# Fuzzy Logic-based Trusted and Power-aware Routing Protocol in Mobile Ad-hoc Networks

Hothefa Shaker[1], Baraa T. Sharef[2] and Zeyad T. Sharef[3]

[1]Modern College of Business & Science (MCBS), Khuwair | 133 Sultanate of Oman
[2] College of Information Technology, Ahlia University, Department of Information Technology, Manama, Kingdom of Bahrain.
[3]College of Engineering, University of Auckland, Auckland, New Zealand

***Abstract*:** Mobile ad-hoc networks (MANETs) have attracted much attention from researchers lately because MANETs are able to provide networks in areas with unavailable fixed network infrastructure. However, some mobile nodes may misbehave by dropping packets to conserve power usage because mobile ad-hoc networks nodes are usually battery operated. In this paper, a fuzzy logic-based routing protocol that considers the battery level of nodes, hop count, and trust among the nodes is proposed. The proposed routing protocol adaptively selects routes that use minimum hop count with the highest level of trust and a sufficient battery level to enhance the reliability of route selection while maintaining the percentage of successfully delivered packets. The result of the simulation shows that the proposed protocol can achieve a high ratio of successfully delivered packets, a lower average end-to-end delay, and a normalized routing load.

***Keywords*:** MANET, routing protocol, fuzzy Logic, trust, power aware**.**

## 1. Introduction

The mobile ad-hoc network (MANET) is a complex distributed system that is used in areas where a fixed network infrastructure is unavailable or wireless ad-hoc connection is needed [1]. MANET is a collection of two or more mobile devices equipped with wireless communications and networking capability. The devices in a MANET can communicate with another device that is immediately within and outside the radio range of the MANET device without relying on an access point or any centralized control. The mobile nodes in MANET can freely join or leave the network at any time, move randomly, and arbitrarily organize themselves. MANET, as a self-organized network, does not have a fixed infrastructure and can be easily set up at any time [2, 3]. MANET is also suitable for use in scenarios such as battlefields, emergency operations, conference halls, and disaster relief operations[4].

Certain intermediate nodes may run low on battery power and some malicious or selfish nodes may try compromise the routing protocol functionality to conserve power usage. Because of the characteristics of MANET such as dynamic topology, need for cooperation between nodes to forward packets, links that can be broken with high mobility, and limited battery power [5]. This effect on nodes may lead to unreliable routing and may make MANET vulnerable to security attacks. In this study, a Fuzzy Logic-based Trusted and Power-aware Routing (FL-TPR) protocol is proposed for the routing selection of MANET to provide more reliable delivery of data packets among the nodes in MANET.

This paper has five sections. The literature review is discussed in section II. The design of the FL-TPR protocol is explained in section III. The simulation and experimental results are presented in section IV. Finally, the conclusion of the paper and future work is given in section V.

## 2. Literature Review

Trust is a relationship among parties in networks. The procedure of trust establishment can improve the security, connectivity and quality of service in the network [6]. Several studies on MANET routing considered trust between the nodes. One popular study that used the trust mechanism is the Trust Ad Hoc On-demand Distance Vector (TAODV) routing protocol, which uses trust metrics to achieve better routing decisions and to penalize uncooperative nodes [7]. In TAODV, the routing messages and routing table of the Ad Hoc On-demand Distance Vector (AODV) [8] was extended to include trust information that can be updated by monitoring the behaviors of the other nodes in the network.

Another protocol is the Reliant Ad-hoc On-demand Distance Vector Routing (R-AODV) proposed in [9]. This work was implemented by modifying the trust mechanism known as the direct and recommendations trust model, which was then incorporated inside the AODV. This incorporation enables the AODV to not only find the shortest path but also find the shortest path that can be trusted. The security is enhanced by ensuring that the data do not go through malicious nodes that have been known to misbehave.

Numerous route selection protocols have been designed with the specific goal of achieving energy-efficient routing because battery power is a critical factor in determining the functionality of MANETs. In [10], Devi et al. attempted to balance the load among nodes, which has been shown to maximize network lifetime and enhancing the QoS and QoE for MANET .

The Localized Energy Aware Routing (LEAR) protocol is based on the Dynamic Source Routing (DSR) protocol but modifies the route discovery procedure for balanced energy consumption. Therefore, the destination node receives a route-request message only when all the intermediate nodes along a route have high battery levels, allowing nodes with low battery levels to conserve battery power [11].

The Conditional Max-Min Battery Capacity Routing (CMMBCR) protocol uses the concept of a threshold to maximize the lifetime of each node and to fairly use the battery like that in LEAR [12]. If one or more nodes in a route have a battery level lower than the threshold and if an alternative route where all the nodes have a battery level higher than the threshold exists, the alternative route is selected. If all possible routes have nodes with a lower battery capacity than the threshold, the max-min route is selected.

However, the threshold value of CMMBCR is fixed unlike in LEAR. This fixed value leads to a simpler design by selecting the shortest path if all nodes in all possible routes have adequate battery capacity (greater threshold). When the

battery capacity for some nodes is below a predefined threshold, the routes that go through these nodes are avoided. Therefore, the time until the first node failure is extended because of the exhaustion of the battery capacity.

