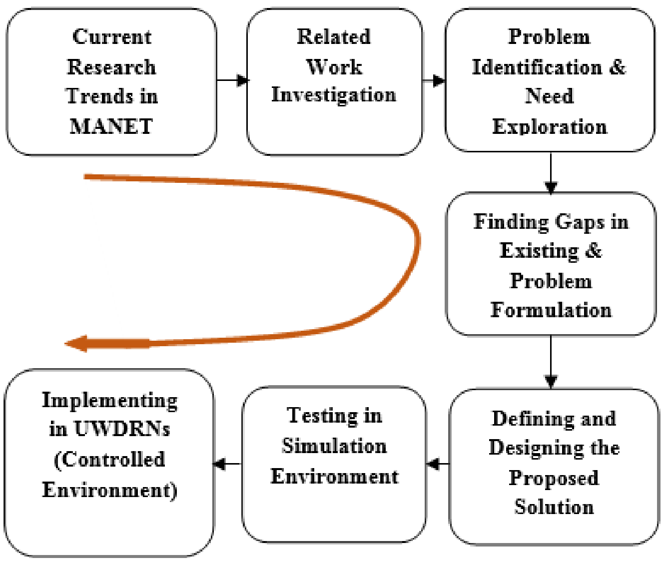


Figure 2 Research Passageway & Life Cycle of Complete Article

4. PROPOSED METHOD

There are numerous request based routing conventions. Among them, AODV is smarter to solve different MANET issues [25]. AODV has superior versatility in nature and energy mindfulness abilities as the contrast with other responsive protocols; therefore, researchers are consequently improving this protocol to develop it in various DRA based applications [26, 27]. Mobile ad-hoc networks can work in an environment where topology can be dynamically changed, and active nodes are open to access, communication can be done without centralized control, etc. [27, 28].

In the early study, many routing protocols are introduced for mobile ad-hoc networks, i.e., AODV, DSDV, DSR, HAMA, E^2-SCRP, ABSR, GA-CRAP, SO-AODV, etc. [29]. These protocols can work in various disaster response applications but lacking somewhere in a performance like SO-AODV in energy efficiency, AODV in security, ABSR, and GA-CRAP in a multipronged account, etc. [5, 29, 30]. Every on-demand based routing protocol (like AODV) needs two-step practice for communication: (i) route-finding and (ii) route maintenance. Route finding is significant and should be optimal. Optimality in route finding can be achieved through various ways like minimum node count in route, least energy consumption in the path, least resource utilization in route, etc. Ant Colony Optimization (ACO), Enhanced-ACO, Swarm based Intelligence, Power efficiency through fuzzy logic, and many more were attempted for optimality in route finding [31]. These efforts elaborated and proved that swarm-based routing and energy-efficient based techniques would provide optimality, reliability, and efficiency in MANETs. A further selection of a reliable path that can exclude critical energy drain nodes from selecting in communication link will increase reliability and optimality of the network. Communication within MANET is another very significant aspect and should be secured from a variety of security threats. AODV was initially introduced without considering security issues during message transmission [22]. Noteworthy efforts have been completed to secure the AODV protocol in an ad-hoc network, but there are still severe challenges to defeat [19].

Figure 3 depicts the authentication cum life cycle architecture of a secure and energy-efficient protocol named E^2S-AODV (Energy Efficient Secure Ad-hoc On-demand Distance Vector). The proposed method can improve the security and optimality issues of traditional AODV (see figure 3). E^2S-AODV selects the optimum path by calculating the residual energy technique, i.e., nodes having sufficient residual energy can participate in communication links, leading to optimality [32, 33]. Hello, messages broadcasted periodically to inform its neighbors that the connection to the host is active. LDW technique authenticates these hello messages. In the end, the original event message was encrypted with CST (Ciphertext Stealing Technique) and qu-Vanstone ECC based public-key cryptography. Further, sub-segment 4.1 presented pseudo-code and sub-section 4.2 elaborates in detail about the proposed effort. This attempt intends to urge energy-optimized and secure ad-hoc on-demand type routing protocol to work for multipronged factors in Disaster Response Applications (DRAs) based MANET.

4.1. Pseudo Code for Proposed Protocol

Notations Used: Destination Node (D_N), Source Node (S_N), Route Request (RREQ), Route Reply (RREP), Lightweight Digital Watermarking (LDW), Cipher-text Stealing Technique (CST), qu-Vanstone based Elliptical curve cryptography (qV-ECC), Residual Energy (R_E). Algorithm of proposed protocol is shown in Algorithm 1.

BEGIN

Step 1: INPUTS: Initial Energy (I_E) set to 100 joules,

Total numbers of participating nodes (N),

Threshold Energy (T_E) = 0.5* I_E.

Step 2: For i: = 1 to N do

RESEARCH ARTICLE

everyNodeBroadcastsHelloToNeighboursLDW();

False;

Step 3: For i: = 1 to N do

sendersBroadcastsRREQwithCST_qV-ECC ();

False;

Step 4: IF (R_E is greater than or equal to T_E)

Node selected for active route formation.

Else

energyEfficientRouteDiscovery ();

End IF;

Step 5: Neighbor node receives RREQ.

If the neighbor is D_N

Destination node performs

D_N _DecryptsMessage();

D_N _RREPtoSource();

Else

REPEAT

forwardRREQtoAdjacent();

UNTIL

D_N is reached.

End If;

Step 6: D_N reply with RREP, and S_N receives multiple RREP with a different sequence number.

Step 7: S_N accepts the optimal route with the latest sequence number and a higher R_E of the route.

