Towards Trust Model in Unmanned Aerial Vehicle Ad Hoc Networks

Moualla Alaa, AlDakkak Oumayma, and AlJnidi Mohamad

***Abstract*—Unmanned Aerial Vehicle ad hoc networks (UAANETs) are originally designed to work in a cooperative environment. These networks are vulnerable to a wide range of attacks due to the lack of predefined infrastructure and the dynamic topology. Security in ad hoc networks, in general, is handled through authentication and encryption. This can be considered as a heavy way to protect the network due to the lack of resources in the nodes. However, trust can be introduced to address a light weight solution for some security issues. In this paper, we focus on the concept of decentralized trust to design an efficient and trustful routing protocol, and ensure stable routes between nodes in spite of the rapidly changing topology, and to provide a mechanism for detecting malicious incorrect packet forwarding attacks. The proposed light-weight trust-quality routing protocol (TQAODV) provides two main functionalities: monitoring the behavior of the neighboring nodes and computing the trust value based on the historical information in the network. Moreover, the new proposed model reduces routing overhead and route discovery frequency. The simulations we used in NS-2 show that the proposed routing scheme gives better performance against attacks compared to the traditional Ad-hoc On-demand Distance Vector (AODV), and improves the packets delivery ratio with about 15%, routing packets overhead and average delay with about 20%, compared to trust AODV.**

***Index Terms*—AODV, lightweight, routing protocol, Security, Trust, UAANET.**

I. Introduction

A group of Unmanned Aerial Vehicles (UAVs) that connected together through wireless channel without any fixed infrastructure or centralized administration is called UAANET unmanned aerial vehicle ad-hoc network [1].

In recent years, there has been numerous growth in the use of this type of networks, such as emergency rescue operations or area search.

As a category of MANET, UAANET's characteristics, including: frequent changes in network topology due to the mobility or the discontinuous operation of nodes, open wireless media, and constrained capability; these networks are vulnerable to security issues in situations where a friendly and cooperative environment is not assumed [2].

In addition, UAANETs offer self-organized and independent behavior of nodes which may lead to malicious and selfish behavior of nodes [3]. Due to the heterogeneous applications, it is mandatory to assure cooperation between nodes, which leads to the need of security in such networks. Cryptographic techniques are the most known solutions for security, but they demand more resource consumption [4]. Trust management, is an alternative security approach as it introduces less computation and energy requirements than cryptography [6] Hence, it is considered a more appropriate solution.

Latest researches have been proposed for trust management indicating that it can be one of the security solutions for UAANETs against various kinds of attacks [5], because nodes need to have trust on each other in order to accomplish the mission with cooperation and coordination. Therefore, to get a secure and efficient UAANETs, trust management should be well defined and described. Trust management schemes allow a node to assess trustworthiness of other network nodes. A trust management technique helps in detecting malicious and selfish node behavior [7], it also enhances the overall network performance. Trust evaluation in UAANET involves several intricate aspects, like node behavior assessment in terms of reliability and performance, and correct recommendation.

The proposed approach in this paper is a distributed trust management scheme. The trust in UAANET nodes is established by detecting misbehaving nodes that maliciously drop packets. These malicious nodes can be detected utilizing reputation concept. The reputation of a node refers to the perception that another node has about its intention and activities. Reputation is used to ensure cooperation among nodes and increase the good behavior in their activities. At the network initialization step, each node is assigned a default reputation value, then the updated values are jointly computed by its neighbors. The higher the reputation value of a node the more trustworthy that node is. The nodes always collaborate to compute the reputation values of their neighbors and mark them as malicious nodes if their reputation values drop below a pre-defined threshold.

We can summarize our contribution in this paper in the following points:

- New malicious nodes detection method.
- Enhanced reputation calculation.
- Involve distributed trust concept in calculations.
- Improve the overall performance using the proposed method.

Manuscript received November 26, 2020; revised February 18, 2021. Date of publication July 9, 2021. Date of current version July 9, 2021.

Authors are with the Higher Institute for applied scientific and technology, Damascus, Syria (e-mails: {alaa.moualla, oumayma.dakkak, mohamed.aljnidi}@hiast.edu.sy).

Digital Object Identifier (DOI): 10.24138/jcomss-2021-0049

The remaining paper is organized as follows. Section II discusses the related works of trust management schemes in ad hoc networks. Whereas in section III, the details of the proposed trust scheme are described. Section IV presents the simulation and the results of the proposed scheme and the conclusion with future work are given in section V.

II. Related Work

In Recent years, a lot of work has been done in the field of UAANET. Either on its security or its trust management. Concerning security issues, the studies include encryption schemes and key management [9][10]. These techniques are more expensive and inefficient in terms of delay and/or complexity. Whereas, trust management techniques have less complexity and less delay [1]. That's why, trust management is a very reasonable scheme to be studied in UAANET.