Potentially promising approaches have recently been developed to establish a path between the source and the destination such as AODV and DSR. The limiting capacity of battery power and the misbehavior of nodes are the most critical issues because a downed node caused by the limited capacity of battery power and the lack of integrity of the packet delivery caused by misbehavior implies partitioning of the network and loss of information. In these studies, several approaches were implemented to individually solve those problems. For example, TAODV attempts to solve the misbehavior nodes by implementing trust mechanisms and monitoring the behaviors of other nodes in the network, and LEAR is an energy aware routing protocol.

In this study work, a new protocol is designed to incorporate the trust level and battery energy level of the nodes that can work together with the idea of finding the shortest path based on the number of hop counts. The incorporation of all these features should lead to a more robust routing protocol when faced prevalent security threats. This routing protocol also utilizes the fuzzy logic system in MANETs to select the optimum path between the source and the destination.

## 3. Fuzzy Logic-Based Trusted and Power-Aware Routing (FL-TPR) Protocol

The FL-TPR protocol is a reliable on-demand routing protocol. The protocol aims to find the route with the highest path reliability level ($R$) based on fuzzy logic inputs such as trust path level ($t_p$), battery energy path level ($e_p$), and the number of hop count ($n$). The relationship between $R$ and the fuzzy logic inputs ($t_p$, $e_p$, and $n$) is presented as

$$R \propto t_p * e_p * \frac{1}{n} \qquad (1)$$

It means that reliability level $R$ is in direct proportion to $t_p$ and $e_p$, and in inverse proportion to $n$. The $R$ value is updated by the fuzzy logic system. When $t_p$ and $e_p$ are low, the value of $R$ should be low. Otherwise, the value of $R$ should be high.

The input fuzzy variable of $n$ has three fuzzy sets: few, normal, and many. The membership functions of $n$ are illustrated in Figure 1.

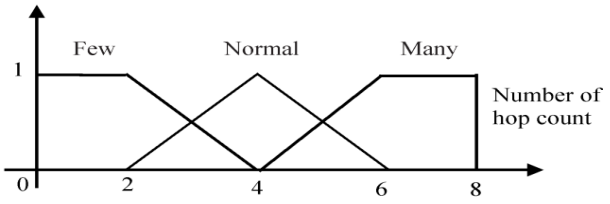


**Figure 1.** Membership functions of fuzzy input variable n

The input fuzzy variable $e$ has three fuzzy sets: low, medium, and high. The membership functions of $e_p$ are shown in Figure 2.

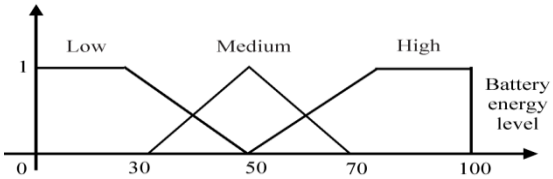


**Figure 2.** Membership functions of fuzzy input variable $e_p$

The input fuzzy variable $t_p$ has three fuzzy sets: low, medium and high. The membership functions of $t_p$ are shown in Figure 3.

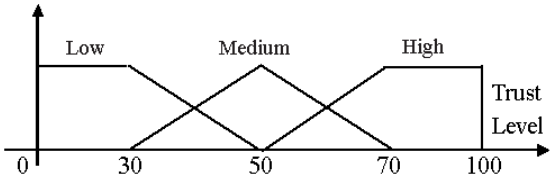


**Figure 3.** Membership functions of fuzzy input variable $t_p$

The output fuzzy variable of the $R$ has five fuzzy sets: bad, poor, moderate, good and excellent. The membership functions of $R$ are shown in Figure 4.

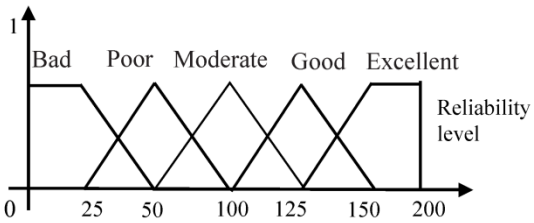


**Figure 4.** Membership functions of fuzzy output variable $R$

Modifying the membership functions values would notably change the sensitivity of the output of the fuzzy logic system based on the inputs. Increasing the number of the fuzzy sets of the variables provides better sensitivity control and increases the computational complexity of the protocol. Table 1 shows the fuzzy rules used in the FL-TPR protocol.