END

Algorithm 1 Proposed Protocol

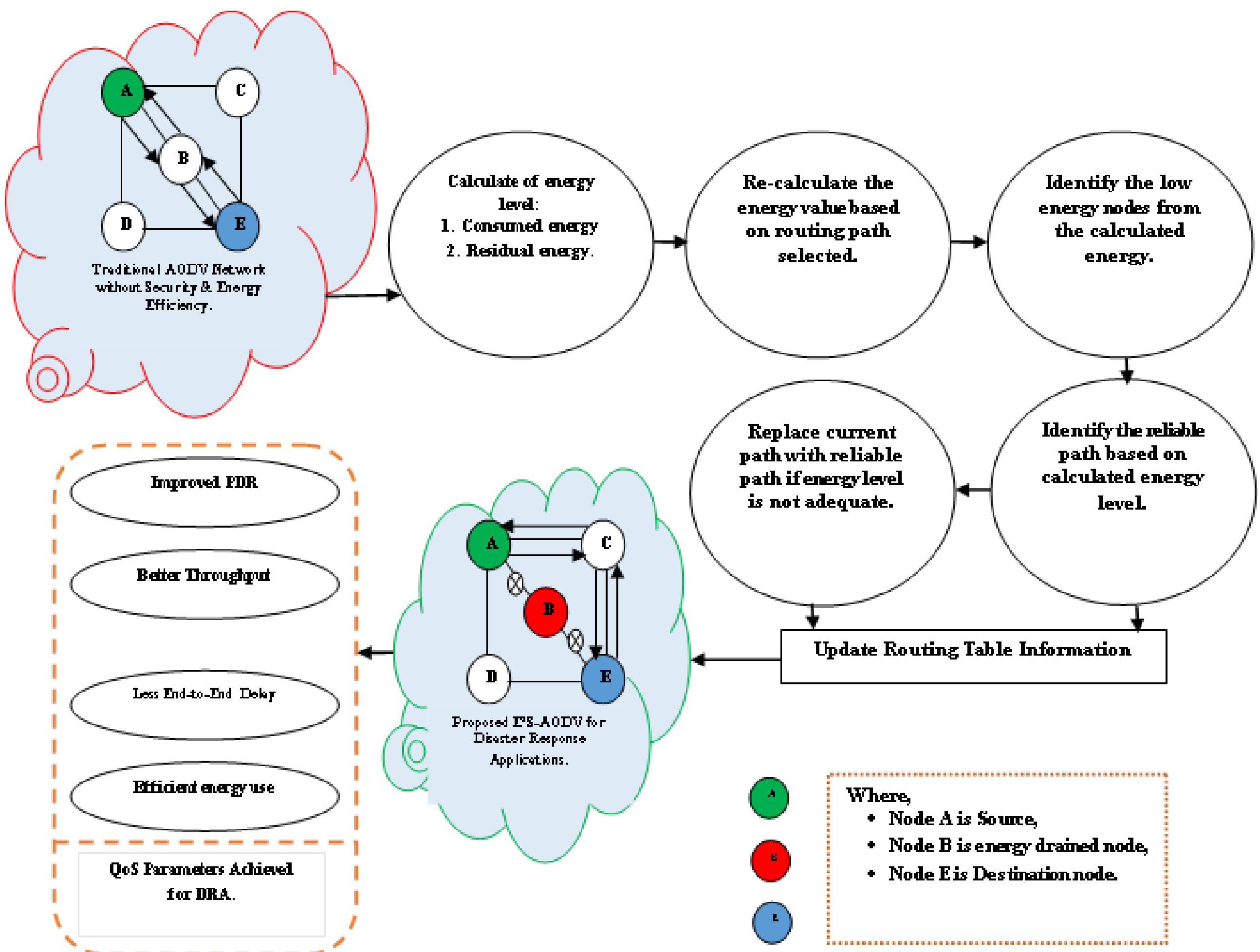


Figure 3 Authentication Diagram cum Life Cycle of proposed E^2S-AODV Routing Protocol

RESEARCH ARTICLE

4.2. Detailed Exploration of the Key Modules in E^2S-AODV

Various used functions and procedures are explained in this sub-section to understand the pseudo-code of E2S-AODV better. All these sub-modules (functions) can work collaboratively as a system and can be implemented in a disaster response based environment. Here, some main task-oriented functions are used and explained as follows:-

(i). everyNodeBroadcastsHelloToNeighboursLDW()

Through this function, every node broadcasts a "hello" message to establish local link connectivity to its adjacent nodes using "Lightweight Watermarking Technique (LDW)." Hello, messages broadcasted periodically to inform its neighbors that the connection to the host is active. LDW technique authenticates these hello messages.

(ii). sendersBroadcastsRREQwithCST_qV-ECC ()

Using this function, the source node broadcasts RREP (Route Request) messages with the help of Cipher-text Stealing Technique (CST) for security of messages and qu-Vanstone Elliptical Curve Cryptography (qV-ECC) based public-key cryptography for public key generation.

(iii). energyEfficientRouteDiscovery()

This function uses residual energy concept for route selection. This module can be explained in two sub-modules, i.e., residual energy analyzer and Drain rate finder.

(iv). Residual Energy Analyzer:

Residual energy of a node is known as remaining energy at each instant of time along with the total initial energy of nodes [33, 35].

$$\text{Residual Energy } (R_E) = \text{Initial Energy } (I_E) - \text{Consumed Energy } (C_E) \quad (1)$$

For any node "i" the Residual Energy (R_E) for a period of "α" at the time "t" can be defined as follows:-

$$R^i_E\,(t+\alpha) = I^i_E\,(t) - C^i_E\,(t+\alpha) \quad (2)$$

Where C^i_E (t+α) is energy consumption (during data broadcast) of node "i" for some time of α.

Further, we can obtain "energy consumption in data broadcast" ($E^i_{Broadcast}$) state of node "i" for broadcasting "n" packets can be calculated as follows:-

$$E^i_{Broadcast}\,(t+\alpha) = n * P^i_{Broadcast}\,(t+\alpha) \quad (3)$$

Where $P^i_{Broadcast}(t+\alpha)$ refers to energy consumption during a broadcast of "n" data packets.

