Efficient and fair node selection algorithm for content distribution in mobile Ad-Hoc Networks (MANETs)

Rawan Hassoubah[1] , Etimad Fadel[2] and Helen Bakhsh[3]

[1]Department of Computer Science, King Abdul Aziz University
Jeddah, Saudi Arabia , roooonly@gmail.com
[2]Department of Computer Science, King Abdul Aziz University
Jeddah, Saudi Arabia , eafadel@kau.edu.sa
[3]Department of Computer Science, King Abdul Aziz University
Jeddah, Saudi Arabia , helen_bakhsh@hotmail.com

Abstract

Mobile Ad-hoc networks are types of networks, which are widely used nowadays, especially with the increasing demand for mobile devices. Deriving solutions in mobile ad-hoc networks is quite challenging due to a variety of reasons, including their decentralized nature, lack of energy and infrastructure, topological changes, and many more. One of the current research areas is regarding content distribution, with a specific focus on selecting the appropriate node for said distribution for better routing. Selecting the wrong node, i.e. one that is malicious or lacks resources, such as battery power, could affect the overall network life time and security. In this research, a model based on multi factors has been implemented for efficient and fair node selection in mobile ad-hoc networks. Factors such as trustworthiness of nodes, energy, and speed were considered and combined to develop an effective and fair node selection mechanism. The proposed work has been applied on AODV routing protocol that is commonly used in MANET. The simulation results showed the efficient performance of the network after implementing the proposed algorithm compared to original AODV and another routing protocol in that it achieved higher packet delivery ratio and lower end-to-end delay but with higher energy consumption.

Keywords:MANET, Network Protocols, Node selection, AODV, Trust management, trustworthiness, node energy, node mobility

1. Introduction

The text must be in English. Authors whose English language is not their own are certainly requested to have their manuscripts checked (or co-authored) by an English native speaker, for linguistic correctness before submission and in its final version, if changes had been made to the initial version. The submitted typeset scripts of each contribution must be in their final form and of good appearance because they will be printed directly. The document you are reading is written in the format that Wireless technology is clearly the basis for the future of information technology; however, traditional cellular and mobile networks are limited by certain infrastructures. Mobile Ad-Hoc Networks (MANETs) are the recent, important evolution in wireless networks. They compose of nodes (devices) that communicate wirelessly and are self-organizing and self-controlling and have dynamic topology. MANETs are self-organizing and has no routers and are flexible. They are used in home networks, in personal area networks, in sensor networks, in the operations of law enforcement, military, remote areas, rescue operations and educational and commercial applications [1][2]. Each node takes the role of a router, forwarding content/traffic to other members in the network. They have limited resources, battery power, bandwidth and storage. Additionally, there is no membership control of the nodes, resulting in many security challenges. In MANET, topological routing protocols could be categorized into three groups: proactive, reactive/on-demand and hybrid protocols [3]. And depending on the network purpose and scope, the appropriate routing scheme is selected and applied.

MANETs security is important and with the absence of a central coordination mechanisms this made it vulnerable to attacks compared to wired networks [4]. One of the current research areas is regarding node selection for content distribution, with a specific focus on selecting the appropriate node for said distribution. Node selection is choosing the next hop node in routing in order to forward the packets to. This strategy is done based on some conditions and pre performed tests to have the best choices. It is usually an add-on or modification of traditional routing protocols. The selection of strong and effective candidate nodes is a key issue in communication [5].

Choosing the next hop node in routing should avoid choosing misbehaving nodes or nodes with limited resources as much as possible. A wrong node selection, for instance, choosing a node that is malicious , selfish, lacking energy power, high speed most likely will have fast disconnection from the network could obviously threaten the network security and/or degrade the overall network performance. Therefore, Node selection mechanisms for packet or content delivery are challenging tasks in this type of networks. Selecting the appropriate and reliable nodes at routing discovery should, therefore, be done very carefully.

Most of recent proposed mechanisms in MANET prefer selecting the node that is most trusted. Others have limited their selection based on trust and available energy. Still others have presented reputation-based schemes to eliminate malicious or selfish nodes only or load balancing. Also, some applied link failure and transmission range into their node selection process. Furthermore, other work was depending on node mobility or speed. While each research was clearly successful, the focus was always only on one or two factors for node selection, as opposed to including and considering multiple factors at the same time. The consequence of this is that mechanisms could, for example, choose a node based on higher trust value, with the selected node having very little energy resources. After a certain time, the selected node will disconnect from the network, leaving the mechanism to redo the selection process; this is costly and can affect performance and network overall lifetime. Other scenarios include the selection of trusted, but also selfish nodes, resulting in the need to consider the node’s resources. Also, the ones who selected nodes with minimum mobility have ignored its limited resources or its trustworthiness. This causes high degree of disconnections or involving malicious nodes in the routing path which threaten the security and performance. There is no previous work that considered more than two factors for node selection. In addition, their focus was, for instance, to implement a reliable routing path or cooperative path with little study of how different factors together could affect the node selection decision process and it later could affect the network performance. In this research three factors are considered for selection: node trustworthiness, node energy and node mobility speed.