**Table 1.** Fuzzy logic rules

| Input | | | Output |
|---|---|---|---|
| $t_p$ | $e_p$ | $N$ | $R$ |
| Low | Low | Few | Poor |
| Low | Low | Normal | Bad |
| Low | Low | Many | Bad |
| Low | High | Few | Moderate |
| Low | High | Normal | Poor |
| Low | High | Many | Poor |
| Low | Medium | Few | Good |
| Low | Medium | Normal | Poor |
| Low | Medium | Many | Bad |
| Medium | Low | Few | Poor |
| Medium | Low | Normal | Poor |
| Medium | Low | Many | Poor |
| Medium | High | Few | Good |
| Medium | High | Normal | Moderate |
| Medium | High | Many | Poor |
| Medium | Medium | Few | Moderate |
| Medium | Medium | Normal | Poor |
| Medium | Medium | Many | Poor |
| High | Low | Few | Moderate |
| High | Low | Normal | Moderate |
| High | Low | Many | Poor |
| High | High | Few | Excellent |
| High | High | Normal | Good |
| High | High | Many | Good |
| High | Medium | Few | Good |
| High | Medium | Normal | Moderate |
| High | Medium | Many | Poor |

In the FL-TPR protocol, the path to be selected is the path with the highest $R$. The basic idea of FL-TPR protocol is that a number of possible paths exists between source node $s$ destination node $d$ when data is sent ($P_1$, $P_2$,……, $P_n$), where $A$ is the total number of possible paths from source $s$ to destination $d$. A number of intermediate nodes ($Q_1$,$Q_2$, ….. ,

$Q_m$) also exist, where $m$ is the total number of possible intermediate nodes to forward packets from source $s$ to destination $d$. Given that the current reliability level $R$ of the $j$th node in the $i$th path is $R_{ij}$, the path reliability level ($R$) of the $i$th path is

$$R_i = \min R_{ij}, j \in (1, \dots, m) \quad (2)$$

Therefore, the selection of the best path can be obtained by:

$$R_{Bp} = max_{i \in A} R_i \quad (3)$$

where $A$ is the set containing all possible paths $A = \{P_1, P_2, \dots\dots, P_n\}$ and $R_{Bp}$ is the best reliability level path.

### 3.1 Trust model representation

In this study, the trust values are the most important input in the fuzzy logics system because trust in MANET can be defined as the level of belief based on the behavior of nodes (or entities, agents, and others) depending on the trust value. The trust model used in this paper was proposed by Huang et al. in [13], which is called the Dynamic Mutual Trust-based Routing protocol (DMTR). The DMTR ensures the security of the entire network by utilizing the idea of the Trust Network Connect (TNC) and improves the security of the selected path.

**Definition 1 (Trust):**

*TS (u)* represents the trust score of node $u$ during the periodical time $t$. The range of *TS(u)* is given as $\{0 \leq TS(u)\ 0 \leq 100\}$, where 0 denotes that the node is untrustworthy and 100 denotes that the node is fully trustworthy.

**Definition 2 (Direct Trust):**

If the transmission between node $A$ and node $u$ is $m$ times during the periodical time $t$, the degree of acceptance of the $i$th time is $S(u, i)$, $S(u, i) \in [0, 1]$. The value 1 denotes that node $u$ absolutely satisfies node $A$ and vice versa. $TF(u, i)$ is assumes as the weight of the $i$th transmission.
The direct trust of node $u$ is defined as

$$Direct_{Trust}(u) = \frac{\sum_{i=1}^{m} S(u,i) * TF(u,i)}{\sum_{i=1}^{m} TF(u,i)} \quad (4)$$

**Definition 3 (indirect Trust):**

The indirect trust of node $u$ is measured by the recommendations of other nodes and is defined as

$$INDirect_{Trust}(u) = \frac{\sum_{i=1}^{m} Tu(i) * Direct_{Trust}(i)}{\sum_{i=1}^{m} Direct_{Trust}(i)} \quad (5)$$

where $Tu(i)$ is the direct trust of node $u$ relative to node $i$, and $Direct_{Trust}(i)$ is the direct trust of node $i$.

$TS(u)$,which is the trust score of node $u$ during the periodical time $t$ is calculated as follows:

$$TS(u) = \alpha * Direct_{Trust}(u) + \beta * INDirect_{Trust}(u) + \gamma * T_l(u) \quad (6)$$

where $\alpha$, $\beta$, and $\gamma$ are the weights of the direct trust, indirect trust, and trust score, respectively.

Therefore, the trust value of the $i$th path ($t_{p\ i}$) is defined as follows.

**Definition 4 (Path Trust):**

The trust value of the $i$th path ($t_{pi}$) is

$$t_{pi} = \Delta - \frac{\Delta - T_{min}}{T_{min} - \omega} \quad (7)$$

where $\Delta$ is the average trust score of the nodes in the path. $T_{min}$ is the minimal trust value in the path. $\omega$ is the boundary value between distrust and trust.

### 3.2 Route Establishment

The FL-TPR selects the *BestPath* (*Bp*) during the route discovery cycle based on the $n$ of the path and the $t_p$ and $e_p$ in the MANET nodes along the path. Each routing table entry contains the list of information as shown in Figure 5.

| Routing Table Entries | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $t_p$ | *InT* | *DT* | *DA* | *DN* | *n* | *NH* | $e_p$ | *R* |
| : | : | : | : | : | : | : | : | : |
| : | : | : | : | : | : | : | : | : |
| : | : | : | : | : | : | : | : | : |

**Figure 5.** Routing table entries

where:

| | |
|---|---|
| $t_p$ | : Trust path level |
| *InT* | : Indirect trust |
| *DT* | :Direct trust |
| *DA* | : Destination IP address |
| *DN* | : Destination sequence number |
| *n* | : number of hop count to destination |
| *NH* | : Next hop |
| $e_p$ | : battery energy path level |
| *R* | : Reliability level |

The process of route establishment is as follows:

(1) ***Route Request (RREQ) at the source node***: The route request (RREQ) message contains the destination IP address, destination sequence number, path reliability level $R$, hop count, battery energy level, direct trust, and indirect trust. The format of the RREQ message is shown in Figure 6.

