ISSN 2229-5518

Improve the Performance of AODV-SOS and FORP-SOS Routing Protocols in MANET for Emergency Rescue Services Based on Obtained Signal Intensity

Khandaker Takdir Ahmed[1], Dr. Tarek Hasan Al Mahmud[2], Md. Jashim Uddin[3], Md. Mustakim Musully Pias[4*]

Abstract— Finding the specific paths between the source and destination nodes in MANET routing protocols is necessary. During a natural calamity, when our regular communication network is disrupted for the damage to the ground station, at that time, AODV-SOS and FORP-SOS routing protocols in MANET are expected as an alternative medium for communication. Such as, when a victim wants help at a time of calamity and contact cannot be established at that time, it is difficult for the victim to communicate with the rescue team if the IP address is not known. Our goal is to fix the issue. We have considered FORP-SOS and AODV-SOS, which constructed S-O-S packets without endpoint addresses in MANET routing protocol FORP and AODV, and figured out their connection strength. This paper aims to enhance the resilience of FORP-SOS and AODV-SOS routing protocols in MANET based on obtained signal intensity to remove S-O-S packets when the accepted signal intensity is lower than a predetermined threshold at each time node accepts an S-O-S packet. Finally, we test our enhanced technique on a network simulator and determine its performance through extensive simulations.

Index Terms— AODV, Disaster, Emergency Rescue, FORP, MANET, RREQ, SOS

1 Introduction

Wireless communication technology is advancing gradually and rapidly. Individuals desire the ability to access their network terminals (laptops, PDAs, etc.) at even a considerable distance [1]. Users have the option to go wherever they want with wireless connectivity. There are many distinct wireless networks, each with its technique of connecting the nodes. They are divided into fixed infrastructure and ad hoc wireless networks [2].

Due to the proliferation of mobile devices that rely on wireless networks, MANET technology is one of the most promising research domains. Subsequently, the unique characteristics of MANET technology provide significant prospects for wireless network improvement [3]. On the other hand, due to its link with severe obstacles, MANET has become one of the most lively and active study domains in communication and networks. For a good reason, MANETs have become a popular network type. It is a network that is easy to set up. Unlike conventional networks, they can be set up at any location. However, regardless of the appealing applications, MANET's capabilities pose many obstacles that must be thoroughly investigated [4].

- *Khandaker Takdir Ahmed is an Assistant Professor in Information & Communication Technology in Islamic University, Kushtia, Bangladesh. E-mail: takdir@ice.iu.ac.bd*
- *Dr. Tarek Hasan Al Mahmud is an Associate Professor in Information & Communication Technology in Islamic University, Kushtia, Bangladesh. E-mail: tarek@iu.ac.bd*
- *Md. Jashim Uddin is an Associate Professor in Information & Communication Technology in Islamic University, Kushtia, Bangladesh. E-mail: jashim@iu.ac.bd*
- *Md. Mustakim Musully Pias is currently pursuing B.Sc. degree program in Information & Communication Technology in Islamic University, Kushtia, Bangladesh. E-mail: pias@ieee.org*

MANET is an autonomous distribution network composed of only mobile terminals [5]. It is expected to be used as one of the communications means when the base station is no longer available in such a disaster. It is utilized to communicate when the base station is no longer available in such a disaster. Many MANET protocols have been proposed to date are designed and assume that the destination IP address is already familiar. However, when a victim seeks help via a MANET in an emergency or a disaster, the destination's IP address may not be aware. In such a case, broadcast messages to an unspecified number of terminals seem adequate, but excess-posted messages may make the limited wireless bandwidth flooded.

Unlike the usual wireless network, MANET does not have particular nodes such as access points, base stations, and routers. So, each MANET node has the functions of an access point and a router, i.e., detection of neighboring nodes, management of the routing table, and the operation of the client terminal, i.e., data transmission and reception. These functions are carried out based on a MANET protocol's routing protocol. Therefore, MANET's performance and property greatly depend on the MANET protocol.

MANET Protocols are classified roughly into two types; one is the proactive type, and the other is the reactive type [6]. In the reactive type protocols, control messages are sent only when a communication demand occurs, and routes are established on-demand [7, 8]. The former has a disadvantage because each node has a heavy load, while communication delays can be decreased. The latter is easier to have increased uncertainty than the former, but each node has less load because control messages are sent only when necessary. We design the proposed protocol based on both proactive and reactive type AODV-SOS and FORP-SOS protocols because it is expected that the securing of the power supply becomes difficult during the disaster [9].

MANET is a mobile node network with a dynamic architecture. There is no central control because of the network's dynamic nature. As a result, nodes communicate with one another via intermediate nodes. During the recent few years, we have observed so many earthquakes in various areas of our country and other countries. For example, in 2015, a magnitude 7.8 earthquake ravaged impoverished Nepal. In addition, Japan was affected by a 9.0 scale massive earthquake in 2011 [10, 11]. When large earthquakes strike, our regular communication can be disturbed, and it can be challenging to communicate in some regions due to physical damage, power outages, and base station congestion.