This paper is organized as follows: section 2 presents the related work. Then, section 3 explains the three factors used for the node selection. Later, section 4 presents the proposed multi factor node selection algorithm. Next, the simulation and results are explained in section 5. Finally, in section 6 the conclusion is presented.

2. Related Work

There are good number of works done by reaches in node selections with the goal of achieving better network security and performance. Node selection for content distribution have attracted the researches as Jailani K. et al [6] have proposed a probability based node selection mechanism based on energy consumption in MANET. They have investigated the energy behavior of nodes; their scheme then selects the best node along the routing path. Mentari et al have proposed a novel trust and probabilistic node selection mechanism for content distribution in MANET in [7]. Their main goal was to achieve a trustworthy node selection and preserving mobile node resources. Later, in [8], they improved their work and compared it against additional node selection models.

Additional research carried out on MANET's security and trust, again with the main focus on improving network performance. One wherein Jan P. et al have proposed in hybrid MANET an algorithm to select a candidate node based on calculations on routing parameters collected from monitoring as presented in [5]. They have found trust level of mobile nodes by a direct trust model, and this trust value is dynamically changing depending on topology changes. Their algorithm, "DSR-Trust", achieved higher throughput but lower number of necessary hops to finding destination node. They have only relied on higher trust value for node selection. In addition, they did not consider the case of two nodes having the same trust value. Another work by Aarti B. and Shweta Y. include the proposal of new parameters for best route selection [9].

Other work in node selection depending on trust or/and energy is the one done by X.liz, Jia P and others , they proposed the ad-hoc on demand trusted path distance vector (AOTDV) routing protocol to discover trustworthy forward paths and alleviate the attacks from malicious nodes [10]. Also, Jan and Lubomir implemented a trust based algorithm for candidate node selection in hybrid

MANET-DTN. Their algorithm provides useful tool for selection of the optimal trusted path [11].

Securing communication in MANETs through trustworthiness is also concerned the researchers Priyanka and Pooja Narula in implementing a routing protocol (TAODV) that is evolution of the original AODV. They applied trustworthiness and intrusion detection system on the routing protocol AODV to have a secure communication. They have proved using simulation that the TAODV performed better than AODV in terms of end-to-end delay and packet delivery ratio [12].

In MANETs, there are number of proposed solutions in identifying or detecting malicious or selfish nodes and eliminating them in MANET. Authors in [13] have proposed a solution, "TE-AODV", to identify the malicious and selfish nodes behaviours in MANET, to achieve a cooperative routing. Deepika k. et al have proposed EESDSR, which improved the security of routing by selecting trustworthy and secure routes without malicious nodes[14]. They have used energy monitoring to differentiate between selfish and malicious nodes in MANET. Finally, in [15], authors presented a novel reputation-based strategy to detect non-cooperative, "selfish" nodes, in addition to selecting an appropriate forwarder node. Their work has improved the delivery ratio and overall network performance.

3. Factors used for node selection algorithm

This section presents the three factors used for the node selection in the proposed algorithm, and how each factor is calculated separately before presenting the algorithm factors are:

- Node trustworthiness.

- Node remaining energy.

- Node mobility speed.

3.1. Trustworthiness

Trust between mobile nodes in MANET is essential to perform interactions. A node with certain good level of trust value is expected to be less likely a misbehaving node. Selecting a node that have a satisfied trustworthiness level will avoid including as much as possible misbehaving nodes in the routing path, either attacks or selfish nodes. Trust is calculated based on the routing information and/or data packets monitoring and with collecting those information the trust will be found between nodes. There are three types of trust calculation models. They are direct trust, indirect trust and a hybrid trust calculation [5] as shown in Fig. 1. In this research the

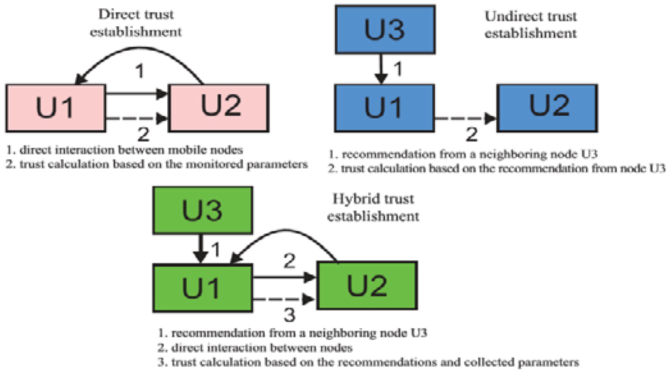

Direct trust establishment
U1
U2
1
2
1. direct interaction between mobile nodes
2. trust calculation based on the monitored parameters
U3
Undirect trust establishment
1
U1
U2
2
1. recommendation from a neighboring node U3
2. trust calculation based on the recommendation from node U3
U3
Hybrid trust establishment
1
2
U1
U2
3
1. recommendation from a neighboring node U3
2. direct interaction between nodes
3. trust calculation based on the recommendations and collected parameters