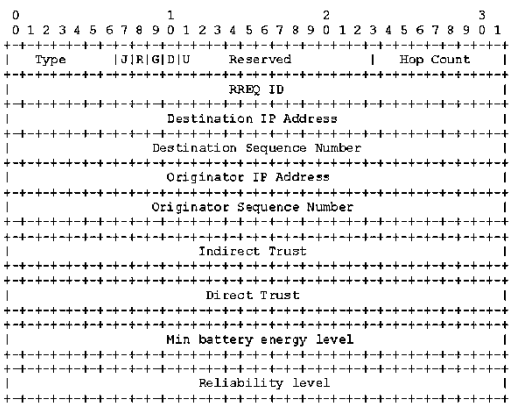


**Figure 6.** Format of RREQ message

When source node $s$ wants to send a message to destination node $d$, source node $s$ first checks the routing table if a valid route to the destination exists. If not, source node $s$ sends the RREQ message and initiates a route discovery process to reach the destination. Source node $s$ broadcasts the RREQ message to its neighbors. When the neighboring node receives the packet, this node broadcasts the packet to the other nodes after adding its $T$ to the RREQ message if an

existing route to that destination is not available. The RREQ message broadcast is shown in Figure 7.

(2) ***Route Request (*RREQ*) at the intermediate node***: When an intermediate node receives the RREQ message from its neighbor, this node first calculates the trust score *TS* for the original node from Eqs. 4, 5 and 6, adds its trust value to the packet, and increases the hop count value in the RREQ message by one. The originator sequence number contained in the RREQ message must be compared with the corresponding destination sequence number in the routing table. If the originator sequence number of the RREQ message is not less than the existing value, the intermediate node compares the *R* contained in the RREQ message to its own *R*. If the reliability level *R* of the node is lower than the one in the RREQ message, the reliability level in the RREQ message is updated.

If the intermediate node is the destination, the intermediate node must immediately update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ message before this node creates a route reply (RREP) message in response to the RREQ message. If the originator sequence number contained in the RREQ message of the packet is greater than the existing value in its routing table, the relay node creates a new entry with the sequence number of the RREQ message. If the originator sequence number contained in the RREQ message is equal to the existing value in its routing table, the reliability level of the RREQ message must be compared with the corresponding reliability level in the routing table. If the reliability level contained in the RREQ message is greater than that in the routing table, the relay node updates the entry with the information contained in the RREQ message.

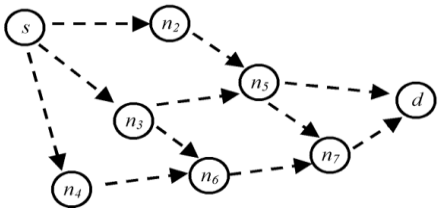


**Figure 7.** Broadcasting the RREQ message.

(3) ***Route Reply (RREP) generation at the destination node:*** The Unicast RREP message is generated by the destination or an intermediate node toward the source node once the intermediate node has received the RREQ message and has a route to the destination (Figure 8). A node copies the destination IP address, originator sequence number, and reliability level from the RREQ message into the RREP message, which is unicast back to the neighbor from which the RREQ message was received.

If the generating node is the destination, this node must immediately update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet before generating a RREP message in response to the RREQ message. The destination node places its sequence number into the destination sequence number field of the RREP message and enters the value zero in the hop count field of the RREP message.

When generating a RREP message, a node copies the destination IP address, originator sequence number, and reliability level from the RREQ message into the RREP message.

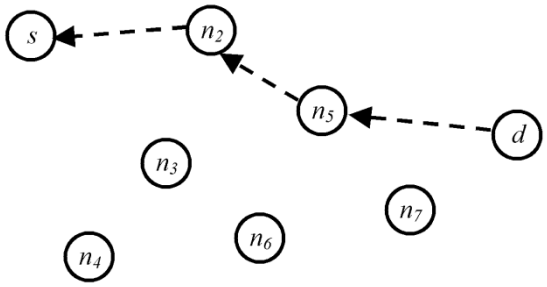


**Figure 8.** Unicasting the RREP message.

**(4) *Route reply (RREP) received at the intermediate node:*** When an intermediate node receives the RREP message from its neighbors, this node first increases the hop count value in the RREP message by one. When the RREP message reaches the source, the hop count represents the distance of the destination node from the source node in hops.

The originator sequence number contained in the RREP message must be compared with the corresponding destination sequence number in the routing table entry. If the originator sequence number of the RREP message is not less than the existing value, the node compares the reliability level contained in the RREP message to its current reliability level to find the lower value and then updates the reliability level of the RREP message with the lower value, which is the latest reliability level of this route.