In this case, if we can ensure secure communication, it is easier for the rescue team to find out the victims, and they can get instantaneous help by using these protocols. MANET is among the probable platforms to really be adopted in these scenarios as a standby network connection. The primary objective of this project is to enhance the activity of the AODV-SOS and FORP-SOS routing protocols in MANETs by creating a technique for deleting "S-O-S Packets" when the quality of the desired signal falls below a certain level. Every node gets an "S-O-S Packets" at the same time. When MANET is engaged in the case of a catastrophe, however, it is based on the presumption that the intended Internet Protocol address is recognized. Still, it is hazardous since this Internet protocol possesses an emergency number.

In this paper, we introduce a suitable MANET protocol for such a case in which a route request can be sent without specifying a destination IP address. We presume that the victims have a source terminal unaware of the evacuation squad's Internet Protocol address. We extend the AODV-SOS protocol to implement an additional "S-O-S packet" packet to send messages without specifying a destination IP address. When the SOS packet arrives at the destination terminal of the rescue team, it enables communication between the victims and the rescue team, and the rescue team can derive information through it. So, it will be able to contribute to the rescue activities.

The main contribution of our study is:

We introduced AODV-SOS and FORP-SOS instead of the AODV and FORP routing protocol. Furthermore, if the obtained transmit power is less than a fixed value, we develop a methodology for discarding "S-O-S" transmissions. By utilizing this proposed solution, the amount of routing traffic delivered will be scaled down, and the PDR is predicted to improve the final result.

The remains of the work are structured as follows:

In Section 2, the Literature Review of this research work. In Section 3, give an overview of AODV and FORP. In Section 4, the Proposed Method for AODV-SOS and FORP-SOS. In Section 5, Results and Discussion. The Conclusion is shown in the Section 6 of this research work.

2 Literature Review

Shulong Peng et al. present an improved routing protocol, but their communication medium is ship-to-ship and shore-to-ship [12]. Therefore, we have considered a vastly populated network and sent data from a specific node to a target node.

Satoru Inazu et al. During a natural disaster, no mechanism for transferring data from the source node to the target node was offered; however, each node functions as a network router, a network host, and routing packets between other nodes, transmitting and receiving data [13]. To solve the issue, we proposed a method of processing SOS packet receiving.

Natarajan Meghanathan et al. Numerous routing protocols are employed. However, the FORP is emphasized in order to obtain the improved protocol known as M-FORP [14]. But there is no clear idea about whether these routing protocols are energy efficient or not. On the other hand, we used both proactive and reactive routing protocols.

E. Alotaibi and B. Mukherjee et al. Mobile devices can form a MANET by connecting dynamically across the wireless medium without the usage of a centralized structure using wireless technologies such as Bluetooth or the 802.11 standards. However, the environment was static, and no mobility model was applied [15].

Lundgren et al. evidence says that sometimes mismatch occurs between the actual connectivity status and the router due to unreliable implement action of hello message [16]. This mismatch is known as "gray communication zones." A hello message detects these zones, regardless of whether or not the neighbor is reachable. However, the actual data message cannot be transmitted between the router and its neighbors. To remove this drawback, one such routing protocol [17] called position-based routing protocol is introduced. These protocols indicate the presence and current location of the user.

Floriano De Rango et al. (2009): The authors of this research examined a study of the behavior of a number of energy-conscious routing metrics when enforced to the OLSR protocol and verified its efficacy in lowering energy usage and extending network duration time when used in conjunction with such a proactive strategy. When energy-conscious conditional MDR metrics are used to combine with the heuristic mechanism for EA-Willingness, the energy behavior of a mobile network improves significantly without compromising additional aspects of performance parameters [18].

Wardi et al. (2011): The authors of this work proposed the REOLSR2 OLSR technique, which is based on residual energy. The REOLSR2 selects MPR networks depending on their accessibility and degree, as well as the remaining energy of their 1-hop neighbors. The objective is to avoid picking MPR nodes with low remaining energy and to prevent concentrating usage of energy in a few nodes. REOLSR2 is a proposed system that reduces energy usage and increases throughput [19].

Chunkang Feng et al. (2012): The authors of this study compared the AODV, DSR, and OLSR routing protocols in terms of network duration time and end-to-end delay. The OLSR MPR selection method causes MPR nodes to consume a lot of energy, resulting in a short lifetime for the OLSR network. ENOLSR improves node energy usage efficiency and enhance the duration time of the network in the absence of an increase in energy usage by increasing the complexity of the MPR selection approach [20].

M. Zhang and P. H. J. Chong et al. Because routing is performed autonomously by nodes via intermediary nodes, MANETs have the ability to reduce infrastructural costs and improve fault tolerance; yet, no cost-effective routing protocol has been deployed [21].