Fig. 1 Trust Calculation Models in MANET

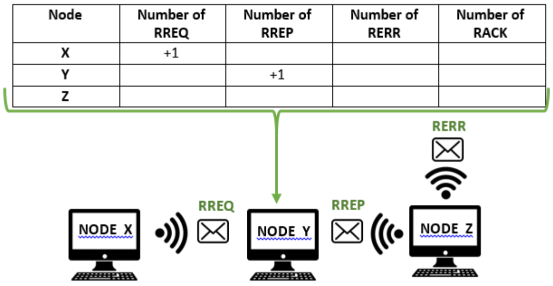
In this research, the direct trust model is used for trust calculation. Where a source node "the one holding the content" finds the trust value of its neighbouring nodes by itself with the direct interaction with those nodes [5]. The value of trust is not sent to further other nodes as recommendation. However, servers locally on that node are used for this and helps it in deciding. The trust value was calculated through two stages they are:

- Stage 1: Obtaining and storing the routing information.
- Stage 2: Trust computing.

In the first stage, two types of parameters were monitored. First, values of routing and data packets sent or received from each mobile node. This includes the following: Route request messages (RREQ), Route replay messages (RREP). Route error messages (RERR). Acknowledgements (RACK). Data packets (D). Second, total number of routing and data packets sent across the mobile nodes. This means, all routing packets sent or received from particular mobile nodes. This includes the following: Total route request messages (R_{treq}), Total replay messages (R_{trep}), Total error messages (R_{trerr}). Total acknowledgements (R_{track}), Total data packets (D_t).

All collected parameters from this stage were stored in the data structure in memory separately for each node.

Fig. 2 illustrates the process of monitoring and collecting parameters from nodes.



Node	Number of RREQ	Number of RREP	Number of RERR	Number of RACK
X	+1			
Y		+1		
Z				

Fig. 2 Process of Monitoring and Collecting Data

In the second stage is Trust calculation. It is implemented on routing information denoted by T_r as partial trust value and it is given by Eq. (1). And trust calculation from data packets Td given by Eq. (2).

$$T_r = W_{rreq} * \left(\frac{R_{req}}{R_{treq}}\right) + W_{rrep} * \left(\frac{R_{rep}}{R_{trep}}\right) + W_{rerr} * \left(\frac{R_{rerr}}{R_{trerr}}\right) + W_{rack} * \left(\frac{Rrack}{Rtrack}\right) \quad (1)$$

$$T_d = W_d * \left(\frac{D}{D_t}\right) \quad (2)$$

Values in the numerator and de numerator were explained before in this section. The values $W_{rreq}, W_{rrep}, W_{rerr}, W_{rack}$ and W_d are constants which define a weight of trust value. Constants are change depending on either attacks type or what we intend to balance in the parameters used in the trust calculation. In this algorithm the constants are assigned the following values
$W_{rreq} = 0.2,\ W_{rrep} = 0.5,\ W_{rerr} = 0.2,\ W_{rack} = 0.2,\ and\ W_d = 0.3$, where the constant W_{rrep} is given the highest weight as it is one of this research goals is to avoid some misbehaving nodes like "selfish nodes" that do not cooperate in the network. Therefore, it is assumed that considering the number of route replies (RREP) as the most effective type of routing packets in calculating trust and it is given highest weight.

The Resulted final trust value of the node was in certain selected range. FTV ranges between [0, 1] , ($0 \leq FTV \leq 1)$ it is represented by the sum of the two partial trust values T_r and T_d as given in Eq. (3).

$$FTV = T_r + T_d \quad (3)$$

The process of final trust value (FTV) computing is illustrated in Fig. 3.

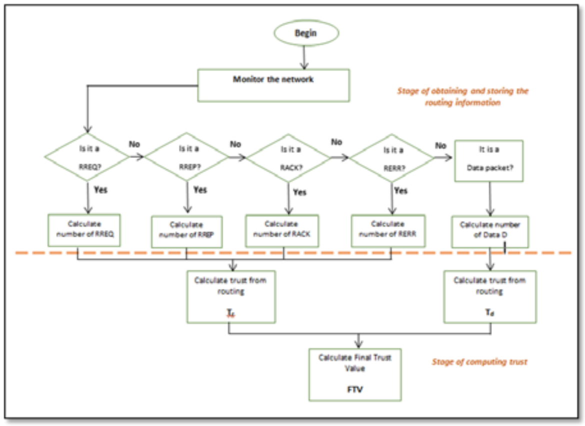


Fig. 3. Final Trust Value Calculation Flow Chart

3.2. Remaining energy

The node selection algorithm was concerned about the remaining energy in each candidate node. Consumed energy of a node is the summation of the energy consumed during the three types of interactions, transmitting, receiving and overhearing [13]. The proposed algorithm selected a node with remaining energy percentage matched a specific threshold value. For a particular node (C) the remaining energy percentage E(c) remaining energy percentage was computed using the remaining energy value "E(c) remaining energy" and the initial energy "E(c) initial energy". And the E(c) remaining energy of a node is the subtraction of the initial energy "E(c) initial energy" and consumed energy "E(c) consumed". The Eq. (4), (5), (6) shows the remaining energy calculation.