Similarly, "energy consumption in receiving state" ($E^i_{Receive}$) of node "i" for receiving "m" packets can be calculated as follows:-

$$E^i_{Receive}\,(t+\alpha) = m * P^i_{Receive}\,(t+\alpha) \quad (4)$$

Where $P^i_{Receive}$ (t+α) refers to the power consumed by node "i" while receiving "m" packets at the receiver at a time interval α. Meanwhile, all nodes also consumed energy in intermediate operations, i.e., in managing, connecting, database updating, etc. This intermediate energy consumption can be denoted as $E^i_{Intermediate}(t+\alpha)$. In this way, total energy consumption "C^i_E (t+α)" can be computed as follows:-

$$C^i_E\,(t+\alpha) = E^i_{Broadcast}\,(t+\alpha) + E^i_{Receive}\,(t+\alpha) + E^i_{Intermediate}(t+\alpha) \quad (5)$$

In the end, the residual energy of node "i" for the time interval "α" can be updated as follows:-

$$R^i_E\,(t+\alpha) = I^i_E\,(t) - \{E^i_{Broadcast}\,(t+\alpha) + E^i_{Receive}\,(t+\alpha) + E^i_{Intermediate}\,(t+\alpha)\} \quad (6)$$

(v). Drain Rate Finder:

Drain rate (D_R) is the measurement of energy utilization by any node. Drain rate is computed for every "t" second's computing interval by taking the average of energy utilization and approximating the energy dissolute per second [35]. Exponential biased moving average means can be used to compute the concrete assessment of D_R. So, Drain rate for a node "i" can be considered by using the following equation:-

$$D^i_R = \lambda * D^i_{R\_old} + (1-\lambda)\, D^i_{R\_latest} \quad (7)$$

Where D_{R_old} symbolizes for earlier calculated value of drain rate and D_{R_latest} is the latest one. The latest drain rate is set as the uppermost priority by taking λ as 0.3. In this way, this will helps better to reflect the current energy consumption of the node.

The drain rate will give us a calculated approximate energy level (T_{Apx_En}) of the mobile device battery's remaining lifetime. This can be found by dividing the remaining battery power (R_E) of nodes by its drain rate (D_R). Further equation 8 will give us the estimated approximate energy time after which the route using this node as an intermediate node shall expire.

$$T_{Apx\_En} = R^i_E\,(t+\alpha) / D^i_R \quad (8)$$

A prefixed energy level named threshold energy (T_E) is set for maintaining a minimum energy level of the battery in all nodes, i.e.,

$$\text{Threshold Energy } (T_E) = 0.5 * I_E \quad (9)$$

Nodes fulfilling the following condition (equation 10) can only transmit the RREQ control messages to their adjacent nodes and participate in the link establishment or route discovery process.

$$T_{Apx\_En} >= T_E \quad (10)$$

RESEARCH ARTICLE

Where T_{Apx_En} is the approximate remaining energy of node and T_E is the threshold energy.

(vi). D_N_DecryptsMessage()

After receiving RREQ at the neighbor node, the node confirms itself as a destination node (D_N). Then this procedure encounters, and D_N decrypts received the message with a public key.

(vii). D_N_RREPtoSource():

Utilizing this function, destination node (D_N) replies to source node with RREP (Route Reply) packet and ensures that message has been successfully reached to the destination via established route.

(viii). forwardRREQtoAdjacent():

If the destination is not reached till now, then through this function, RREQ (route request) messages can be forwarded to adjacent nodes.

In the proposed solution, the modules mentioned above/functions are team up very well and role as a whole system that can be implemented in underwater disaster response application based UWMANET.

5. SYSTEM ARCHITECTURE

The underwater sensor organization's overall design is thoroughly inspected before applying and analyzing it for any particular disaster situation. A node's abilities are useful if the node can collaborate with the climate, other underwater nodes. Figure 4 depicts the overall architecture of an underwater disaster based network. At the bottom layer of the network, sensor nodes are installed with computational power and data storage capacity. They accumulate data through other sensors and correspond with different nodes through short-range acoustic connection. A floating base station is established to collect data from a sensor network. This base station will also forward this sensed information to the onshore surface station through satellite for various predictions.

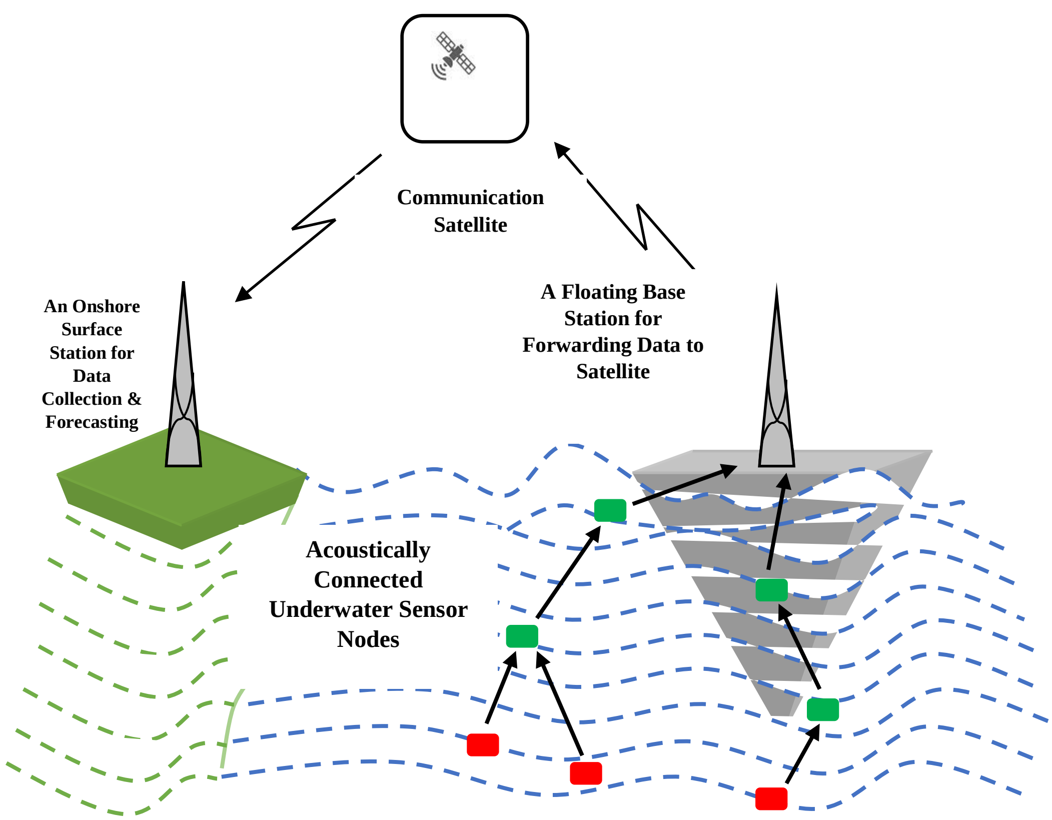


Figure 4 Logical System Architecture of Underwater Disaster Response Network (UDRN)

Primarily, the underwater sensors (UWSNs) and underwater acoustic networks (UWANETs) are set up in the ocean (figure 4). Sensor nodes can be operated with a rechargeable and limited replaceable battery. These sensing nodes are installed to collect ocean behavior and underwater changes. Stored and collected data is forwarded to the floating base station. The floating station is used to collect data from various sensing nodes, and further, it will deliver the sensed data to the onshore surface station through satellite. The floating station also gathers information about battery drains rate and maintains minimum power of used battery for communication within the network. In this way, an acoustically connected network achieved energy efficiency during underwater data transfer from the sensing node to a floating base station. After collecting data on the onshore surface station, this data can be processed for analyzing, forecasting to get real-time underwater behavior of the ocean to predict any disaster like situations.