3 Overview of AODV and FORP

3.1 AODV (Ad hoc On-Demand Distance Vector)

AODV is the reactive type MANET protocol. Figure 3.1 shows the route establishment process of the AODV. When a new destination requires a route, the root node broadcasts a route request packet to determine the endpoint route. A node that accepts the route request packet directly from the source node generates a (reverse) route to the root node and re-broadcasts the route request packet when it is not the endpoint [22]. By repeating this re-broadcasting, the route request packet is forwarded to the endpoint. When the endpoint node accepts the route request packet, it unicasts the route reply packet to the last node by using the (reverse) route. The node that accepts the route reply packet generates the (forward) route to the node that sent the route reply packet and unicasts the route reply packet by using the (reverse) route [23]. By continuing this process, the route is formed successfully when the route reply packet reaches the root node. Intermediate nodes (except the root and endpoint node) put the information about neighbor nodes to the "precursor list" when it unicasts the route reply packet. If the intermediate node already has the route information to the destination, there is a case that the node sends back the route reply packet. Note that the intermediate nodes do not re-broadcast the once received route request packet to prevent excess packet flooding [24].

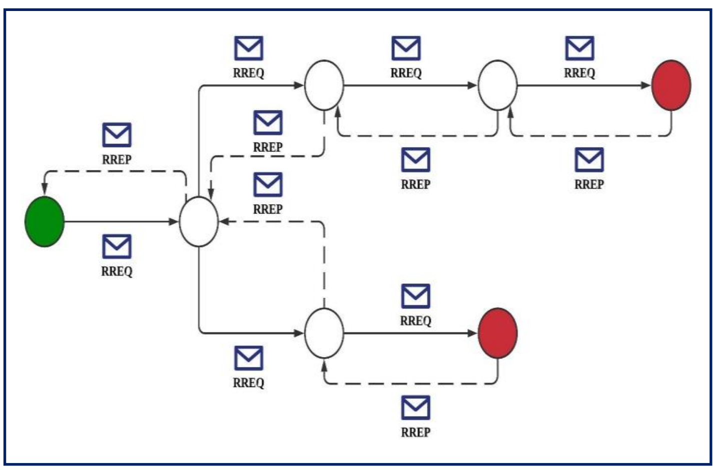

Figure 3.1 Route Establishment Process of the AODV

3.2 FORP (Flow-Oriented Routing Protocol)

Usually, RET and LET are employed to construct the path in the FORP routing protocol. The movement speed, moving direction, location information between two terminals, and communicable range are all used to calculate the LET. The minimal LET value of the links that comprise the route is RET. Figure 3.2 depicts the terminal's spatial connection for LET computation. Let (m_i, n_i) and a_i and θ_i denote the coordinates, speed, and mobility node's direction of i, and (m_j, n_j), a_j and θ_j Be the coordinates, speed, and mobility node's direction of j, and c be the communicative range. The LET between two terminals is calculated as follows:

$$LET = \frac{-(pq + rs) + \sqrt{(p^2 + r^2)c^2 - (ps - qr)^2}}{p^2 + r^2} \quad (1)$$

Where

- $p = a_i cos\theta_i - a_j cos\theta_j$ $\quad q = m_i - m_j$
- $r = a_i sin\theta_i - a_j sin\theta_j$ $\quad s = n_i - n_j$

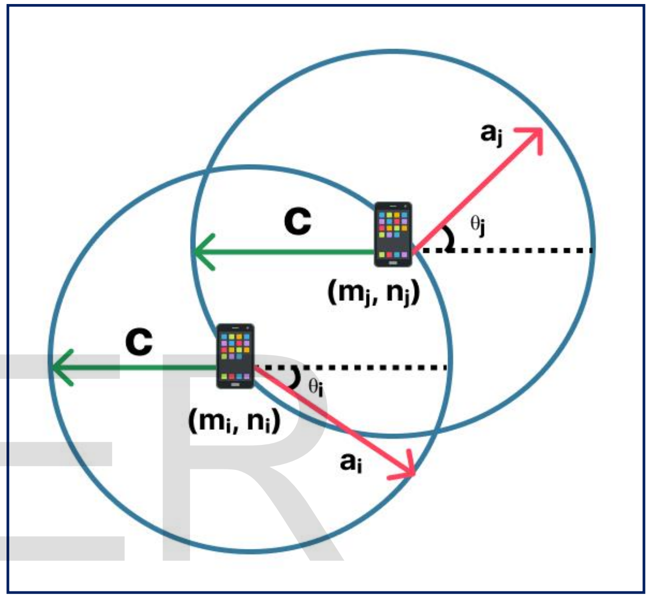

Figure 3.2 The relationship of a node to other nodes for LET calculations

The source node sends out a route request packet with the endpoint internet protocol address specified in the top. The nearby node that accepts the route request calculates the link expiration time based on the information in the route request for the neighboring node and compares it to the route expiration time in the route request. If it is less than route expiration time, it is necessary to update route expiration time information. Following that, verify the endpoint internet protocol address; if you don't own it, replicate the route request and re-broadcast [25]. When the targeted endpoint receives a route request, it waits a predetermined period of time, known as the Waiting Time (WT), before receiving more route requests. Compare the route expiration time values in every route request to the route and unicast route reply packet with the highest route expiration time if several route requests are received after the waiting period. When the route reply returns to the root node, the route is completed [13].