$$E(c)_{consumed} = \quad (4)$$

$$E(c)_{transmission} + E(c)_{reception} + (N-1) * E(c)_{overhearing}$$

$$E(c)_{remaining\ energy} = E(c)_{initial\ energy} - E(c)_{consumed} \qquad (5)$$

$$E(c)_{remaining\ energy\ percentage} = \frac{E(c)_{remaining\ energy}}{E(c)_{initial\ energy}} * 100 \qquad (6)$$

The remaining energy percentage in previous Eq. (6) calculated frequently for each candidate node separately after some time interval. If it was found to be less than 50% then the energy level value was assigned to 1. And, in case it exceeded 50% then the energy level value was assigned to 2. Energy percentages are stored in nodes locally for later use.

3.3. Mobility speed

The mobility of nodes affects the number of average connected paths, as well as, the performance of the routing algorithm. One of the major issues in MANETs is how to reduce the link breakage as much as possible that is usually due to mobility of mobile nodes. The node selection algorithm aimed to select a node with minimum speed. However, selecting a node that is moving in high speed can break the routing path by moving the node out of the route. In this research, nodes are assigned random values of speed measured by m/s. Speed values ranges between 0 to 10 m/s. And the mobility model used is the random waypoint mobility model. The algorithm will select the node with minimum speed.

4. The proposed multi factor node selection algorithm

Node selection algorithm is activated whenever there is a packet requires to be forwarded to next hop node in the routing path. Routing in MANET was done using the AODV (Ad-hoc On-demand distance vector) routing protocol. Assuming that a MANET combined of specific number of nodes in the topology. All nodes in the network were assigned default value of trust and varying random numbers of energy and speed. The following are the assumptions considered:

- The entire nodes in the topology operated in a promiscuous mode.
- All links are bidirectional.
- A node that is holding the packet is the one that called source and performs the decision of selection processes.
- All candidate nodes assumed to be only the directly connected nodes or (one-hop nodes).
- Routing tables are updated with the selected reliable nodes as next hop nodes in the routing path.
- Acknowledgments are one hop type.

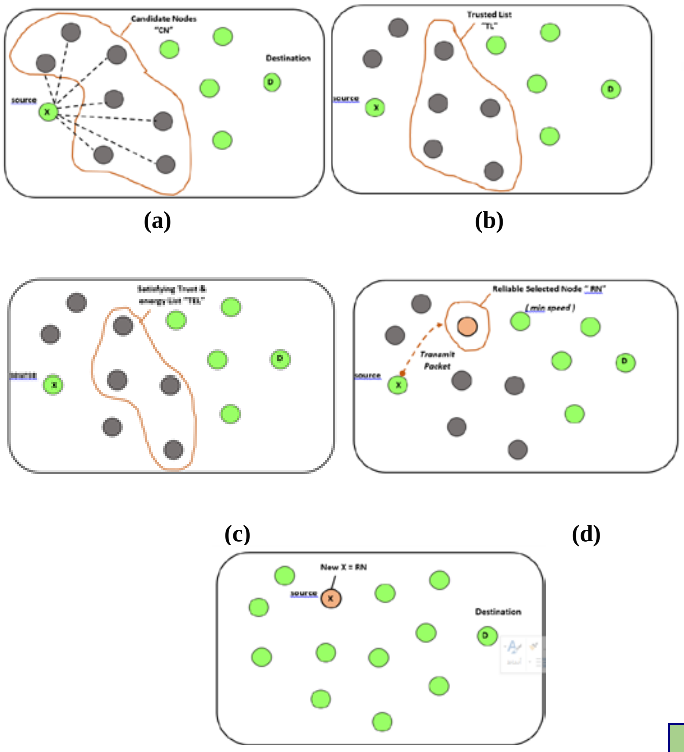
In the proposed algorithm the sender or source node X will discover its directly connected neighbours to have a list of candidate nodes through "Hello messages". This Candidate Node list called CN and compose of the nodes (CN1, CN2, CN3,…...CNn), where n is the total number of candidate nodes for selection. Once CN discovered using "Hello messages" it is given initial values for each of the factors. After constant time intervals CN were sending passive acknowledgments back to node X with its information about routing and data packets, energy and mobility speed. Once received, node X, were able to calculate the trust value of its neighbors, remaining energy levels and reading the node speed.