Because of nodes' limited battery capacity, it is crucial to introduce a power-aware (energy efficient) MANET-based routing protocol. The required protocol should be aware of power consumption, and nodes should utilize battery power efficiently. A node should indicate if its power drain or power level will be less than a predefined threshold value. Power failure can affect the performance of network communication. E^2S-AODV is a novel energy-efficient routing protocol where power is utilized efficiently using two energy concepts: a drains rate analyzer and a residual energy finder.

The flow chart in figure 5 illustrates the overall route while examining the underwater atmosphere. The complete system is dedicated to underwater ocean behavior, and resources are busy in collecting real-time data. After analyzing the collected data at the onshore surface station, this system can predict or forecast the current ocean situation or help sense any disaster-like situation.

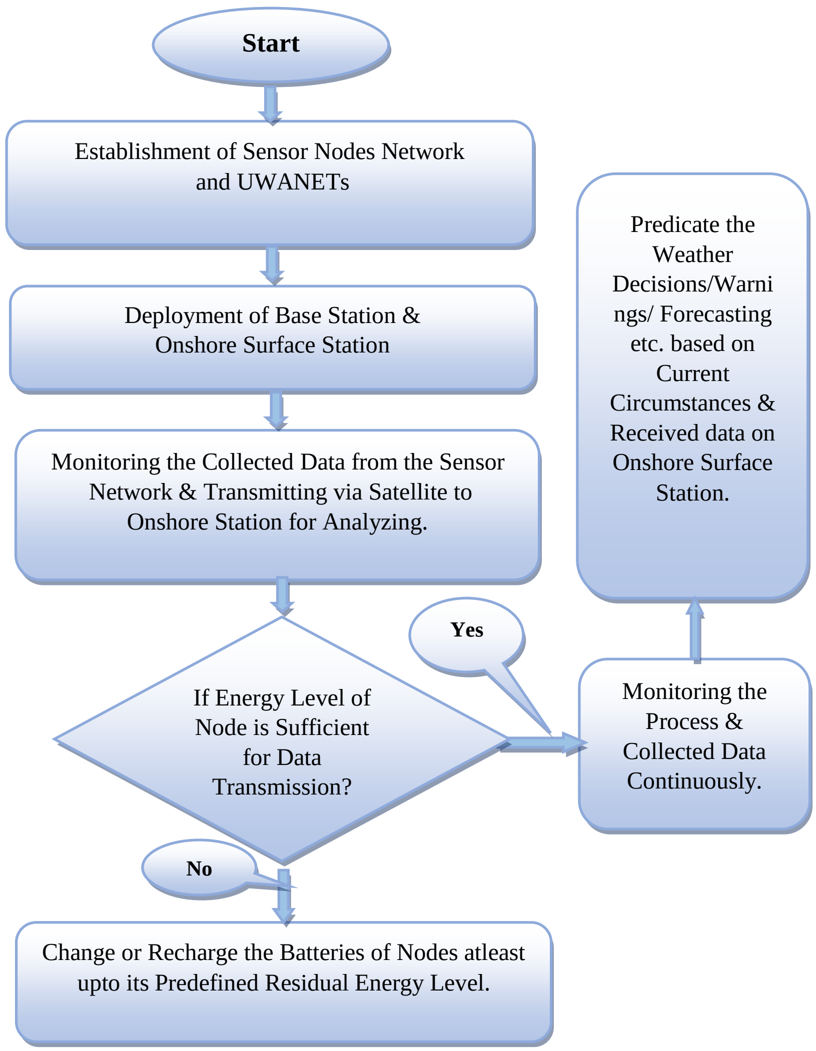


Figure 5 Flow Chart of Underwater Disaster Response Network (UWDRN)

6. SIMULATION ENVIRONMENT SETUP

The proposed E^2S-AODV is verified by organizing a few trials using a simulator NS-2 and achieved results are compared with past works. A famous simulator NS-2.34 version is used for result analysis. HAMA, SO-AODV, ABSR, and E2-SCRP are existing underwater disaster response-based UWMANET protocols compared with the proposed solution for authenticating results. All network parameter values and simulator organization are depicted in table 2.

Simulation	Parameter Values
Simulator	NS-2.34
Simulation Area	3000m*3000m
Simulation Round	200
Simulation Time	~1000 sec.
Sensing Range	300m
MAC Type	802.11
Initial Energy	100 joules
Channel	Wireless Channel
Antenna Type	Omni-directional
Radio Propagation	Two-Ray Ground
Interface Queue	DropTailPriQueue
Mobile Nodes	25, 50, 75, 100, 125, 150
Pause Time	0s
Speed	1.0, 2.0, 5.0, 7.0, 10.0 m/s
No. of Connections	6 (25 nodes); 13 (50 nodes); 20 (75 nodes); 26 (100 nodes); 33 (125 nodes); 41 (150 nodes)
Routing Protocols	HAMA, SO-AODV, ABSR, E2-SCRP,GA-CARP, E2S-AODV
Traffic Sources	TCP
Performance Metrics	PDR, end-to-end delay, Throughput

Table 2 Simulation Organization for Proposed E2S-AODV

7. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

This section will deliver result analysis and various QoS metric evaluation. Different QoS metrics like packet delivery ratio, end-to-end delay, and throughput, security, energy utilization are analyzed and further compared with some existing protocols. Examined QoS metrics will help in proving the achieved advancement of the proposed method over previous solutions.