4 Proposed Method for AODV-SOS and FORP-SOS

We propose a unique MANET protocol that extends the

AODV protocol by implementing an additional packet named the "S-O-S packet" that enables the transmission of messages without identifying the destination IP address. Figure 4.1 shows the flow of the procedure at the terminal when the SOS packet is received in the proposed protocol. The source node initiates the SOS packet (terminal of the victim). It is broadcast like an RREQ packet; however, the distinction is that the destination address is not mentioned. When a node is not the destination node, it receives an S-O-S packet. If the rescue team's destination terminal receives an S-O-S packet, it unicasts the route reply packet using the reverse route, and the route is successfully created when the route reply packet reaches the root node. Then communication can begin. When a root node gets multiple route reply packets, it creates a multi-path, as illustrated in Figure 4.2.

By implementing this S-O-S packet, the victim can request assistance even if the rescue team's IP address is unknown.

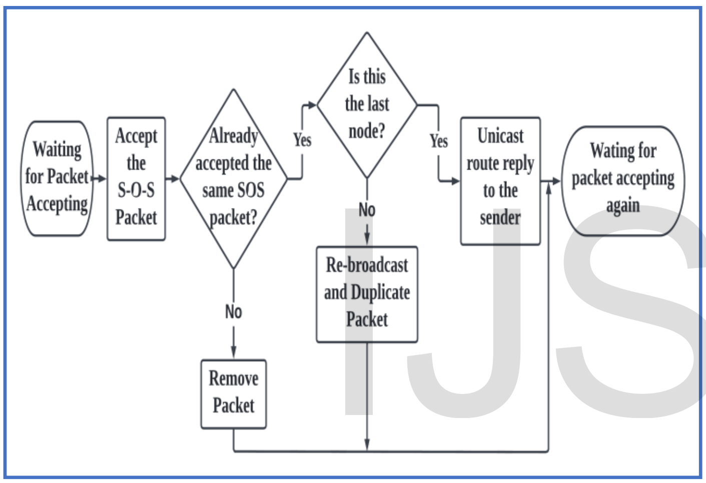

Figure 4.1 Flow Chart of Processing SOS packet Receiving

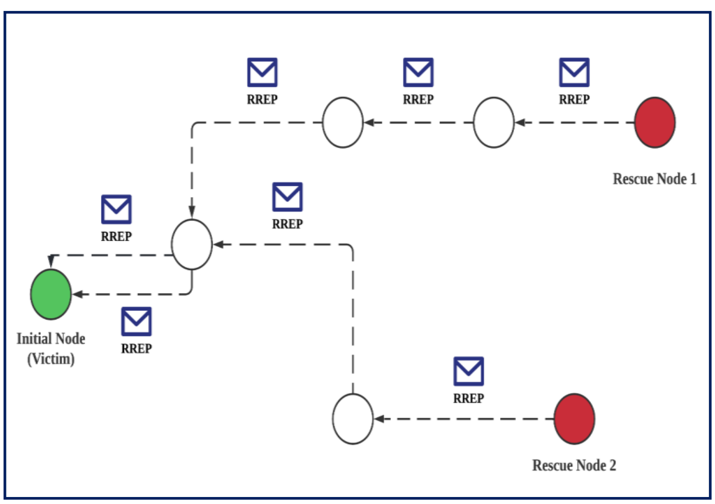

Figure 4.2 Establishment of multi-path

For route search in FORP-S-O-S, S-O-S packets without the endpoint internet protocol address in the top were employed. Furthermore, the RREP only returns a specific word as the recipient terminal, such as a rescue squad. Figure 4.3 depicts an example of FORP-SOS route construction. **I** denote the root node, F denotes endpoint node, and M1, M2, and M3 are the other nodes. The source node I sends out an SOS message with the destination IP address omitted from the header. M1 and M2 calculate LET and update RET after receiving the S-O-S packet, using the information I supplied in the S-O-S packet and their own location information. M1 and M2 are not endpoint terminals, hence SOS packets are duplicated and rebroadcast. M1 and M2 send S-O-S packets, which are accepted by F and M3, respectively. F accepts an S-O-S packet and compute link expiration time before comparing it to the S-O-S packet's RET. Because LET is greater than RET in the example presented in Figure 4.3, RET is not modified. Because F denotes the endpoint terminal, it does not duplicate the S-O-S packet and instead of waiting for subsequent S-O-S packets to arrive until the time WT has passed. M3 broadcasts SOS packets and performs the same operation as M1 and M2. Within the time WT, it is assumed that F accepts the S-O-S packet sent by M3. F compares the route expiration time in the S-O-S packets accepted from M1 and M3 and sends route reply to the node with the higher route expiration time. In the example of Figure 4.3**,** because route expiration time from M3 is longer than route expiration time from M1, route reply is unicast to M3, and then arrives at I via M2, completing the trip.