Trust as a concept, has been introduced in the network studies since Blaze *et al.* [11] presented trust as an important parameter in network security. Trust management schemes allow network nodes to evaluate their trustworthiness based on their behavior. So, they enhance the overall network performance by isolating selfish nodes which have the lowest trust values. To evaluate the trustworthiness, nodes can either just calculate it, based on direct observation, or consider the nodes prior behavior [12]

This approach can be applied in different networks to secure them using trust management schemes. Lots of studies have also been proposed in this field such as sensor networks [13], IoT [14] and vehicular networks [22].

Singh *et al.* in [15] have proposed fuzzy classification trust based secure clustering scheme (TBCS). The proposed scheme works in highly dynamic environments and uses multi-criteria for classification and optimization to evaluate nodes' trust. But this scheme has more energy consumption. Besides, it assumes a cluster hierarchy for the network, which is lead to single point of failure, i.e. higher probability of network failure.

Mohammed *et al.* [16] analyzed the requirements for efficient UAV communication. They have discussed various trust-based protocols and management schemes that can be used in both UAANET and MANET. However, this work does not consider neither the different mobility patterns nor the energy consumption.

In [17], Yuan *et al.* have presented a trust-based connectivity analysis between the nodes. The link remains valid only if the estimated trust value is higher than a predefined threshold. But, this scheme is just effectively working in high UAVs density cases and has a big establishment delay due to the required learning phase.

Singh *et al.* in [18] have defined a fuzzy classification trust model (FCTM) for UAANET. This scheme is based on nodes behavior and collaboration in the network. Also, it uses social parameters and Quality of Service (QoS) to enhance the trust evaluation. However, this scheme is an entity-centric non distributed approach.

However, in [19] Mattew *et al.* try to Find the neighbors directly from inter-object distances in MANET. This work is effective in the presence of noise, but its computational complexity is in increase. Besides, it has not been studied in UAANET.

Also, Shabut *et al.* [20] have proposed a recommendation-based trust model with clustering technique to dynamically filter out attacks related to dishonest recommendations. The main limitation in it is that the node's past behavior is not considered.

A distributed mechanism to deal with selfish nodes in MANET has been proposed by Li *et al.* [21], which meet the trust requirements of data packets only without considering the routing protocol or the topology of the network.

As we can see from the previous studies, the main concern in UAANET researches is the lacking of security and trustiness, and when this concern is overcome, another issue is raised which is the over usage of resources, i.e. we need much energy and much memory to be in a secure trust network. And that's what we are trying to overcome and reaching a fully trusted network.

In this paper we use Hidden Markov Model (HMM) [22] trust to describe a trust-based distributed technique for UAANET, to overcome the different aforementioned problems including the prevention of selfish node attack.

III. System Model and Proposed Scheme

As UAANET is an ad-hoc network, self-detect misbehaviors cannot be counted as a trust measurement, because node could not be sure that all of its one hop neighbors are normal. However, selfish nodes cannot be detected by nodes that do not send any packets. For that reason, collaboration is mandatory between nodes in a network, each node should monitor the behavior of its neighbors to get their trust value and broadcast it to other neighbors.

The proposed protocol takes into account two main parameters; first the historical data of nodes' trust which leads to more robust values. Second, the broadcasting of nodes' trust is just to one hop neighbors and not the whole network, this leads to much reliability and fault-tolerant routing protocol, without over heading or flooding of the network.

Our trust model technique is illustrated in Figure 1 and can be described as follows;

A. Monitoring Module

Each node will monitor its neighbor's packet forwarding activities. The monitoring process is related to the proportion of correctly forwarded packets with respect to the total number of packets received by that node during a fixed time. That value will be transferred to the trust module in order to analyze it and take the appropriate action as described later.

B. Trust Evaluation Module

The main function of the trust evaluation module is the trust management which involves collecting information, trust calculation and updating values.

B.1. Information collection

In the information collection phase, the values to calculate trust are gathered and stored in the node table as follows. To gather information, we use two aspects:

- Direct monitoring: this aspect is used when node A itself monitors the behavior of its neighbor B as in section 1.

- Indirect monitoring: this aspect represents the perception that node A receives from its neighbors about node B when any node of B's neighbors discover packets dropped exceeding the threshold defined. Using the broadcasting technique would inform the node A about misbehavior of node B.