Node X constructed a table called Neighboring Nodes (NN) table that contains a single entry for each of the CNs. Each entry in this NN table contains the calculated Final Trust Value (FTV $_i$), remaining energy percentage (EC $_i$) and mobility speed (NB $_i$), where i is the candidate node sequence number in the CN list. For instance, C1 node indicating the first candidate node with the attributes FTV1, EC1 and NB1. And C2 node indicating the second candidate node with the attributes FTV1, EC1 and NB1. Assuming in the case of having N number of CN the NN table will contain N number of entries as well. At the time when Node X will not receive an acknowledgment from certain neighbour node (C) its entry in the NN table will be removed. On the other hand, in case of a new C node became in direct communication with node X, a new entry was added for it as well. Table 1. shows the NN table information. FTV and EC values were constantly changing and re measured after certain time intervals. While node’s NB was assumed to be constant. The selected reliable node RN for packet forwarding was chosen based on those table entries.

Table 1. Neighbouring Nodes (NN) table

Node_ID	Final_Trust _Value (FTV)	Remaning_ energy _percentage (EC)	Mobility_ speed (NB)

The following graphs in Fig.4 presents the node selection process. In (a) shows the candidate nodes that are directly connected with the source node. (b) Shows the result after applying the trust algorithm to produce the trusted list (TL). Then, (c) illustrates the result after applying the remaining energy calculation producing the list of nodes with a satisfied trust and energy called (TEL). Later, graph (d) illustrates the reliable node selected after testing the node's speed to have the resulted selected node (RN). Finally, the last graph (e) mentions the new source allocation, that is, the new source becomes the reliable selected node.



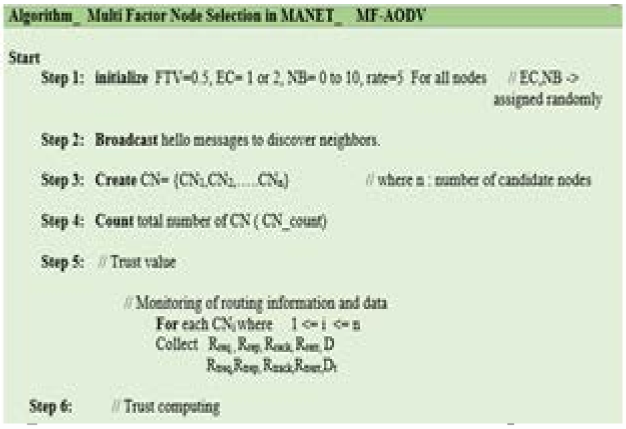
(a) **(b)**

(c) **(d)**

(e)

Fig.4. Node Selection Process, (a): Candidate nodes, (b): Trusted List, (c): Satisfied trust & energy list, (d): Node selection after testing speed, (e): new source

The proposed algorithm (Multi factor node selection "MF-AODV") is presented in Fig. 5 and the flow chart is illustrated in Fig. 6.



```
Algorithm_ Multi Factor Node Selection in MANET_  MF-AODV

Start
    Step 1:  initialize FTV=0.5, EC= 1 or 2, NB= 0 to 10, rate=5 For all nodes    // EC,NB ->
                                                                                  assigned randomly

    Step 2:  Broadcast hello messages to discover neighbors.

    Step 3:  Create CN= {CN1,CN2,....CNn}          // where n : number of candidate nodes

    Step 4:  Count total number of CN ( CN_count)

    Step 5:  // Trust value

                // Monitoring of routing information and data
                   For each CNi where   1 <= i <= n
                   Collect  Rreq , Rrep, Rrack, Rrerr, D
                            Rreq,Rrep, Rrack,Rrerr,Dt

    Step 6:     // Trust computing

    Step 9:     Read NB of node                       // Node mobility speed
    Step 10:    If ( FTVi >=0.5 )                     // trust threshold
                    add node CNi to TL                // trusted list
                    rate +1
                    TL_count+1
                Else
                    rate-1

    Step 11:    For ( TLi where 0 <= i <= TL_count )
                    IF ( ECi (TLi) ==1)               // remaining energy threshold
                        Add node TLi to TEL           // satisfied trust & energy list
                        rate +1
                        TEL_count+1
                    Else IF ( ECi (TLi) ==2)
                        rate-1

    Step 12:    For ( TELi where 0 <= i <= TEL_count )
                    Find min NB in TELi               // minimum speed "speed threshold"
                    Add rate +1  for minimum NB node

    Step 13:    Select RN with highest rate value.    // reliable node
    Step 14:  Set next node X ==RN                    // new source
    Step 15:  repeat from step 2 until packet reaches destination
End
```

Fig. 5 Multi Factor Node Selection Algorithm

Parameters	Value
Routing protocols	AODV, TE-AODV, MF-AODV
Simulation area	1000 m X 1000 m
Time of simulation	100 s
Transmission range	250 m
Number of nodes	15, 20 ,30
Maximum speed of nodes	10 m/s
Model placement	Random
Mobility model	Random way point
Pause time	10 s
Traffic type	UDP
Reference value of trust	W_{rreq} =0.2, W_{rrep}=0.5, W_{rerr}=0.2, W_{rrack}=0.2,W_{d}=0.3
Number of packets sent	100 p