If the sequence number in the routing table is marked as invalid or if the destination sequence number in the RREP message is greater than the copy of the destination sequence number of the node, the intermediate node creates a new entry with the destination sequence number of the RREP message and marks the destination sequence number as valid. The reliability level field in the route table entry is set to the reliability level contained in the RREP message.

## 4. Simulation

The performance of the three protocols, AODV, TAODV and FL-TPR, are compared using three performance metrics: packet delivery ratio, average end-to-end delay, and normalized routing load.

- **Packet delivery ratio** is the ratio of the data packets delivered to the destinations to the packets generated by the constant bit rate (CBR) sources[14]. The success of a protocol is shown by the performance of delivering packets from source to destination.
- **Average end-to-end delay** of data packets is the total delay experienced by the packet experiences while traveling toward the destination. This metric describes the packet delivery time. A lower end-to-end delay leads to better routing protocol performance.
- **Normalized routing load** is the number of routing packets transmitted per data packet delivered at the destination. This metric generally evaluates the efficiency of the routing protocol.

In the simulation, the IEEE 802.11 MAC protocol with a distributed coordination function (DCF) is used. The protocol is implemented using network simulator version 2 (NS-2) [15, 16].

### 4.1Simulation scenarios

*A- Nodes Misbehavior*

In this simulation, the trust values $t_v$ and battery energy $e_v$ values are assigned randomly $t_v \in \{0 \le t_v \le 100\}$ and $e_v \in \{0 \le e_v \le 100\}$ to each node. Therefore, the nodes may have different trust values *t* and battery energy *e* values. The possibility of dropping a packet caused by nodes misbehavior corresponds to the trust values $t_v$ and battery energy $e_v$ values given to that node. The probability of each node in dropping a packet, *Pd*, is given by the following equations:

$$Pd\ (t_v) = 100 - trust\ value \quad (8)$$

For example, a node would drop data packets 50% of the time if a node is given a trust value $t_v$ of 50. Also, a node would drop data packets if battery energy $e_v$ of node equal to zero.

By contrast, each node has a fixed power-level value, which is randomly assigned to all nodes at the beginning of the simulation. Over time, each node will slowly lose power. The power level reduction of the node can be determined using the formulation given below:

- When the node is under load, the power-level reduction per interval $p_{\downarrow(LR/i)}$ can be calculated as

$$p_{\downarrow\left(\frac{LR}{i}\right)}(\%) = 100\% \times \frac{T_s}{P_{FBwL}} \quad (9)$$

- When the node is idle, the power-level reduction per interval can be calculated as

$$p_{\downarrow\left(\frac{LR}{i}\right)}(\%) = 100\% \times \frac{T_s}{P_{FBwoL}} \quad (10)$$

where $T_s$ is interval time per second; $P_{FBwL}$ is the estimated value of the full battery power level when the node is under load, which is set up to $1\frac{1}{2}$ h (5,400 s); and $P_{FBwoL}$ is the estimated value of the full battery power level when the node is idle, which is set up to 6 h (21,600 s). Once the power level of a node reaches zero, the node is considered dead and will no longer be forwarding packets.

*B- Assumptions*

During out simulation experiments, we assumed there is a watchdog system to monitor the misbehavior of nodes and inform other nodes about the misbehaving nodes so that each node can be assigned a trust value based on these misbehaviors. It is assumed also the battery power of each node will decrease over time based on its load and the battery power of each node can last up to six hours in the case of without packet load, and one and half hour in the case of with packet load.

*C- Scenarios*

Two different scenarios were simulated to evaluate the performance metrics of the FL-TPR routing protocol.

In the first scenario, 50 nodes are fairly distributed within a 750 m × 750 m area with a transmission range of 250 m. The pause time varied from 10 s to 60 s, and the simulation period was 900 s. The nodes were allowed to move up to a maximum speed of 10 m/s. The traffic type was CBR. The parameters for the first scenario are shown in Table 2.

The second scenario has the same parameters as shown except for a lack of pause time and the allowance of nodes to move with a maximum speed of 15 m/s to 50 m/s.

**Table 2.** Simulation Parameters for Scenario 1.

| | |
|---|---|
| Number of Nodes | 50 nodes |
| Simulation Time | 900 s |
| Network Area Size | 750 m × 7500 m |
| Max Speed of node | 10 m/s |
| Mobility Model | Random way point |
| Traffic Type | CBR |
| Packet Size | 512 bytes |
| Connection Rate | 4 pkts/sec |
| Pause Time | 10 s to 60 s |
| Number of Connection | 5 |

### 4.2Simulation Results

Figure 9 illustrates the packet delivery ratio for AODV, TAODV and the FL-TPR routing protocols for scenario 1. In this scenario, the FL-TPR protocol has a larger packet delivery ratio compared with that of the AODV and TAODV. The AODV selects a path based solely on hop count (shortest) regardless of the trust and the battery energy values assigned to nodes, which lead to the low percentage of the packet delivery ratio of the AODV. TAODV selects a path based on the trust values given to nodes regardless the hop count (shortest path) and the battery energy values assigned to nodes. This could increase the percentage of packet delivery ratio as compared to AODV which depends on shortest path only.