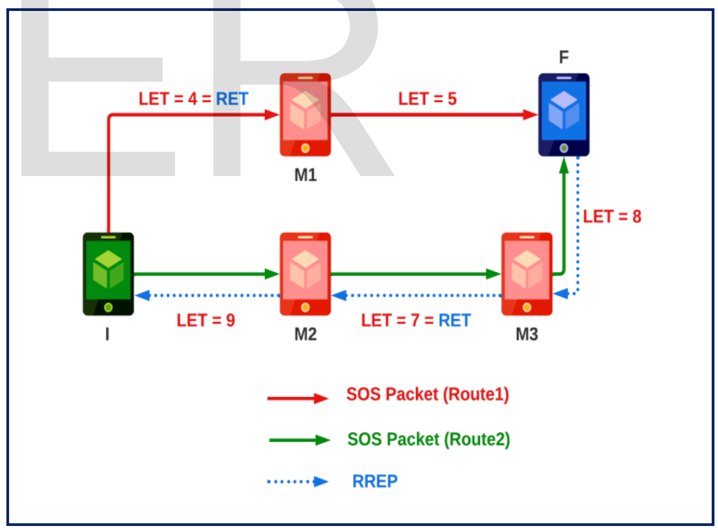

Figure 4.3 The positional relationship of each terminal

Figure 4.4 illustrates how the proposed method can be used to build a route. **I** is the root node, F is the endpoint node, and M1, M2, and M3 are the other nodes. The terminal accepting the S-O-S packet analyzes the received signal strength indicator (RSSI) value of the accepted S-O-S packet to a predetermined threshold value. The S-O-S packet is copied and rebroadcast if it exceeds the threshold. The S-O-S packet is deleted if the received signal strength indicator accepted packet's value is less than the threshold value.

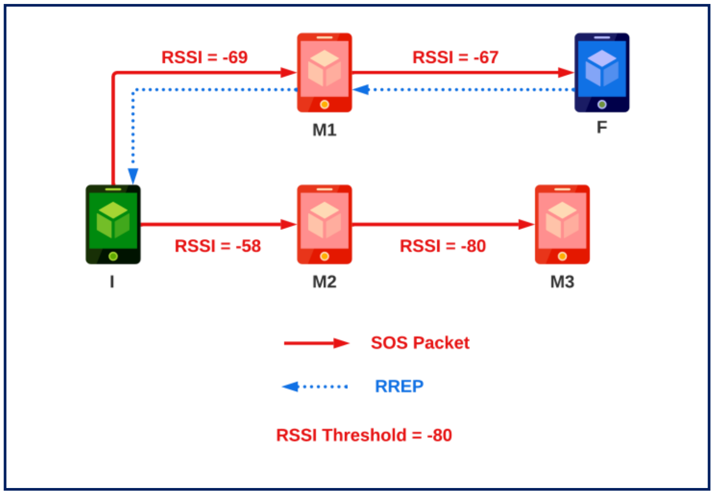

Figure 4.4 A route developed using the proposed method as an example

5 Results and Discussion

A network simulator is used to test the suggested technique. A Network scenario has been developed based on a premise whereby a sick person delivers a request for assistance. Fig 5.1 depicts the Network scenario that was constructed. 600[m] × 600[m] is the size of the simulation area. The emergency response node and other general nodes travel at a walking pace throughout the simulated environment, but the victim node remains stationary. All seed values have the exact

node placement. The node movement, on the other hand, is distinct. The victim node sends data packets at 1024 bits per second. Each terminal's antenna gain is 0[dB]. IEEE 802.11g is the wireless standard, as well as the supply of power, is 0.01 W.

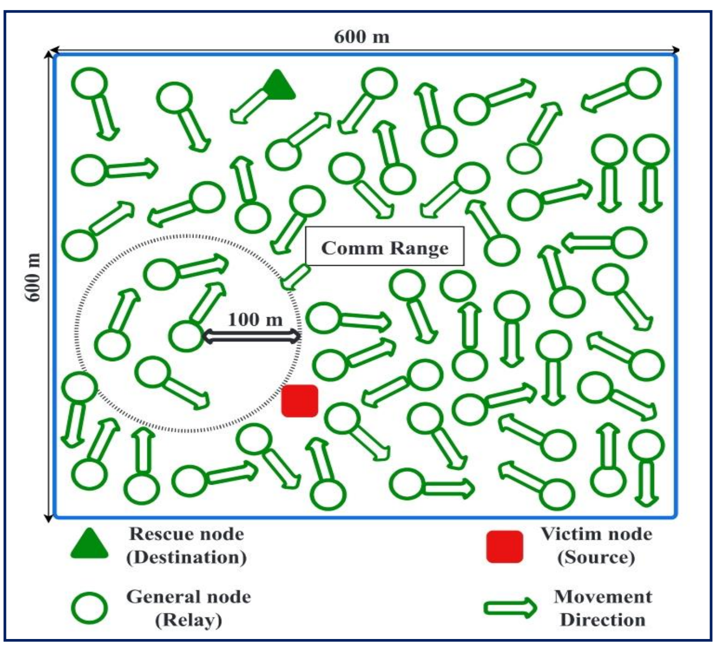

Figure 5.1 Simulation Model

As assessment indices, PDR and routing traffic volume are used. Packet delivery ratio is the degree of info that search party nodes get compared to data that victim nodes send to the rescue team nodes. The aggregate of the "S-O-S packet" and each Route Reply, Route Request, and Route Error packet shows the amount of routing packet that has been transmitted.