Table 2. Simulation Setup

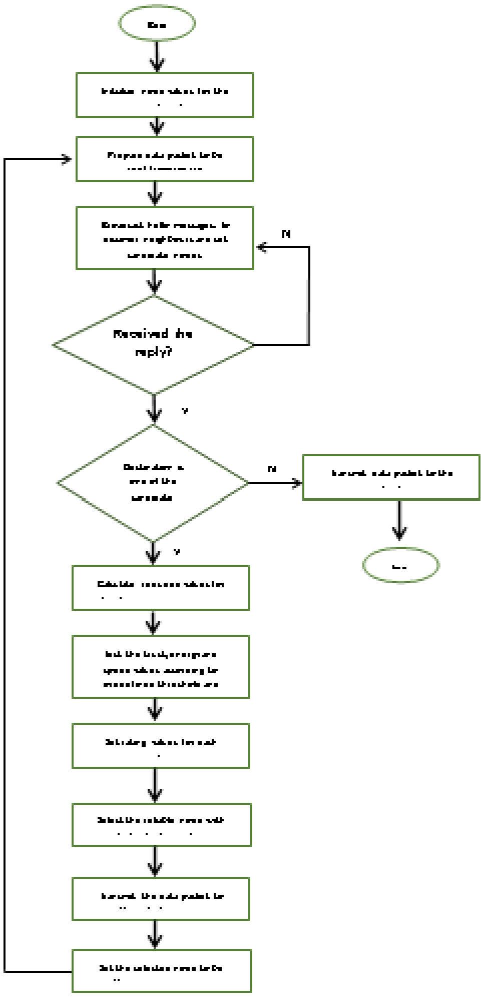


Fig. 6 Flow chart of the proposed algorithm

5. Simulation and results

The proposed node selection algorithm effectiveness was tested using simulation with the NS-3 "network simulator 3" [16], [17], [18]. The scenario implemented and evaluated using three different metrics. The main goal is testing the effectiveness of using three different factors for reliable node selection (trust, energy and speed) and compare it against the original AODV routing protocol [19], [20] and another protocol in the literature TE-AODV "Trust Energy AODV" [13]. The proposed work was overall a modification of the AODV routing protocol. The metrics tested are the packet delivery ratio, end-to-end delay and energy consumed.

5.1 Simulation experiment

The network nodes distributed using the Random way point mobility model in a 1000 m X 1000 m simulation area. There was one source node and one destination node and the simulation runs over 100 sec (simulation time). There were 100 packets sent over the network every one second each of 1024 byte. The simulation setup and parameters listed in Table 2.

In this simulation different number of nodes were tested (15, 20 and 30). The three metrics used for evaluation are the following:

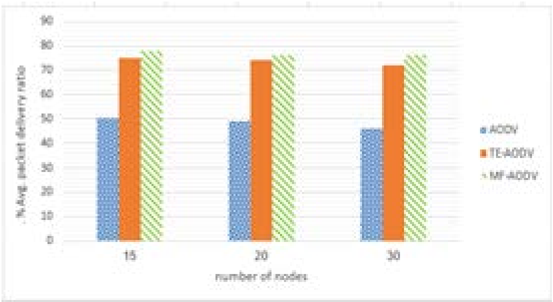
- Packet delivery ratio (PDR): It is the ratio of total data received to total data sent from source node to destination node.
- Average end-to-end Delay (ETED): The average end-to-end delay time that a packet takes to traverse from the source to the destination in seconds. In other words, the time taken between MANET packet creation at the source node and the packet delivery to the destination node.
- Energy Consumed (EC): It is the energy consumption per second during the simulation time. [6].

5.2. Simulation results

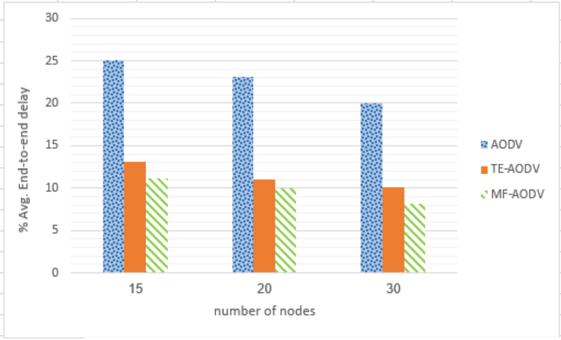
This section illustrates the scenario implemented in the simulation and its results as following:

5.2.1 Varying number of nodes for different MANET protocols scenario

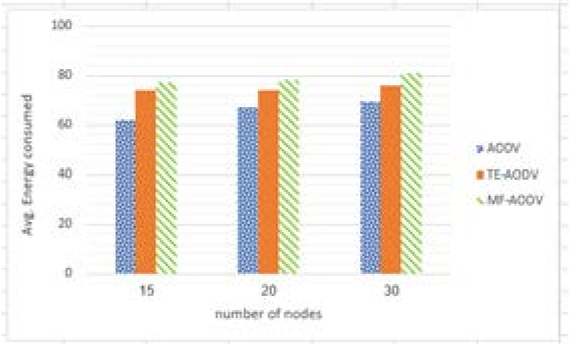
In this scenario, nodes simulated according to parameters in Table 2. The number of nodes tested were 15, 20 and 30 nodes. The simulation run, first, on "original AODV" routing protocol with the mentioned number of nodes and the three metrics are calculated. Then, second run on the "TE-AODV" (Trust and Energy- Ad-hoc on Demand Distance Vector) mentioned in literature [16]. Finally, run on the proposed "MF-AODV". The results of the three metrics (PDR, ETED and EC) compared against those three protocols with varying number of nodes. Fig. 7 Illustrates the graphs results for the three protocols in regard to three performance metrics "parameters" for different number of nodes.



(a) Avg. packet delivery ration VS. No. of nodes



(b) Avg. end-to-end delay VS. No. of nodes



(c) Avg. energy consumed VS. No. of nodes

F
j
ℓ
.

7. Performance parameters with varying number of nodes in different routing protocols. a. Packet delivery ratio, b. End-to-end delay, c. Energy consumption

Fig.7.a. shows the packet delivery ration Vs. number of nodes. Notice that the "TE-AODV" has significant higher average PDR than "AODV" as it implements a cooperative routing paths. And the proposed "MF-AODV" has higher PDR compared to both of "AODV" and the "TE-AODV". This is because, the "MF-AODV" implements a dynamic calculation of trust and energy of nodes this leads to encouraging nodes to be more cooperative and not selfish ,therefore, cooperate more in packets forwarding. Also, it has selected nodes with low mobility speed that does decrease the connection breakup as much as possible. Therefore, achieved higher PDR.

Fig.7.b. shows a plotted graph of the end-to-end delay Vs. number of nodes. The "AODV" has the highest end-to-end delay as it doesn't uses any minimization procedures for malicious nodes that causes packets drop and delivery delays. On the other hand, the "TE-AODV" and "MF-AODV" have close average end-to-end delay with the "MF-AODV" having lower value.

Fig. 7.c. shows the energy consumed Vs. number of nodes for each routing protocol. Energy is measured by joules per second "j/s" and after measuring the total average of energy consumed by each of the routing algorithms, it was noticed that the proposed "MF-AODV" have consumed more energy compared to other protocols. Because it involved extra calculations and packet data overhead. In addition, required routing data monitoring and collection that uses more energy. Also, the "TE-AODV" have higher energy consumption compared to "AODV" but lower than the "MF-AODV". This because, the "TE-AODV" used only two factors for node selection compared to the proposed algorithm that based on three factors. A summary table of the comparison between the routing algorithms in 15 nodes case illustrated in Table 3.

	Routing algorithms		
Performance Metrics	**AODV**	**TE-AODV**	**MF-AODV**
Avg. Packet delivery ratio - %	50.15	74.91	78.04
Avg. End-to-end delay - %	25.05	13.04	11.09
Avg. Energy consumed -J	62.02	73.83	77.28

Table 3. Summary comparison of performance metrics for different routing algorithms

6. Conclusion

MANET are type of networks that has number of characteristics that made its security a challenge. Most of the research focused their attention on MANET routing. This research aims to enhance network performance and security by selecting efficient reliable node for packets forwarding. The selection of reliable nodes was based on three factors, they are: trust, energy and nodes mobility speed. The proposed work has achieved good average of packet delivery ratio by, first, selecting nodes that are trusted and avoid the ones that are malicious like selfish nodes. Selfish nodes that do not cooperate in routing and decreases the packet delivery ratio. Second, selected nodes with a satisfied energy level and, third, nodes with minimum speed. Therefore, decreased the amount of disconnection from the network and reduced delays. After performing the simulation on the proposed multi factor node selection algorithm or "MF-AODV" it showed the following. The "MF-AODV" has significant higher PDR than "AODV" and "TE-AODV". End-to-end delays are considered low compared with other protocols but at close level to the "TE-AODV". Also, the "MF-AODV" has higher average of energy consumed compared to the other protocols. That is due to, the extra amount of calculation and routing packets overhead.

7. Future work

As a future vision the "MF-AODV" could be improve by adding more factors for node selection. Such as, bandwidth, communication range and location. The proposed algorithm could be studied more and adjusted to consume less energy by implementing less calculations and reducing packets overhead as much as possible. The work could be compared to other research done in the same field as well.

References

[1] Parul Gupta, (2016) ” A Literature Survey of MANET,” *in International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 2.