7.1. Packet Delivery Ratio (PDR)

The packet delivery ratio can evaluate network performance. PDR can be achieved after dividing the total packet sent by source (TPss) by packet delivered at the receiver (TPrr). Any protocol's PDR must be high compared to other protocols for better data delivery ratio [4][36].

$$PDR\% = (TPss/TPrr) * 100 \quad (11)$$

Number of Nodes	ABSR	HAMA	EESCRP	SO-AODV	Proposed EES-AODV
20	68	71	74	76	79
40	72	73	77	79	82
60	73	75	80	82	84
80	75	78	82	84	87
100	77	79	85	87	90
120	79	81	87	88	92
140	83	86	88	90	93
160	84	88	90	91	95
180	86	89	93	95	96
200	87	91	95	96	98

Table 3 Packet Delivery Ratio (PDR) Vs. No. of Nodes

Table 3 shows the Packet Delivery Ratio (PDR) Vs. No. of Nodes. Figure 6 depicts the overall comparative graph regarding various existing protocols, i.e., ABSR, HAMA, SO-AODV, EESCRP, and proposed. The graph indicates that the proposed protocol performs better as compared to multiple current protocols. Proposed EESAODV reached up to 97% successful data transmission and achieved the highest rank among all. SO-AODV and EESCRP are approximately the same and reached an upper limit of 95% but not better than the proposed one. HAMA arrived only 91% of PDR. ABSR was worst among all, with an 87% packet delivery ratio. Therefore, the proposed protocols performed exceptionally well and achieved the highest PDR.

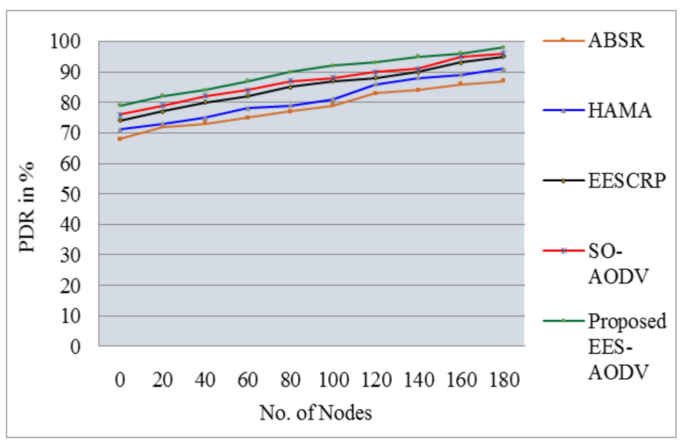


Figure 6 Packet Delivery Ratio (PDR) Vs. No. of Nodes

7.2. Security

AODV traditionally does not support data packet safety without knowing its adjacent link active status while information sharing in the network [22]. The proposed

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/207979 Volume 8, Issue 1, January – February (2021)

RESEARCH ARTICLE

protocol will eliminate this issue by offering a "lightweight digital watermarking" (LDW) method for broadcasted "hello" packets that will inform its neighbors that the connection to the host is active. Additional watermark bits are added to the data packets before using LDW on them. Added bits are directly related to data packet size. This technique is applied to the sink node for message authenticity. If any amendment happens while receiving messages at the sink node, then the sink node will abandon that data packet or message. Actual data transmission (event packets) is secured by "ciphertext stealing technique (CST)" with encryption qu-Vanstone ECC based public-key cryptography. CST modifies the last two blocks of the message. The encryption and decryption process is done with qu-Vanstone ECC-based public-key cryptography that only generates the key. In this way, the proposed E2S-AODV ensures security in data transmission.

7.3. Energy Utilization

Moveable devices, i.e., mobiles, laptops, palmtops, and PDAs are most likely to be used for data communication in MANETs [29]. These mobile (moveable) devices have one critical issue to be taken care of, i.e., limited battery power [30]. Any mobile node utilizes the battery's capacity in many tasks like in communication, for listening data requests, collision, channel sensing in idle state, higher bit rate, dynamic topology, path searching or inactive state, etc. [37, 38]. Energy utilization assessment is the main component of this research and performed by energyEfficientRouteDiscovery() module using two sub-modules, i.e. (i) Residual Energy Analyzer and, (ii) Drain Rate Finder. For efficient utilization of battery power, two essential attributes of energy named "residual energy" (RE) and "drain rate) (DR) are employed. RE is the leftover energy of any device before the drain, and DR is the drain rate measurement of the battery. RE and DR are both directly related to network performance. The proposed energy model efficiently tackles the power utilization issues using both these energy attributes and utilizes minimum energy while communicating in disaster response applications.

E^2S-AODV protocol selects the optimal path which has sufficient residual energy to complete the communication process. Thus, an established link will be reliable in terms of available power and energy used efficiently in data transmission. Critical nodes having power less than "threshold energy" cannot take part in a communication path. The proposed protocol is compared with several existing protocols, i.e., ABSR, HAMA, EESCRP, etc as shown in Table 4.

Figure 7 show that the proposed method consumes least energy during communication. When number of nodes reaches to200, then E2S-AODV improves energy utilization by 11% compared to the existing best available EESCRP. ABSR and HAMA are the worst in terms of energy consumption due to the heavy data load.

Number of Nodes	ABSR	HAMA	EESCRP	Proposed EES-AODV
20	0.6	0.5	0.2	0.1
40	0.9	0.7	0.3	0.2
60	1.5	1.0	0.6	0.4
80	1.6	1.2	0.8	0.5
100	1.9	1.5	0.9	0.7
120	2.2	1.7	1.0	0.8
140	2.6	2.0	1.2	0.9
160	2.9	2.4	1.3	1.1
180	3.1	2.5	1.6	1.3
200	3.3	2.8	1.8	1.6