The test was run by switching the "s" value, which regulates the node's movement in six different ways while the number of neighbors is 600, the Duration is 0.30 sec, and the Received signal level is -60 dBm. Figures 5.2, 5.3, 5.4, and 5.5 indicate the quantity of network load sent and the PDR findings, respectively. As demonstrated in Figures 5.2, 5.3, 5.4, and 5.5, the throughput is improved, and the number of network loads delivered is reduced for changing seeds. Applying an RSSI base rate to the "S-O-S packet" will provide a harmonious path if no base rate is used. Table 1 represents the simulated value for Traffic and PDR for AODV and AODV-SOS. Respectively Table 2 represents the simulated value for Traffic and PDR for FORP and FORP-SOS.

Table – 5.1 Traffic and PDR for AODV and AODV-SOS

	Amount of Traffic		Packet Delivery Rate	
Seed No.	AODV	AODV-SOS	AODV	AODV-SOS
1	1723	1256	56	61
2	3218	2813	64	69
3	5918	4815	66	72
4	5732	7892	83	66
5	8927	7102	62	78

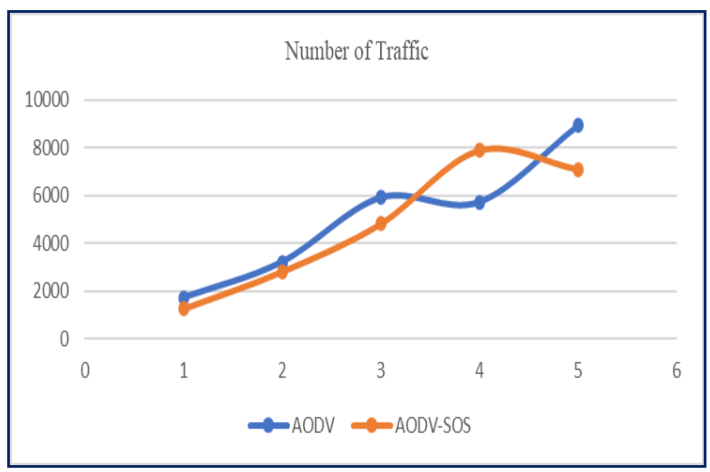

Figure 5.2 The number of traffic sent per seed value for AODV & AODV-SOS

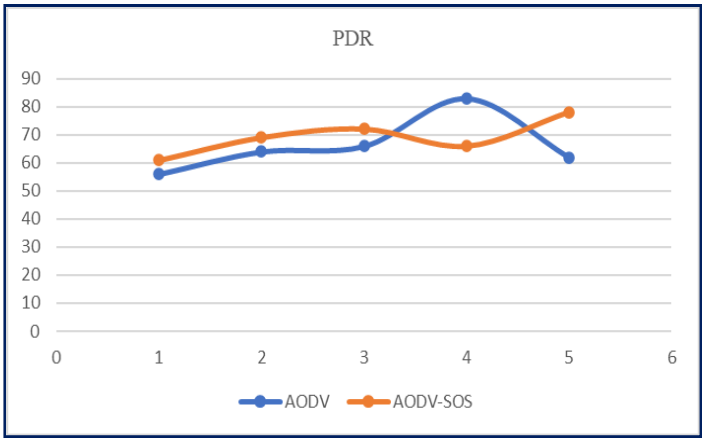

Figure 5.3 Packet delivery rate per seed value for AODV & AODV-SOS

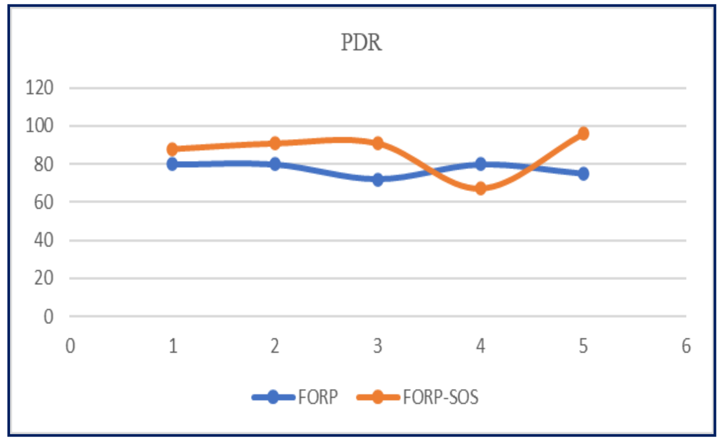

Figure 5.5 Packet delivery rate per seed value for FORP & FORP-SOS

Table – 5.2 Traffic and PDR for FORP and FORP-SOS

	Amount of Traffic		Packet Delivery Rate	
Seed No.	**FORP**	**FORP-SOS**	**FORP**	**FORP-SOS**
1	6113	4487	80	88
2	6122	3258	80	91
3	8756	3287	72	91
4	4852	7165	80	67
5	8286	2122	75	96