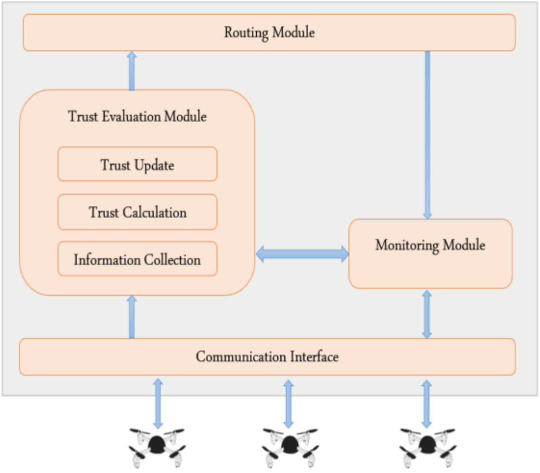

Fig. 1. Proposed System Architecture

The misbehavior of a node is determined using a threshold while monitoring the packet drop. This means when the number of packets being dropped becomes bigger than the threshold, a critical behavior is detected and some new routes need to be computed regardless the intention behind this dropping (malicious action or unintended link broken).

Our proposition only requires interactions with neighbors and stores only information about nearest neighbors because broadcast technique might cause an overload in the network, so we use it in limited range; i.e. the node can broadcast its corresponding information just to its one hop neighbors. This is an important feature to save energy, reduce processing calculations and memory. Each node will have a trust table for its neighbors, which contains two columns, the first one represents the node's neighbor ID and second one represents its trust level based on some calculations (to be clarified later). This table is updated whenever a node's trust is changed as described below. Each entry on the trust table is associated with a timeout. Therefore, an entry is erased from the Trust Table whenever the node associated to that entry is no longer a neighbor or when it expires.

B.2. Trust Calculation

Let's define the trust level for node b from node a as $T_a(b)$ [23] with the following formula

$$T_a(b) = \alpha D_a(b) + (1-\alpha) I_a(b) \qquad (1)$$

This value consists of two parameters. $D_a(b)$ is the direct trust from a about b which represents the trust of b based on a monitoring only. $I_a(b)$ is the indirect trust which represents the recommendations of node a neighbors. α is a parameter between $[0,1]$ to choose the relevant weight of the trust calculation as depending on the direct monitoring or the neighbors' opinion.

The direct trust parameter $D_a(b)$ in turn consists also of two parameters

$$D_a(b) = \beta Q_a(b) + (1-\beta) L_a(b) \qquad (2)$$

where $Q_a(b)$ is the current value of trust from a about b and $L_a(b)$ is the last value reordered in trust table in a about b. In addition, the variable β is between $[0,1]$ and is used to adjust relevant weights.

Due to node's mobility, two nodes may obtain each other trust value without being in adjacent positions. So, an aggregation method is needed to define the whole trust value. But, when using an aggregation method, time and energy will be consumed, so it is important to use as a simpler method as possible to save time and energy. To get an effective simple method, we may use the following formula

$$I_a(b) = \prod_{1}^{n} T_{N_i}(b) \qquad (3)$$

where $T_{N_i}(b)$ is the trust value from neighbor nodes N_i about b.

The value $I_a(b)$ is getting smaller as the neighbors have lower trust values about b, so, any node needs good neighbors reputation to get higher trust value.

B.3. Trust Update

As nodes move rapidly and the topology change dynamically, the nodes may join or leave the network for any reason and the values they have about trust become non valid. So, update trust values for nodes are always needed as old values expire after a specific time period. As seen in the previous section, the trust value is updated whenever a node calculates trust about another node.

If a new node c wants to join the network, node a should calculate its trust value, and since node a does not know anything about c yet, the default value should be assigned in node a trust table. If the value is 1, this means the new node is fully trustful, but this may lead to a vulnerability in the network due to the risk that node c may cause after joining the network and acting as selfish node. On the other hand, if the default trust value of new node is 0, this will lead to completely untrustworthiness node, which may be false prediction as another nodes may know about c. To be in a fair situation, the value of 0.5 is used as a default value. This value will lead to trustfully node if it is healthy, and will lead to low trust value and possible threat if any mal action is done.

C. Routing Module

We define a trustor, who forms and evaluates the trust relationship. A trustee, who performs tasks. Trustor evaluates trust relationship based on those tasks.

To implement routing in the network, we use AODV (Ad hoc On demand Distance Vector) protocol. Each node will add new fields (ID, RC) to the RREQ (route request) message when discovering the route. The new fields represent the trustee ID and the recommendation from trustor about it. This process will help to minimize the route overhead. So, the routing algorithm can be summarized as in Figure 2:

- Let node a , the source, wants to send information to node b which is the destination and nodes $\{c_i\}$ are the intermediate nodes.
- If the path existed, information will be sent from a to b using the routing table in intermediate nodes.
- If the path does not exist, node a will broadcast RREQ message to its neighbors.
- The neighbor of a , the intermediate node c_1 for example, will monitor node a and compute the trust value based on section B-2.
- If the trust value is higher than the threshold, which we defined at the network initialization, i.e. the node is good, node c_1 will add node a to its trust table and rebroadcast the RREQ message to its neighbors after adding the fields $a'ID$ and $a'RC$ to the RREQ.
- The process will be repeated till reaching the destination node b .
- When RREQ is delivered to the destination b , node b will compute trust values for its neighbors and send RREP (route reply) message to the node that have the higher trust value.
- The neighbor of b , which is intermediate node c_2 for example, will compute trust value for node b and send the RREP message to the node which has the highest trust value.
- The reply process will continue till reaching the source node a .
- Now, the path is ready and trusted to transmit data between source and destination.