Table 4 Energy Utilization (Joules) Vs. No. of Nodes

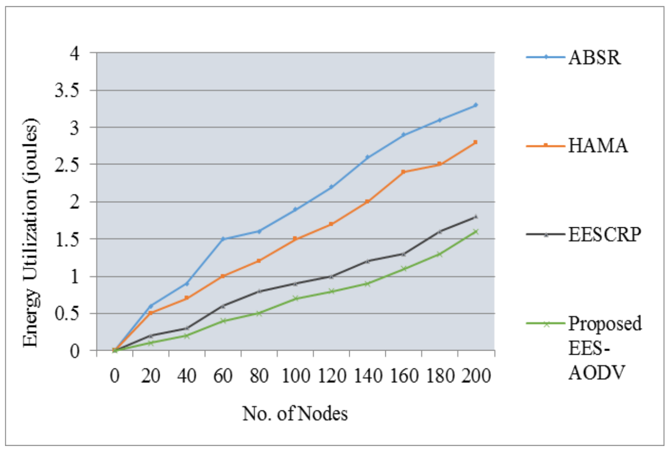


Figure 7 Energy Utilization (Joules) Vs. No. of Nodes

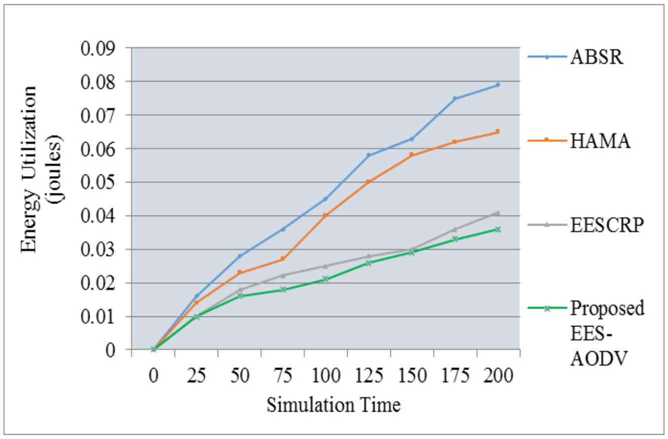
Figure 8 demonstrates that when the energy utilization is compared on behalf of simulation time again proposed solution gives better performance. When the total simulation time reaches 900(s), E2S-AODV improves energy utilization by 12% compared to the existing best available EESCRP. Again HAMA and ABSR are the worst performers among all. Table 5 shows the results obtained for the Energy Utilization in joules Vs. Simulation Time.

No. of Nodes	ABSR	HAMA	EESCRP	Proposed EES-AODV
25	0.016	0.014	0.01	0.01
50	0.028	0.023	0.018	0.016
75	0.036	0.027	0.0222	0.018
100	0.045	0.04	0.025	0.021
125	0.058	0.05	0.028	0.026

RESEARCH ARTICLE

150	0.063	0.058	0.03	0.029
175	0.075	0.062	0.036	0.033
200	0.079	0.065	0.041	0.036

Table 5 Energy Utilization in Joules Vs. Simulation Time



7.4. End-To-End Delay

End-to-end delay is a QoS metric that defined the interval between the data packet generation time and when the last bit arrives at the destination [39]. This metric is achieved by adding various delays, i.e., delay due to route discovery, processing delay (P_{Delay}), transmission delay (T_{Delay}), propagation delay ($D_{Propagation}$), etc. [40].

De2e (End-to-end delay) = $P_{Delay} + D_{Propagation} + T_{Delay}$ (12)

No. of Nodes	ABSR	HAMA	EESCRP	SO-AODV	Proposed EES-AODV
20	20	18	14	15	10
40	36	27	18	20	15
60	48	39	26	27	21
80	60	48	36	39	32
100	78	69	56	61	50
120	96	82	60	69	56
140	108	97	75	84	64
160	116	109	88	93	76
180	128	123	94	99	85
200	142	134	102	112	96

Table 6 End-To-End Delay (s) Vs. No. of Node

Figure 9 depicts the achievements in end-to-end delay metrics corresponding to several nodes. As usual, HAMA and ABSR are the worst performers and increase the end-to-end delay because of their multi-hop interactions. EESCRP and SO-AODV are almost similar when 100 nodes are deployed. After that, EESCRP performs some better end-to-end delay. The proposed method performs significantly well and shows an 8% reduction in energy consumption than the previously best available EESCRP. Table 6 shows the results obtained.

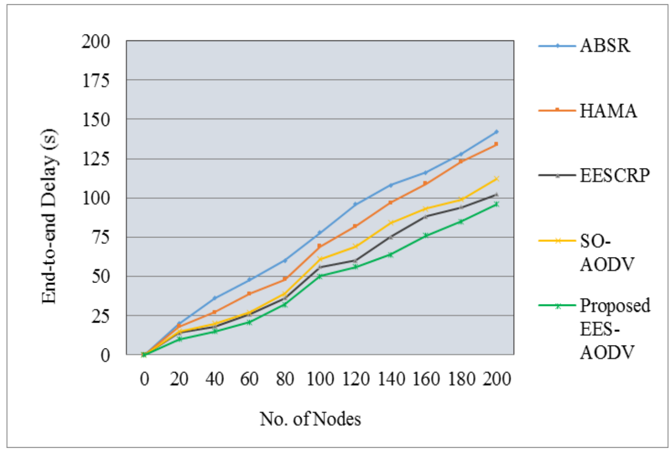


Figure 9 End-To-End Delay (s) Vs. No. of Node

7.5. Throughput

Throughput metric is a proportion of the total packets that arrives effectively to a recipient from the sender. The time it takes by the receiver to receive the last bit of the previous packet is called Throughput [41].

Throughput= $(No.\ of\ packet\ delivered * packet\ size\ in\ bits) \div (Total\ Simulation$ Duration) (13)

No. of Nodes	ABSR	HAMA	EESCRP	SO-AODV	Proposed EES-AODV
20	20	25	38	40	45
40	50	65	70	74	80
60	70	80	115	118	125
80	100	120	135	145	150
100	125	140	175	182	200
120	150	170	225	230	240
140	180	210	250	265	280
160	200	240	280	295	310
180	225	260	315	320	350
200	250	300	360	365	380

Table 7 Throughput vs. No. of Node

Figure 10 reveals that the proposed E^2S-AODV performs better Throughput at the receiver as compared to prior ones. Again HAMA and ABSR are comparatively the same and worst throughput performers. EESCRP and SO-AODV are showing almost the same Throughput but not better than the proposed method; further, when the number of nodes increases, Throughput also increases for all forms. E^2S-AODV demonstrates 4.5% and 5% enhancement in

RESEARCH ARTICLE

throughput corresponding to SO-AODV and EESCRP. The obtained results are shown in Table 7.