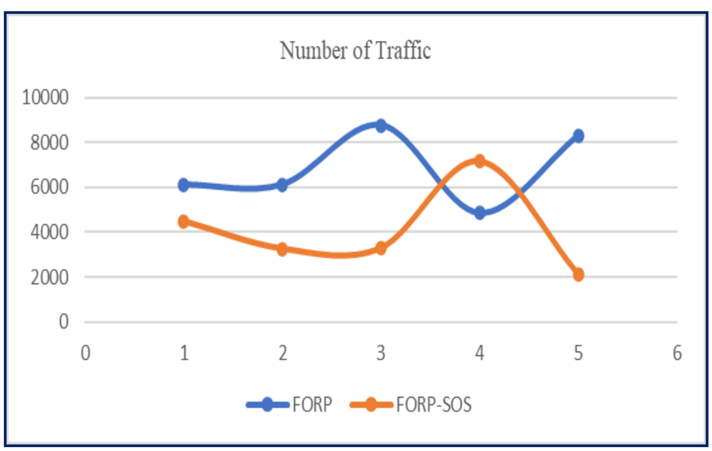

Figure 5.4 The number of traffic sent per seed value for FORP & FORP-SOS

From the above graph, we calculate that the number of network load transmitted for AODV & AODV-SOS has decreased by 8.22% (average value) as we as the PDR (per seed value) for AODV & AODV-SOS have increased by 3.71% (average value). On the othe other hand, the number of routing traffic sent (per seed value) for FORP & FORP-SOS has decreased by 32.51% (average value), and the PDR (per seed value) for FORP & FORP-SOS has increased by 8.91% (average value).

The number of routing traffic sent increases with seed value 4, yet the packet delivery rate decreases. Because the terminal can receive fewer S-O-S packets that are more significant than the "Received Signal Strength Indicator" base rate based on the end device specification, it is assumed that S-O-S packet repeat transmission will increase, and a path will be unable to create.

6 Conclusion

We have proposed a MANET protocol for an emergency situation of the disaster, etc. A route request can be sent without specifying a destination IP address by extending the AODV & FORP protocol to implement the SOS packet. The proposed protocol is implemented and evaluated in the network simulator Riverbed Modeler 18.0. To increase packet delivery rates and reduce routing traffic in AODV-SOS and FORP-SOS, we proposed a strategy for discarding packets when the strength of the receiving signal falls below a predetermined limit, and evaluating its effectiveness using six simulations. Finally, the number of routing traffic sent was decreased in some cases through packet removing operations based on the received signal strength indicator threshold, and the PDR was increased. It is essential to fixed applicable received signal strength indicator thresholds for future tasks and figure out effectiveness using more practical simulation parameters. Also, it is necessary to consider the general terminals' movements, effects of buildings, and obstacles to the radio wave. We will evaluate the proposed protocol's performance by using more precise models that include the above considerations. In addition, the function that some relay nodes temporarily hold messages of the victim nodes when a route establishment is difficult and send them to the rescue nodes after the communication route is established should be considered.

ACKNOWLEDGMENT

By the financial support of University Grants Commission of Bangladesh through Islamic University, Kushtia in the fiscal year of 2021-2022.

REFERENCES

[1] Al-Omari, S.A.K. and P. Sumari, An overview of mobile ad hoc networks for the existing protocols and applications. arXiv preprint arXiv:1003.3565, 2010.

[2] Maurya, P.K., et al., An overview of AODV routing protocol. International Journal of Modern Engineering Research (IJMER), 2012. **2**(3): p. 728-732.

[3] Goyal, P., V. Parmar, and R. Rishi, Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 2011. **11**(2011): p. 32-37.

[4] Shenbagapriya, R. and N. Kumar. A survey on proactive routing protocols in MANETs. in 2014 International Conference on Science Engineering and Management Research (ICSEMR). 2014. IEEE.

[5] Raza, N., et al., Mobile ad-hoc networks applications and its challenges. Communications and Network, 2016. **8**(3): p. 131-136.

[6] Bajaj, R., G. Bathla, and L. Pawar. Behavioral Analysis of Reactive Protocol of MANET. in 2021 2nd Global Conference for Advancement in Technology (GCAT). 2021. IEEE.

[7] Er-Rouidi, M., et al. An energy consumption evaluation of reactive and proactive routing protocols in mobile ad-hoc network. in 2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV). 2016. IEEE.