When any node leaves the network, the neighbor will choose the next node, with the highest value of trust.

IV. Simulation Results

In this section, the simulation environment and results of the proposed trust model are discussed. First, the initial trust level will be optimized. Next, network performance including packet delivery ratio (PDR), routing overhead ratio and delay parameters are evaluated in both normal and malicious environments.

We use NS-2 to simulate the proposed method in 2D environment. The simulation scenario consists of nodes with 250 m transmission range, which follows a random way point mobility model in a 1000 m × 1000 m area.

The other parameters of the environment are summarized in the Table 1.

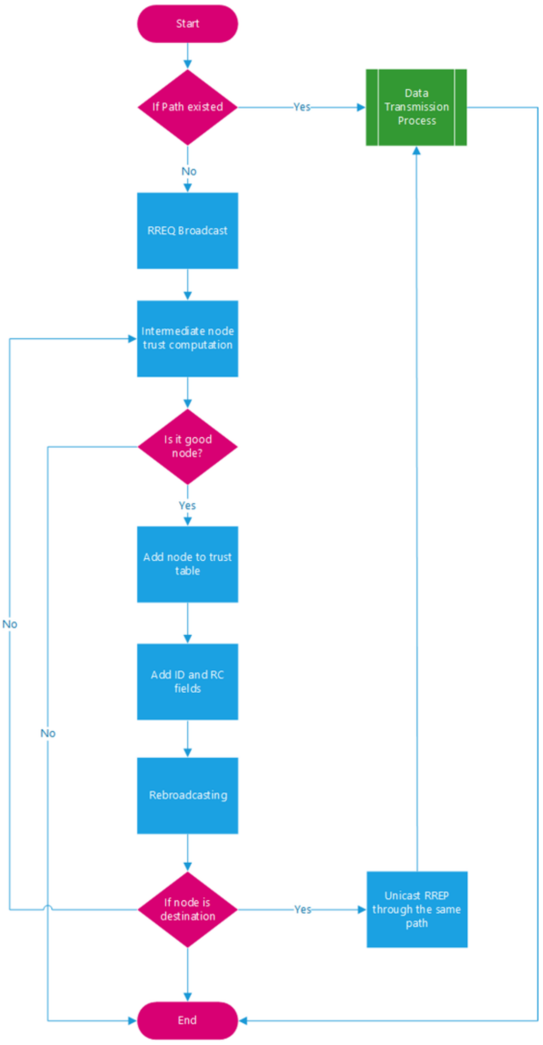

Fig. 2. Proposed Routing Algorithm

TABLE I
THE SIMULATION ENVIRONMENT PARAMETERS

Parameter	Value
Number of nodes	40
Node speed	[0 - 30] m/sec
Mac layer	802.11b
Simulation duration	60 sec
Traffic source	CBR
Channel capacity	2 Mb/sec
Packet size	512 bytes
Default trust value	0.5

A. Trust level

First of all, we define trust level as a range between [0,1] where 1 is a fully trusted and 0 is a fully trustless.

We defined three values for the initiated trust: 0.1 for pessimistic strategy, 0.5 for the moderate, and 0.9 for the optimistic strategy. All nodes adopt the same strategy. Also, all nodes have the same nature (same UAV). Figures 3 and 4 present the average trust level for all neighbors about one node. We have two scenarios, composed of 5 nodes, the initiated trust levels of nodes are [0.1, 0.5, and 0.9] and the trust value for the observed node will be 0.9 for the first scenario and 0.1 for the second scenario. All these scenarios will be done with value $\alpha = 0.5$.

Figure 3 shows the average trust level during simulation period which is 60 sec, in three ways to reach the 0.9 trust value. We can see that the trust level for specific node in pessimistic way starts in low level 0.1 and tends to the expected level 0.9 which is the trust level we have defined for the nodes. Also, we can see that in moderate way the trust level starts in certain level 0.5 and tends to the expected one, whereas in optimistic way the trust level stay around the normal level we have defined 0.9.

We can notice that after 10 sec in the moderate way the trust value stays around the expected value, whereas in the pessimistic way there are about 15 seconds to reach the expected trust value. So, it would be very useful to get this transient shorter to get better results as in the moderate way.