[2] Jai Shree Mehta, Shilpa Nupur, Swati Gupta, (2015) ”An Overview of MANET: Concepts, Architecture & Issues,” *in International Journal of Research in Management, Science & Technology* ,vol. 3, no. 2.

[3] Sofian Hamad, Salem Belhaj and Muhana M. Muslam, (2017) "Smart Selection of Candidate Neighbors for Efficient Route Discovery in MANETs ," *in Journal of Applied Sciences*, ISSN 1812-5654.

[4] Jayalakshmi V, Dr. Abdul Razak T, (2014) “Selection of Trusted Nodes in MANET by using Analytic Network Process,” *in COMPUSOFT, An international journal of advanced computer technology*, vol. 3, no. 3.

[5] Jan Papaj, Lubomir Dobos, Roman Palitefka, (2014) “Candidate node selection based on trust for cognitive communication of mobile terminals in hybrid MANET – DTN,” *in 5th IEEE International Conference on Cognitive Info communications*.

[6] J. Kadir, O. Ghazali, M. Firdhous and S. Hassan , (2011) "Node Selection Based on Energy Consumption in MANET", *InterNetWorks Research Group, School of Computing, University Utara Malaysia,* Malaysia September, 15.

[7] M. Djatmiko, R. Boreli, A. Seneviratne, and S. Ries, (2011) "Trust-based content distribution for mobile ad hoc networks," modelling, analysis simulation of computer and telecommunication systems (MASCOTS). *2011 IEEE 19th international symposium* , .pp. 433–436.

[8] Djatmiko, M., Boreli, R., Seneviratne, A., & Ries, S, (2013) "Resources-aware Trusted Node Selection for Content Distribution in Mobile ad hoc Networks," *Wireless networks 19*, no. 5, 843-856.

[9] A. Bairagi, S. Yadav and M. Student. (2014) "A New Parameter Proposed for Route Selection in Routing Protocol for MANET," *International Journal of Information Technology (IJIT)*, no. 1.

[10] X. Li Z. Jia P. Zhang R. Zhang H. Wang, (2010) "Trust-based on-demand multipath routing in mobile ad hoc networks," *IET Information Security, Special Issue on Multi-Agent & Distributed Information Security*.

[11] Jan PAPAJ, Lubomir DOBOS, (2014) "Trust Based Algorithm for Candidate Node Selection in Hybrid MANET-DTN," *information and communication technologies and services*, vol.12 , no. 4.

[12] Priyanka Garg and Pooja Narula, (2015) "Securing Communication in MANETS s Through Trustworthiness Using ns2," *International Journal of Engineering Research,* ISSN: 2348-4039 & Management Technology",vol.2, no.3.

[13] U. Venkanna, Jeh Krishna Agarwal and R. Leela Velusamy. (2014) "A Cooperative Routing for MANET Based on Distributed Trust and Energy Management," *Wireless Personal Communications*, 1-19.

[14] D. Kukreja, S. Kumar Dhurandher, and B. V. R. Reddy, (2015) "Enhancing the Security of Dynamic Source Routing Protocol Using Energy Aware and Distributed Trust Mechanism in MANETs." *In Intelligent Distributed Computing*, pp. 83-94. Springer International Publishing.

[15] C. Chandrima, A. Banerjee, S. Chakrabarti, and A. Chakraborty. (2015) "A Novel Approach for Non-cooperative Node Detection and Avoidance Using Reputation-Based Scheme in Mobile Ad hoc Network," *In Computational Advancement in Communication Circuits and Systems*, pp. 279-289.

[16] NS-3 simulator, *https://www.nsnam.org/*

[17] Network simulator 3, *http://networksimulator3.com/network-simulator-3-free-download/*

[18] UIO, NS3 simulator, *https://www.uio.no/studier/emner/matnat/ifi/INF5090/v11/undervisningsmateriale/INF5090-NS-3-Tutorial-2011-Oslo-slides.pdf*

[19] Khaled Ahmed Abood Omer, (2016) "The Impact of Node Misbehavior on the Performance of Routing Protocols in MANET," *International Journal of Computer Networks & Communications (IJCNC)*, vol.8, no.2.

[20] Swati Puri and Vishal Arora, (2014) " Routing Protocols in MANET: A Survey," International Journal of Computer Applications, vol.96, no.13.

Rawan S. Hassoubah Obtained her bachelor degree in Information systems from Taibah university, in Saudi Arabia since 2008 .A current masters student in computer science department at King Abdul Aziz University, Jeddah, Saudi Arabia. Recently working as lecturer in Jeddah University Saudi Arabia.

Etimad Fadel Ph.D. in Computer Science, Distributed Systems, De Montfort University, UK since 2006. Assistant professor in computer science department at king Abdul Aziz University, Jeddah, Saudi Arabia

Helen Bakhsh Ph.D. since 2017. Assistant professor in computer science department at king Abdul Aziz University, Jeddah, Saudi Arabia.