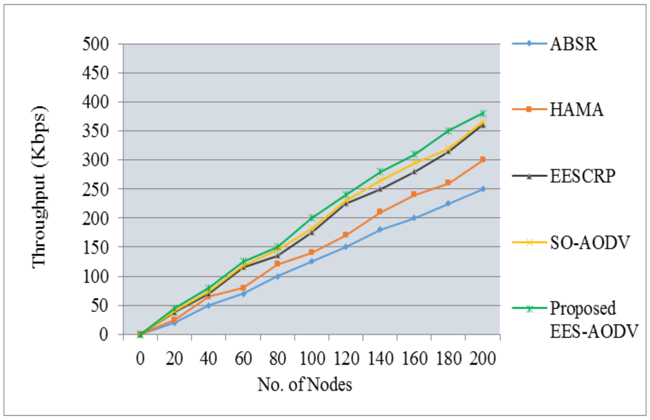


Figure 10 Throughput vs. No. of Node

8. CONCLUSION

In this article, a new on-demand based routing protocol named E^2S-AODV is presented for UWMANET based underwater disaster response network (UDRN). In the proposed method, a new security technique CST with qV-ECC based public-key cryptography is used, which authenticates and secures the messages at the receiver and improves security. An efficient energy model is used, which efficiently utilizes battery power. Residual energy "$R^i_E\ (t+\alpha)$" and drain rate "D^i_R" are two energy parameters that are used for energy computations in the network. Experiments are simulated for E^2S-AODV protocol and concluded that the proposed method works exceptionally well for small and large-sized networks with minimum computational efforts compared to existing SO-AODV, HAMA EESCRP, and ABSR. Various network metrics like PDR, Security, Energy utilization, Throughput, and End-to-end delay are analyzed for the proposed protocol. E^2S-AODV achieved 2% improvements in PDR, 5% enhancements in Throughput, 8% reductions in end-to-end delay, and 11% reductions in energy utilization compared to its near existing competent.

9. FUTURE SCOPE

The proposed protocol is available for an additional reduction in node/network power utilization, and any scheduling technique can be implemented for this. New energy-efficient and secure methods can be introduced so that innovative methodologies can be applied for betterment in the proposed protocol. The scope in E^2S-AODVis also open for enhancement on various disaster response applications based on disaster response network fields.

REFERENCES

[1] K. Singh, and A. K. Yadav. A Qualitative and Quantitative Analysis of Routing Protocols in MANET, International Journal of Advanced Research in Computer and Communication Engineering, 5(7), 2016.

[2] K. Singh, and R. Gupta. Comparative Assessment and Performance Analysis of Numerous Mobile Ad-Hoc Network Routing Protocols, Journal of Computational and Theoretical Nanoscience, Vol. 16, pp. 3906–3911, 2019.

[3] K. Singh, and R. Gupta. SO-AODV: A Secure and Optimized Ad-Hoc On-Demand Distance Vector Routing Protocol over AODV with Quality Metrics for Disaster Response Applications, To be Published in Journal of Information and Technology Reserch (JITR), 14(3), by IGI global publications , US, 2020.

[4] K. Singh, and R. Gupta. E^2S-AODV: An Energy Efficient Multipronged Reliable Strategy ensuring Secure and Scalable QoS over Disaster Response Applications, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No.4, July – August 2020.

[5] A. K. Yadav, and A. Kush. E^2-SCRP: An Energy Efficient Secure Cluster based Routing Protocol for 3D Underwater Acoustic MANET (UWMANET), International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, 8(11), 2019.

[6] Shanen Yu, Shuai Liu, Peng Jiang, "A High-Efficiency Uneven Cluster Deployment based on Network Layered for Event Coverage in UWSNs", Sensors Basel, MDPI, Vol. 16, Issue.2, PP. 2016.

[7] Seyed Mohammed Ghoreyshi, AlirezaShahrabi, TuleenBoutaleb, Mohsen Khalily, "Mobile Data Gathering with Hop-Constrained Clustering in Underwater Sensor Networks", IEEE Access, vol.7, pp. 21118-21132.

[8] S. Cai, Y. Zhu, T. Wang, G. Xu, A. Liu and X. Liu, "Data Collection in Underwater Sensor Networks based on Mobile Edge Computing," in *IEEE Access*, vol. 7, pp. 65357-65367, 2019, doi: 10.1109/ACCESS.2019.2918213.

[9] Fang Zhu, Junfang Wei, "An Energy Efficient Routing Protocol Based on Layers and Unequal Clusters in Underwater Wireless Sensor Networks". Journal of Sensors. 2018. 1-10.

[10] Guilista Khan, Rakesh Kumar Dwivedi, "Autonomous Deployment and Adjustment of Nodes in UWSN to Achieve Blanket Coverage (ADAN-BC)", International Journal of Information Technology, PP. 1-10, 2018.

[11] Zhongsi Wang, Bang Wang, "A Novel Node Sinking Algorithm for 3D Coverage and Connectivity in Underwater Sensor Networks", Ad Hoc Networks, Vol. 56, PP. 43-35, 2017.

[12] Mohammed Reza Khosravi, HmaidHabibRostami, "Efficient Routing for Dense UWSNs with High-Speed Mobile Nodes using Spherical Divisions", The Journal of Supercomputing, Vol. 74, Issue 2, PP. 696-716, 2018.

[13] Gomathi R.M, J Martin Leo Manickam, "Energy Efficient Shortest Path Routing Protocol for Underwater Acoustic Wireless Sensor Network", Wireless Personal Communications, Vol.98, Issue.4, PP. 1-14, 2017

[14] R.M. Gomathi, J. Martin Leo Manickam, "Energy Efficient Static Node Selection in Underwater Acoustic Wireless Sensor Network", Wireless Personal Communications, pp. 1-19.

[15] ChhaganLal, Roberto Petroccia, KonstantinosPelekanakis, Mauro Conti, Joao Alves, "Toward the Development of Secure Underwater Acoustic networks", IEEE Journal of Oceanic Engineering, IEEE Journal of Oceanic Engineering, Vol.12, issue.4, PP. 1075-1087, 2017.

[16] Yue Zhao, Bo Tian, Zhouguo Chen, Yiming Liu, Jianwei Ding, "An Energy-Efficient Key Agreement Mechanism for Underwater Sensor Networks", Lecture Notes in Electrical Engineering, Vol. 450, PP.1-13, 2017.

[17] Jing Yan, Xian Yang, XiaoyuanLuo, Calian Chen, "Energy Efficient Data Collection over AUV-assisted Underwater Acoustic Sensor Network", IEEE Systems Journal, PP. 1-12, 2018.