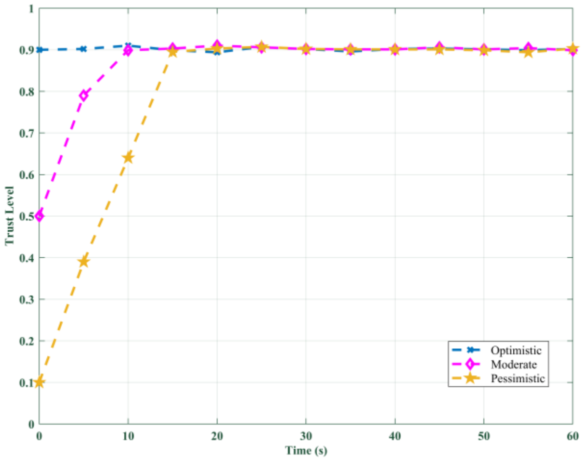

Fig. 3. Trust level prediction for healthy nodes vs Time

In Figure 4, the scenario is done to reach 0.1 trust value in the same three ways during 60 seconds. In the optimistic way, there is about 18 seconds to reach the correct trust value, whereas there is about 10 seconds in the moderate way. And we notice that the trust value stayed around the correct value 0.1 in the pessimistic way. Also, in this scenario we can notice that the moderate way is the best in comparison with the other ways because optimistic and pessimistic ways are working by contrast against each other.

So, as a result, we should define a moderate trust value as a default value for all nodes in the network in order to save time and get better performance. Now, we move on to study the network performance using our proposed method in both healthy networks and malicious ones, i.e. when there are malicious nodes in the network. To do so, we use 4 scenarios and implement them in the network.

The first scenario is in healthy network which all nodes with a speed of 5 m/s. The second scenario is also in healthy network, but with nodes speed 30 m/s. then we combine the results of the previous two scenarios to get the network performance when the nodes speed change between 5 – 30 m/s.

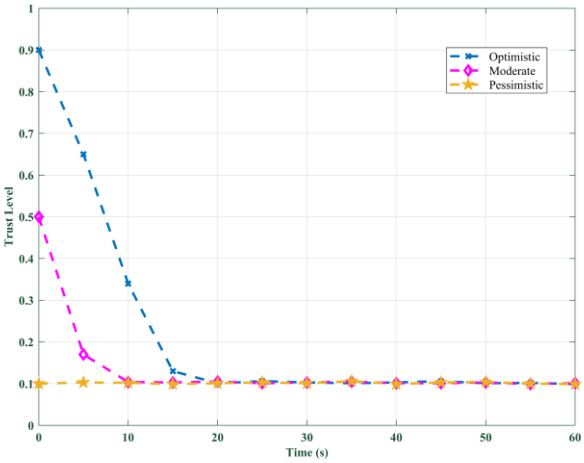

Fig. 4. Trust level prediction for malicious nodes vs Time

The third scenario would be in a malicious network. Here we define just 2 nodes as malicious nodes and measure the overall performance. While the forth scenario in a malicious network with 10 malicious nodes. Also, we combine the results to get the overall vision of the network performance in case there are malicious nodes.

We use the following parameters: packet delivery ratio, End to End Delay and routing overhead. Then, we compare our results with other results when using traditional AODV and TAODV [24], which are standard protocols to compare with.

V. Packet Delivery Ratio

Figure 5 presents the packet delivery ration (PDR) in healthy network using three methods (traditional AODV, TAODV and the proposed method). The PDR is calculated in various nodes speed value. As we see, the traditional AODV gives about 80% as PDR, and it is getting lower as the nodes move faster to reach about 67% when speed is 30m/s. on the other hand, TAODV gives about 82% at the beginning, and descends to 79% at speed 30 m/s, Whereas in our proposed scheme the enhancement comparing AODV is about 5% at the speed of 5m/s, and the enhancement increases to about 18% at speed 30 m/s. compared with TAODV, our proposed method is better in 2.5% almost at all speed range from 5 to 30 m/s.

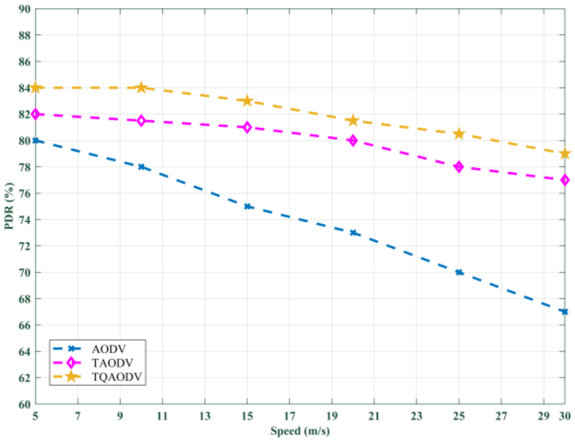

Fig. 5. Packet Delivery Ratio for healthy nodes vs Speed

In Figure 6, we can find the PDR in malicious network using also the three methods. When using traditional AODV, we see that the PDR is greatly getting lower when the number of malicious nodes increase, Whereas in TAODV, the PDR is staring about 82% in healthy network, and drops to 66% when there are 10 malicious nodes. In our proposed method, the PDR is better in 2.5% in healthy network and is improved by about 15% when there are 10 malicious nodes, which leads to say that our method can work efficiently in malicious networks rather than AODV or TAODV.