[8] Rahman, M.A., et al. A simulation based performance comparison of routing protocol on Mobile Ad-hoc Network (proactive, reactive and hybrid). in International Conference on Computer and Communication Engineering (ICCCE'10). 2010. IEEE.

[9] Kyogashima, T. and K. Gyoda, Proposal of a MANET Broadcast Protocol that Supports Disaster Relief Request. IEICE Proceedings Series, 2016. **61**(4809).

[10] April 2015 Nepal earthquake. Available from: https://en.wikipedia.org/wiki/April_2015_Nepal_earthquake.

[11] 2011 Tōhoku earthquake and tsunami. Available from: https://en.wikipedia.org/wiki/2011_T%C5%8Dhoku_earthquake_and_tsunami.

[12] Peng, S., et al. Implementation of an improved AODV routing protocol for maritime ad-hoc networks. in 2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). 2020. IEEE.

[13] Inazu, S., O. Oyakhiire, and K. Gyoda. Evaluation of MANET Protocol FORP-SOS for Disaster Relief Communication Considering Received Signal Strength. in 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC). 2019. IEEE.

[14] Meghanathan, N., T. DeMarcus, and E.S. Addison. Multicast extensions to the flow-oriented routing protocol and node velocity-based stable path routing protocol for mobile ad hoc networks. in 2009 International Conference on Ultra Modern Telecommunications & Workshops. 2009. IEEE.

[15] Alotaibi, E. and B. Mukherjee, A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 2012. **56**(2): p. 940-965.

[16] Lundgren, H., E. Nordströ, and C. Tschudin. Coping with communication gray zones in IEEE 802.11 b based ad hoc networks. in Proceedings of the 5th ACM international workshop on Wireless mobile multimedia. 2002.

[17] Royer, E.M. and C.-K. Toh, A review of current routing protocols for ad hoc mobile wireless networks. IEEE personal communications, 1999. **6**(2): p. 46-55.

[18] De Rango, F. and M. Fotino. Energy efficient OLSR performance evaluation under energy aware metrics. in 2009 International Symposium on Performance Evaluation of Computer & Telecommunication Systems. 2009. IEEE.

[19] Hirata, K., Y. Higami, and S.-y. Kobayashi. Residual energy-based OLSR in mobile ad hoc networks. in 2011 International Conference on Multimedia Technology. 2011. IEEE.

[20] Feng, C., Y. Zhou, and W. Du. The comparison and analysis of ad-hoc routing protocols based on energy and the modification of the OLSR. in Proceedings of 2012 2nd International Conference on Computer Science and Network Technology. 2012. IEEE.

[21] Zhang, M. and P.H. Chong. Performance comparison of flat and cluster-based hierarchical ad hoc routing with entity and group mobility. in 2009 IEEE Wireless Communications and Networking Conference. 2009. IEEE.

[22] Mueller, S., R.P. Tsang, and D. Ghosal. Multi-path routing in mobile ad hoc networks: Issues and challenges. in International workshop on modeling, analysis, and simulation of computer and telecommunication systems. 2003. Springer.

[23] Chang, Y.-C., Z.-S. Lin, and J.-L. Chen, Cluster based self-organization management protocols for wireless sensor networks. IEEE Transactions on Consumer Electronics, 2006. **52**(1): p. 75-80.

[24] Su, M.-Y., WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. computers & security, 2010. **29**(2): p. 208-224.

[25] Perkins, C.E. and E.M. Royer. Ad-hoc on-demand distance vector routing. in Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications. 1999. IEEE.

BIBLIOGRAPHY

Khandaker Takdir Ahmed received his M.Sc. and B.Sc. degree in 2011 and 2010 from the Dept. of Information & Communication Technology, Islamic University, Kushtia-7003, Bangladesh. He is currently working as an Assistant Professor in the Department of Information & Communication Technology at Islamic University, Kushtia-7003, Bangladesh.

Dr. Tarek Hasan AL Mahmud received the B.Sc. and M.Sc. degrees in Information and Communication Technology from Islamic University, Kushtia-7003, Bangladesh. He obtained his Ph.D. degree in signal and information processing from the University of Science and Technology of China, Hefei, China. He is currently working as an Associate Professor in the Department of Information and Communication Technology at Islamic University, Kushtia-7003, Bangladesh.

Md. Jashim Uddin received his M.Sc. and B.Sc. degrees in 2006 and 2005 from the Dept. of Information & Communication Technology, Islamic University, Kushtia-7003, Bangladesh. He is currently working as an Associate Professor in the Department of Information & Communication Technology at Islamic University, Kushtia-7003, Bangladesh.

Md. Mustakim Musully Pias is a B.Sc. student in the Department of Information and Communication Technology (ICT) at Islamic University, Kushtia-7003, Bangladesh. Besides, he is a research assistant of the Mobile Ad-hoc Networking lab in the Department of Information and Communication Technology at Islamic University, Kushtia-7003, Bangladesh.