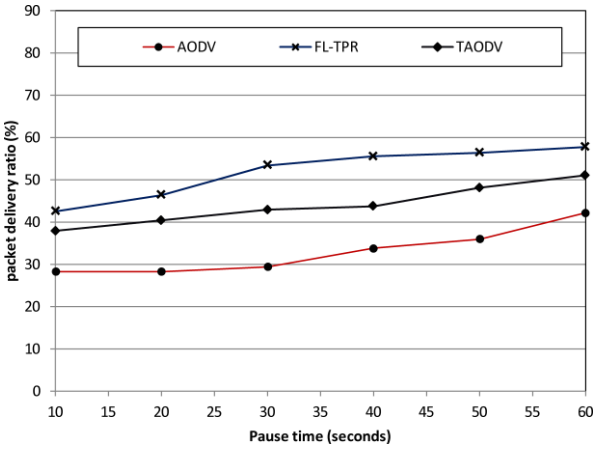


**Figure 9.** Packet delivery ratio for scenario 1

The FL-TPR selects a route based on the reliability level of path *R*, which is fuzzified in the FL-TRR protocol using trust level $t_p$, battery energy $e_p$ and hop count *n*. However, the FL-TPR avoids low trust and battery energy values, which gives the FL-TPR a better packet delivery ratio.

Figure 10 illustrates the average end-to-end delay for the AODV, TOADV and the FL-TPR routing protocols. Several misbehaved nodes exist in the network in AODV. A portion of the packets has to wait in buffer for a long time and the nodes are required to find a new route to the destination. If the packets still pass through the network, a high end-to-end delay occurs. TAODV depends on trusted path which will avoid untrusted nodes, but it may select long path to destination. The FL-TPR routing protocol depends on the trusted nodes with high battery energy and the trusted nodes to select a route and forward packets. Therefore, the possibility of having a broken route caused by misbehaved nodes is avoided. The packets no longer have to wait in buffer for a long time because the current route exists.

However, the FL-TPR protocol performs better than the AODV protocol in terms of average end-to-end delay.

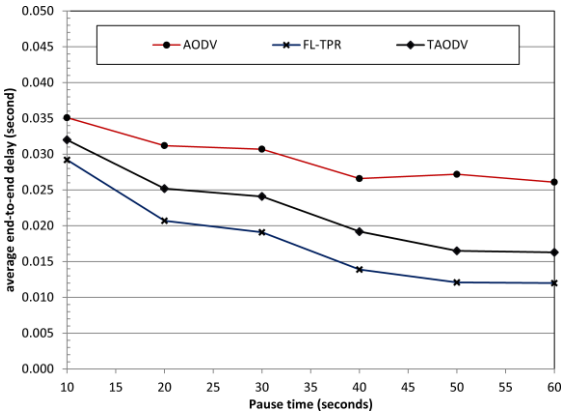


**Figure 10.** Average end-to-end delay for scenario 1

The FL-TPR and TAODV may have a higher average end-to-end delay than the AODV protocol because the route selection mechanism in both TAODV and the FL-TPR may choose a longer and more trusted path than the shortest path in the AODV as shown in Figure 11.

In Figure 11, the three paths between source node *s* and destination *d* and the two values on each edge represent trust value $t_p$ and battery energy $e_p$.

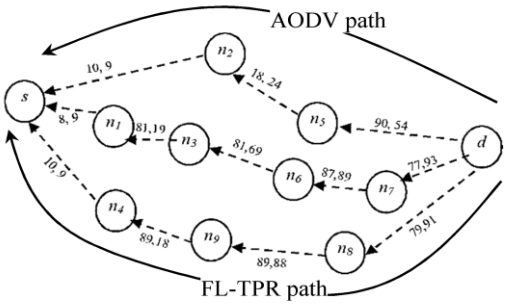


**Figure 11.** Example of an ad-hoc network with trust and battery level values

The edge between *s* and $n_2$ has the values 10 and 9 for $t_p$ and $e_p$, respectively. The AODV selects path *s*, $n_2$, $n_5$, *d* because it has few hop count (3 hops), whereas FL-TPR selects path *s*, $n_4$, $n_9$, $n_8$, and *d* despite the higher hope count (4 hops) because of the better trust and battery values of this path.

However, this experiment shows that the FL-TPR and TAODV performs better than the AODV because the possibility of having broken routes caused by misbehaved nodes is higher in the AODV than TAODV and the FL-TPR. In AODV, the path chosen is the shortest path but may have to be recalculated because of the misbehaved nodes, which yield to higher end-to-end delay. TAODV could avoid some of misbehaved nodes but it may choose the longest path. The possibility of recalculating the path is lower in the FL-TPR because of the routing mechanism, which depends on higher trust and battery energy values and a lower number of hops.

In Figure 12, the FL-TPR protocol actually generates a lower routing load then the AODV and TAODV. The AODV may choose the shortest path but this path may contain untrusted and zero-powered nodes that may drop the packets. Therefore, the path breaks and a new path will have to be recalculated, which generates more overhead packets (RREQ and RREP messages). TAODV may choose path that contain zero-powered nodes that may drop the packets and/or longest path to destination. Therefore, Nodes in TAODV generates more RREQ and RREP messages in order to reach the destination. The FL-TPR performs better because the path often does not have to be recalculated and it depends on hop count to find path between source and destination.