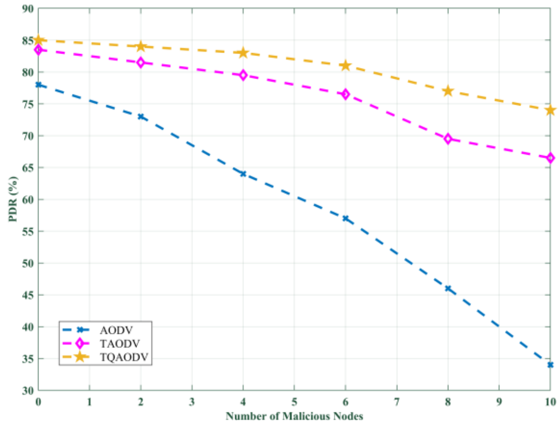

Fig. 6. Packet Delivery Ratio vs Number of malicious nodes

VI. Routing Overhead

The results of measuring routing overhead parameter in simulation are shown in Figure 7. For healthy network, as we increase speed we can see that our proposal is better than TAODV by 21% when nodes move in 5 m/sec. when nodes reach to 30 m/sec, our proposal is better with 18.5%.

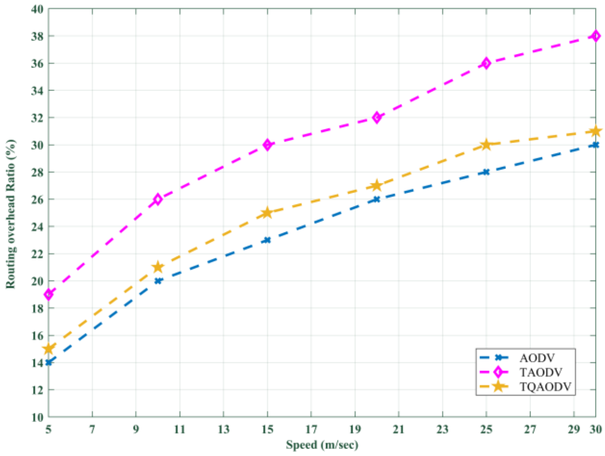

Fig. 7. Routing Overhead Ratio for healthy nodes vs Speed

In Figure 8, in a malicious network, we can find that our proposed is getting better as the number of malicious nodes is increased. The enhancement is about 19% in healthy network and increases to 23.5% when 10 malicious nodes are in the network.

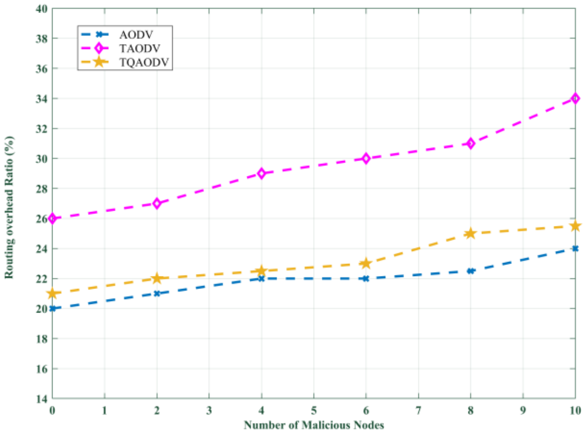

Fig. 8. Routing Overhead Ratio vs Number of malicious nodes

VII. End to End Delay:

Figure 9, shows that the enhancement in End to End Delay, using our proposed method is about 8.5% compared to AODV and about 6% compared to TAODV when the nodes speed is 30 m/sec in healthy network.

In Figure 10, we see that the enhancement in malicious network is increased by about 27% compared to AODV and by about 11% compared to TAODV in the presence of 10 malicious nodes in the network.

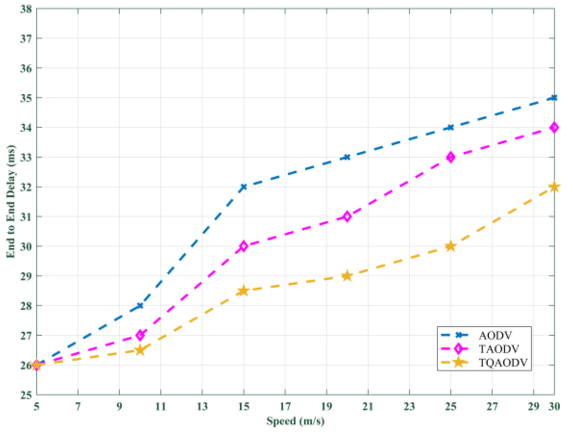

Fig. 9. Average End to End Delay for healthy nodes vs Speed

VIII. Conclusion and Future Research

In this paper, we have provided an efficient and trust routing protocol for UAANET, through proposing a flexible trust scheme based on historical information, which provides nodes with a mechanism to evaluate the trust level of its neighbors. The basic idea is to use packet forwarding historical information and recommendations of other neighbors to calculate the trust level of other nodes. The performance of the proposed protocol, as given above, indicates that we have got better results compared to trust AODV in terms of packet delivery ratio, End to End Delay and routing overhead.