[18] Bisen, Dhananjay & Sharma, Sanjeev. (2017). An enhanced performance through agent-based secure approach for mobile ad hoc networks. International Journal of Electronics. 105. 1-21. 10.1080/00207217.2017.1355019.

[19] T. S. Vamsi, P. Kumar, and T. Sruthi. Performance Analysis of AODV Routing Protocol in MANET under Blackhole Attack, Journal of Engineering Research and Application, ISSN: 2248-9622, 9(5), pp. 58-63, 2019.

RESEARCH ARTICLE

[20] Sathiamoorthy, J., Ramakrishnan, B. A Reliable Data Transmission in EAACK MANETs Using Hybrid Three-Tier Competent Fuzzy Cluster Algorithm. Wireless Pers Commun 97, 5897–5916 (2017). https://doi.org/10.1007/s11277-017-4817-8
[21] Mohanakrishnan, U., Bhagavathiperumal, R. & Jayaraman, S. A Trusted Waterfall Framework Based Peer to Peer Protocol for Reliable and Energy Efficient Data Transmission in MANETs. Wireless Pers Commun 102, 95–124 (2018). https://doi.org/10.1007/s11277-018-5829-8.
[22] C. Perkins, E. B. Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing, Retrieved March 1, 2001.
[23] Andel, Todd & Yasinsac, Alec. (2006). On the credibility of MANET simulations. Computer. 39. 48 - 54. 10.1109/MC.2006.242.
[24] Arora, D., Millman, E. & Neville, S.W. Enabling richer statistical MANET simulations through cluster computing. Cluster Comput 16, 989–1003 (2013).
[25] Ochola, Elisha & Eloff, Mm & Van der Poll, John. (2012). Mobile ad-hoc network security challenges under AODV routing protocol. 113-122.
[26] Pandya, Morli. (2013). Review on security issues of AODV routing protocol for MANETs. IOSR Journal of Computer Engineering. 14. 127-134. 10.9790/0661-145127134.
[27] Alghfari, Fawaz & Saeed, Khalid. (2016). Energy Consumption Analysis of AODV and ABHMAODV Routing Protocols in MANET.
[28] Anjum, S.S., Noor, R.M. & Anisi, M.H. Review on MANET Based Communication for Search and Rescue Operations. Wireless Pers Commun 94, 31–52 (2017).
[29] Sara, Getsy & Subu, Neelavathy & Sridharan, D.. (2010). Evaluation and Comparison of Emerging Energy Efficient Routing Protocols in MANET. ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY. 1. 37-46. 10.21917/ijct.2010.0006.
[30] M. Barati, K. Atefi, F. Khosravi and Yashar Azab Daftari, "Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET," 2012 International Conference on Computer & Information Science (ICCIS), Kuala Lumpeu, 2012, pp. 636-642, doi: 10.1109/ICCISci.2012.6297107.
[31] Mostafa Abd-El-Barr, Bambang Sarif, "Swarm intelligence versus direct cover algorithms in synthesis of Multi-Valued Logic functions", Applied Computing and Informatics Available online 10 March 2020.
[32] N. Khanna and K. K. Naik, "Design and implementation of an energy efficient routing approach based on existing AODV protocol in Mobile Adhoc Networks for military," 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES), Sultanpur, 2016, pp. 216-222, doi: 10.1109/ICETEESES.2016.7581388.
[33] P. Paranavithana and A. Jayakody, "Compromising AODV for better performance: Improve energy efficiency in AODV," 2017 6th National Conference on Technology and Management (NCTM), Malabe, 2017, pp. 201-204, doi: 10.1109/NCTM.2017.7872854.
[34] Patel, Maitri & Patel, Manish. (2018). Energy Efficient Routing Using Residual Energy and Stability in Mobile Ad-Hoc Network. 857-861. 10.1109/ICIRCA.2018.8597298.
[35] Shivashankar, & Suresh, H.N. & Varaprasad, Golla & Jayanthi, Guruswamy. (2014). Designing Energy Routing Protocol With Power Consumption Optimization in MANET. Emerging Topics in Computing, IEEE Transactions on. 2. 192-197. 10.1109/TETC.2013.2287177.
[36] Sharma, Manmohan & Rashid, Mamoon. (2020). Security Attacks In MANET -A Comprehensive Study.
[37] Vu Khanh, Quy & Hung, Le. (2020). A Trade-off between Energy Efficiency and High-Performance in Routing for Mobile Ad hoc Networks. Journal of Communications. 10.12720/jcm.15.3.263-269.
[38] Anjum, Shaik & Md. Noor, Rafidah & Anisi, Hossein. (2015). Review on MANET Based Communication for Search and Rescue Operations. Wireless Personal Communications. 10.1007/s11277-015-3155-y.
[39] M. Zaki, Salim & Ngadi, Md & Razak, Shukor. (2009). A review of delay aware routing protocols in MANET. ISSR Journals, CS Letters. Vol. 1 (1). 1-12.
[40] Z. Chen, W. Zhou, S. Wu and L. Cheng, "An Adaptive on-Demand Multipath Routing Protocol With QoS Support for High-Speed MANET," in IEEE Access, vol. 8, pp. 44760-44773, 2020, doi: 10.1109/ACCESS.2020.2978582.
[41] Gutiérrez, Daniel & Askalani, M. & Toral, S.L. & Barrero, Federico & Asimakopoulou, Eleana & Bessis, Nik. (2015). A Survey on Multihop Ad Hoc Networks for Disaster Response Scenarios. International Journal of Distributed Sensor Networks. 2015. 10.1155/2015/647037.

Authors

Karan Singh is a research scholar in M.M. Institute of Computer Technology and Business Management, Maharishi Markandeshwar (Deemed to Be University), Mullana, Ambala, Haryana, India. His areas of interest are Ad-hoc Networks, MANET Security and Cryptography etc.

Dr. Rajeev Gupta is working as assistant professor in Dept. of Computer Sc. & Engineering, M.M. Engineering College,, Maharishi Markandeshwar (Deemed to Be University), Mullana, Ambala, Haryana, India. He has 15+ years of teaching, research and software development experience. His Research interest includes Image processing, Visual Sensor Network and Mobile Ad-hoc Network. He is an Associate Life Member of Computer Society of India (CSI), Member of International Association of Engineers (IAENG) and Middle East Association of Computer Science and Engineering (MEACSE).