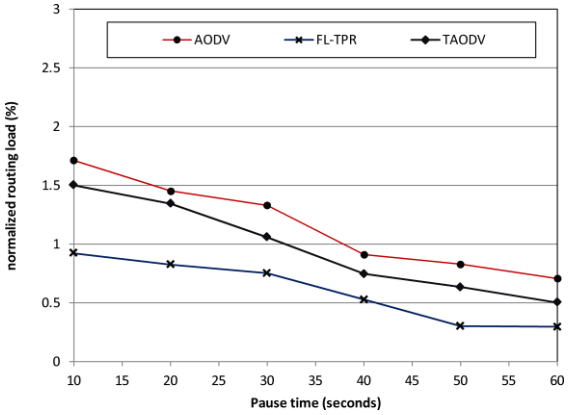


**Figure 12.** Normalized routing load for scenario 1

Figure 13 illustrates the packet delivery ratio for the AODV, TAODV and FL-TPR routing protocols for scenario 2. In this scenario, an increase in node speed reduces the packet delivery ratio for all three protocols because of high mobility, which leads to unstable routes between the source and destination nodes. However, the experiment result for the FL-TPR shows better performance than the AODV and TAODV in terms of packet delivery ratio.

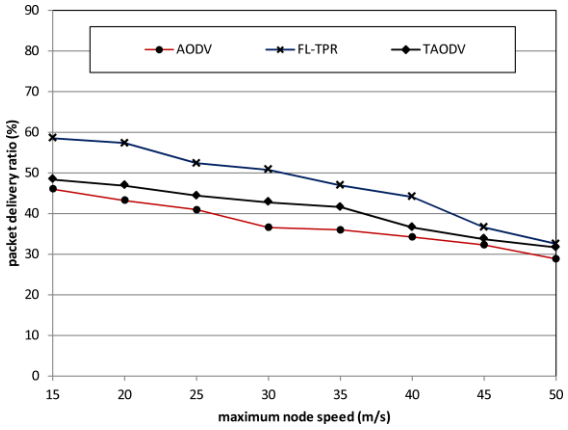


**Figure 13.** Packet delivery ratio for scenario 2

Figure 14 illustrates the average end-to-end delay for the AODV, TAODV and FL-TPR routing protocols. In all three protocols, the average end-to-end delay increases when the maximum speed increases as well because of the unstable network caused by the high speed of the movement of the nodes. The nodes in all protocols are required to find a new route when the current route is broken because of high mobility [17, 18,19].

Misbehaved nodes are also the cause reason of the broken route in the AODV, which is affected by the speed of the nodes and the misbehaved nodes. TAODV can reduce the percentage of broken route caused by untrusted nodes. The FL-TPR helps the nodes in reducing the effect of misbehaved nodes by avoiding low trusted and battery energy nodes. However, the FL-TPR still performs better than the AODV in terms of average end-to-end delay.

Figure 15 illustrates the normalized routing load for the AODV, TAODV and FL-TPR routing protocols. The normalized routing load in TAODV and FL-TPR is expected to increase because of the extra messages that should be generated when the chosen path is longer than that in AODV

as shown in Figure 11. These messages lead to a highly normalized routing load. However, the experiment result shows that FL-TPR and TAODV actually generates a lower routing load than AODV because the rate for the broken route is higher in AODV. FL-TPR has better performance by not having to recalculate the path often and it will avoid zero-powered nodes.