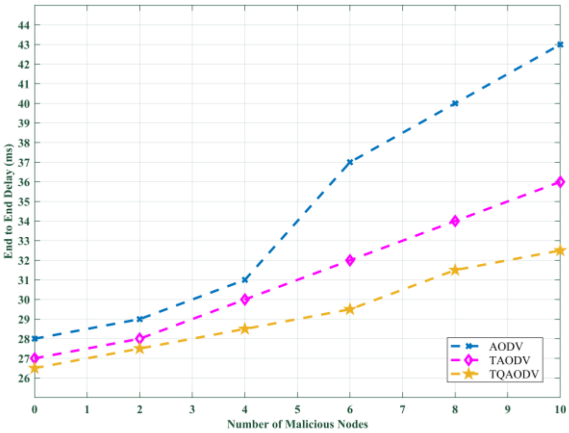

Fig. 10. Average End to End Delay vs Number of malicious nodes

The packet delivery ratio is getting increased 15%, while the end to end delay is decreasing 7% and the overhead is decreasing 19%. As future works, first, 3D movements considerations will be added. Second, we plan to add special security mechanism to the proposed scheme that will allow to enhance the overall performance of the system without overloading the nodes. Then we can compare our proposal with a big variants of other protocols and increase the measurement parameters in both sides (trust and security). Hence, we seek to get a complete efficient secure and trusted protocol in UAANET.

REFERENCES

[1] Singh, Kuldeep & Verma, Anil & Aggarwal, Palvi. (2018), "Analysis of Various Trust Computation Methods: A Step toward Secure FANETs," DOI: 10.1201/9780429424878-7.

[2] Ezedin Barka, "A Trusted Lightweight Communication Strategy for Flying Named Data Networking". *sensors 2018, 18, 2683*; DOI:10.3390/s18082683

[3] Sentürk, E. (2016)," Security Issues in Flying Ad-hoc Networks (fanets)," *Journal of Aeronautics and Space Technologies, 9(2), 13-21*

[4] Janani V S and Manikandan, "Efficient trust management with Bayesian Evidence theorem to secure public key infrastructure-based mobile ad hoc networks," *EURASIP Journal on Wireless Communications and Networking (2018) 2018:25, Springer*, DOI 10.1186/s13638-017-1001-5

[5] Akbani, R., Korkmaz, T., & Raju, G. V. S. (2012), "Mobile ad-hoc networks security," *In Recent Advances in Computer Science and Information Engineering (pp. 659-666). Springer Berlin Heidelberg.*

[6] E. Barka, C. Kerrache , N. Lagraa, A. Lakas, T. Calafate and J-C. Cano. "UNION: A Trust Model Distinguishing Intentional and Unintentional Misbehavior in Inter-UAV Communication" *(2018)*

[7] Jhaveri RH, Patel NM, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks". Int J Commun Syst. 2017;30(7)

[8] K. Singh and A. K. Verma, "A Trust Model for Effective Cooperation in Flying Ad Hoc Networks Using Genetic Algorithm," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 0491-0495, doi: 10.1109/ICCSP.2018.8524558.

[9] Altawy, R., & Youssef, A. M. (2016). Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. ACM Transactions on Cyber-Physical Systems, 1(2).

[10] Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Homeland Security (HST), 2012 IEEE Conference on Technologies for (pp. 585-590). IEEE

[11] Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized trust management. In Proceedings 1996 IEEE symposium on security and privacy (pp. 164–173). IEEE

[12] Ashraf, S. (2019). Culminate Coverage for Sensor Network through Bodacious-Instance Mechanism. *i-manager's Journal on Wireless Communication Networks* , 8(3), 1-9. https://doi.org/10.26634/jwcn.8.3.17310

[13] GD Devanagavi, N Nalini, RC Biradar, "Secured routing in wireless sensor networks using fault-free and trusted nodes". International Journal of Communication Systems, 2016

[14] Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: a trust management model based on fuzzy reputation for internet of things," Computer Science and Information Systems, vol. 8, no. 4, pp. 1207–1228, 2011.

[15] Singh, K., Verma, A.K. TBCS: A Trust Based Clustering Scheme for Secure Communication in Flying Ad-Hoc Networks. Wireless Pers Commun (2020). https://doi.org/10.1007/s11277-020-07523-8

[16] Mohammed, F.; Jawhar, I.; Mohamed, N.; Idries, A. Towards trusted and efficient UAV-Based communication. IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 388–393

[17] Yuan, X.; Wei, Z.; Feng, Z.; Xu, W. Trust connectivity analysis in overlaid unmanned aerial vehicle networks. In Proceedings of the 2017 17th International Symposium on Communications and Information Technologies (ISCIT), Cairns, QLD, Australia, 25-27 September 2017; pp. 1–6

[18] Singh, K.; Verma, A.K. FCTM: A Novel Fuzzy Classification Trust Model for Enhancing Reliability in Flying Ad hoc Networks (FANETs). Adhoc Sens. Wirel. Netw. 2018, 40, 23–47.

[19] ML Elwin, RA Freeman, KM Lynch, Distributed Voronoi neighbor identification from inter-robot distances. IEEE Robot. Autom. Lett. 2(3), 1320–1327 (2017)

[20] A.M Shabut, K.P Dahal, S.K Bista, I.U Awan, Recommendation based trust model with an effective defense scheme for MANETs, IEEE Trans. Mob. Comput. 14(10), 2101–2115 2015

[21] X. Li, Z. Jia, P. Zhang, R. Zhang and H. Wang, "Trust-based on demand multipath routing in mobile ad hoc networks," IET Information Security, 2010

[22] K. X. Ouyang, B. Vaidya and D. Makrakis, "A Probabilistic-Based Trust Evaluation Model Using Hidden Markov Models and Bonus Malus Systems". 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing, Boston, MA, 2011, pp. 1004-1011, doi: 10.1109/PASSAT/SocialCom.2011.35.

[23] S. Ashraf, M. Gao, Z. Chen, H. Naeem, A. Ahmad and T. Ahmed, "Underwater Pragmatic Routing Approach Through Packet Reverberation Mechanism," in *IEEE Access*, vol. 8, pp. 163091-163114, 2020, doi: 10.1109/ACCESS.2020.3022565.

[24] Kajal S. Patel, "Trust based Routing to avoid malicious nodes in MANET " International Journal of Control Theory and Applications 9(21), 2016, pp. 105-110, September, 2016.

Moualla, Alaa has Engineering Degree in Telecommunication Systems, from the Higher Institute of Applied Sciences and Technology (HIAST), Damascus, Syria, 2007. Master Degree in Computer Networks from the Higher Institute of Applied Sciences and Technology (HIAST), Damascus, Syria, 2016. A PhD student in Communication Network Security in HIAST also.

He has interests in Cryptography and Network Security and teaches these subjects in "Communication Systems" master in HIAST as an assistant teacher, in addition to his interests in communication, Information and Data Processing. He is a teacher at the Higher Institute of Applied Sciences and Technology (HIAST), Damascus University and And in the Syrian Virtual University (SVU).

Al Dakkak, Oumayma has Engineering Degree in Systems' Electronics, National High School of Electronics and Radio-Electricity in Grenoble (ENSERG), France, 1985. Postgraduate Degree (DEA) in Electronic Systems (ENSERG), France, 1985 also. A PhD in Electronic Systems from "Speech Communication Institute/Institut de la Communication Parlée"- "Institut National Polytechniques de, Grenoble" (ICP-INPG), France, 1988.

She has interests in Cryptography and Data Security and teaches theses subjects in "Communication Sytems" master in HIAST, in addition to her interests in Speech and Natural Language Processing domain, and Arabic Language Resources. Prof. Al Dakkak is a Research Director at Higher Institute for Applied Sciences and Technology HIAST, Lecturer at the Information Technology Engineering Faculty, Damascus University. And in the Syrian Virtual University (SVU). She is Member of Syrian Computer Society, and a Member of ISCA-WANA sub-committee since 2006. Also, Head of Communication Department in HIAST (2007-2014).

ALjnidi, Mohamad has Engineering Degree in Compyter Science from the Higher Institute of Applied Sciences and Technology (HIAST), Damascus, Syria, 1996. Master Degree in Computer Networks from Pierre et Marie Curie University (Paris VI), Paris, France, 2005. And a PhD in Computer Network Security from TELECOM ParisTech (ENST: Ecole Nationale Superieurs des Telecommunications), Paris, France, 2009. He has interests in Information and Network Security and teaches theses subjects in "Communication Sytems" Master in the Higher Insttute of Applied Sciences and Technology (HIAST), in addition to his interests in Autonomic Communications, Software Defined Networks and Cloud Computing. He is an assistant professor at the Higher Insttute of Applied Sciences and Technology (HIAST), the Arab Academy for E-Business (ARAEB), and the Syrian Virtual University (SVU). He is a Member of the administrative committee in the Syrian Computer Society (SCS).