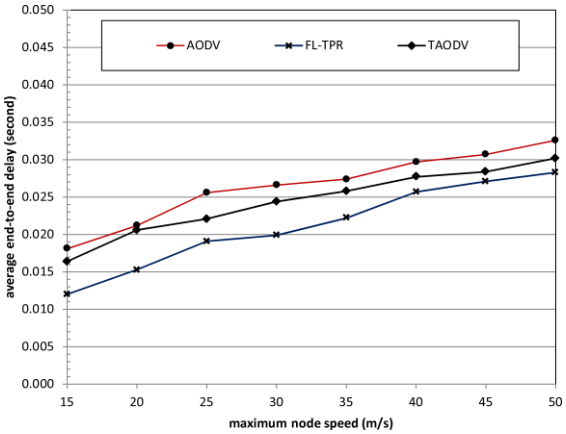


**Figure 14.** Average end-to-end delay for scenario 2

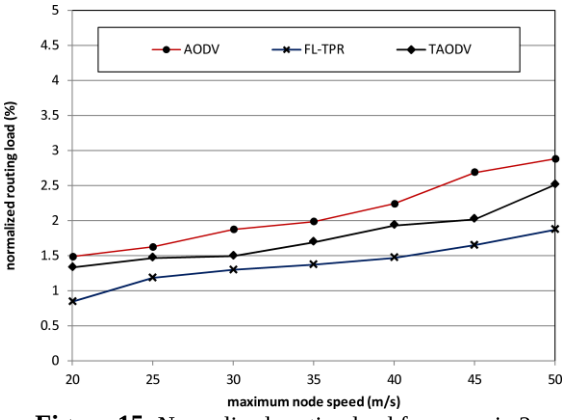


**Figure 15.** Normalized routing load for scenario 2

## 5. Conclusion

This paper presents a new MANET on-demand routing protocol called the FL-TPR protocol. The FL-TPR protocol provides an improved performance protocol by considering the trust level and battery energy levels of the nodes along the path and the hop count. The proposed protocol was implemented and simulated using the NS-2 network simulator. In the simulation, each node is given a trust value and a battery energy level. These values are associated with the possibility of a packet drop by the node. The simulation result shows that the FL-TPR protocol provides a higher percentage of successful data delivery than the AODV and TAODV. The proposed protocol also performs better than AODV and TAODV in terms of end-to-end delay and normalized routing load.

This work has been done for a single unicast routing protocol. The next step in developing a general optimal routing protocol is the extension of our trust battery model into the multipath routing protocol in the MANETs. We will also further look at some issues that have not been addressed in this paper such as minimizing storage, resource consumption, ensuring optimal paths, and minimizing network load.

## References

[1] H. Arya, and A. Chauhan. "Survey on Various Routing Protocols and Mobility Models used in Mobile Ad Hoc Network." Current Trends in Information Technology 9, no. pp 40-45. 2002.

[2] S. S. Mohamed, I. Abdel-Fatah, and M. A. Mohamed. "Performance evaluation of MANET routing protocols based on QoS and energy parameters." International Journal of Electrical & Computer Engineering. pp. 2088-8708. 10. 2020.

[3] V. K. Quy, N. T. Ban, V. H. Nam, D. M. Tuan, and N. D. Han. "Survey of recent routing metrics and protocols for mobile Ad-hoc networks." Journal of Communications 14, no. 2, pp 110-120. 2019.

[4] B. T. Sharef, A. R. Al-Breiki, H.. Jassim, Z. T. Sharef, "Review of Wireless Sensor Networks: Challenges and Threats", International Journal of Innovative Science and Research Technology. Vol.3, No. 4, pp. 980-984. 2018.

[5] Djenouri, Djamel, Lyes Khelladi, and Algiers Nadjib Badache. "A survey of security issues in mobile ad hoc and sensor networks." IEEE Communications surveys & tutorials 7, no. 4 .2020.

[6] Borkar, Gautam M., and A. R. Mahajan. "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks." Wireless Networks 23, no. 8 pp 2455-2472.2017

[7] X. Li, M. R. Lyu and J. Liu, "A trust model-based routing protocol for secure ad hoc networks," in Aerospace Conference, 2004. Proceedings. 2004 IEEE, pp 1286-1295.2004

[8] S. R. Das, E. M. Belding-Royer and C. E. Perkins, "Ad hoc on-demand distance vector (AODV) routing,". RFC 3561. 2003.

[9] H. S. Jassim, S. Yussof, T. S. Kiong, S. Koh and R. Ismail, "A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network," in Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, , pp 547-554.2009

[10] V. S. V. Devi. "Energy efficient multipath routing protocol for MANET for enhancing QoS and QoE in multimedia applications." Int. J. Commun. Networks Inf. Secur. 8, no. 3, pp 158-170. 2016.

[11] K. Woo, C. Yu, D. Lee, H. Y. Youn and B. Lee, "Non-blocking, localized routing algorithm for balanced energy consumption in mobile ad hoc networks," in Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 2001. Proceedings. Ninth International Symposium on 2002,, pp. 117-124.2002

[12] C.-K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," Communications Magazine, IEEE, vol. 39, pp. 138-147, 2001.

[13] H. Chuanhe, C. Yong, S. Wenming and Z. Hao, "A trusted routing protocol for wireless mobile ad hoc networks," 2007.

[14] J.-H. Song, V. Wong and V. C. Leung, "Load-aware on-demand routing (LAOR) protocol for mobile ad hoc networks," in Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual, pp. 1753-1757. 2003

[15] I. C. S. L. M. S. Committee, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," ed: IEEE Std, 1997.

[16] S. Kurkowski, T. Camp, N. Mushell and M. Colagrosso, "A visualization and analysis tool for ns-2 wireless simulations: inspect," in Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 13th IEEE International Symposium on, 2009, pp. 503-506. 2009

[17] B. T. Sharef, R. Alsaqour, M. Alawi, M. Abdelhaq, and E. Sundararajan. "Robust and trust dynamic mobile gateway selection in heterogeneous VANET-UMTS network." Vehicular communications 12: pp 75-87.2018.

[18] B. T. Sharef., R. A. Alsaqour, and M. Ismail. "Vehicular communication ad hoc routing protocols: A survey." Journal of network and computer applications, pp 363-396.2014
[19] B. Annane, A. Alti, and O. Ghazali. "SecNetworkCloudSim: An Extensible Simulation Tool for Secure Distributed Mobile Applications." Int. J. Commun. Networks Inf. Secur. Vol. 12, No. 1., pp. 47-62, 2020.