Analysing the fairness of trust-based Mobile Ad Hoc Network protocols

Comparing the fairness of AODV and TAODV protocols in scenario driven simulations

Ivan Daniel Burke
Department of Computer Science
University of Pretoria
Pretoria, South Africa
iburke@csir.co.za

Renier van Heerden
Command, Control and Information Warfare, Defence, Peace, Safety and Security
Council for Scientific and Industrial Research
Pretoria, South Africa
rvanheerden@csir.co.za

Martin S Olivier
Department of Computer Science
University of Pretoria
Pretoria, South Africa
moliver@cs.up.ac.za

Abstract— **A Mobile Ad hoc Network (MANET) consists out of a collection of mobile nodes capable of sending and/or receiving wireless communications. MANETs are generally unstructured networks with no centralized administration. MANETs use routing algorithms to establish routes among nodes. This unstructured nature presents the opportunity for misbehaviour among nodes.**

Trust based MANET routing protocols have been developed to counteract malicious behaviour, in an effort to establish fair node behaviour. Recent research has shown that the trust protocols themselves introduce unfair behaviour among nodes.

This paper presents basic MANET scenarios and monitors the fairness of TAODV and TEA-AODV routing protocols.

Keyword: MANET; fairness; TAODV; TEA-AODV

I. INTRODUCTION.

A Mobile Ad hoc Network (MANET) consists out of a collection of mobile nodes capable of sending and/or receiving wireless communications [1]. Each node within the network acts either as a sender, receiver or intermediate node during transmission [2]. This eliminates the need for centralised administration. This open nature of MANET communications makes it an attractive option for military and peace relief operations where pre-existing infrastructures are either damaged or none existent [1].

The lack of centralised administration makes MANETs a target for network attacks and node misbehaviour [3]. Each node has limited resources and by acting selfishly they can optimise their gain at the cost of the other network nodes, resulting in an iterative Prisoner's dilemma [4]. Trust based protocols have been introduced to counter node misbehaviour [5], [6], [7]. These trust based protocols negatively influence the Quality of Service within the network [8]. Recent research has shown that edge nodes within MANETs tend to be unfairly penalized by these trust algorithms due to their typographical location within the network [5], [8].

In this paper, a scenario-based analysis is performed between Trusted Ad hoc On Demand Distance Vector Routing (TAODV) and Trusted Energy Aware Ad hoc On Demand Distance Vector Routing (TEA-AODV) with regard to fair treatment of trustworthy nodes.

The remainder of the paper is structured as follows: Section II provides a motivation for the need of fairness within MANET networks. Section III, takes a look at related protocols and proposed addendums to existing protocols. Section IV describes the criteria for evaluating fairness within the context of this paper. Section V describes the results of each protocol selected for evaluation, the paper concludes in Section VI.

II. MOTIVATION.

Reference [10] describes different levels of a computer network user's needs with a pyramid, based on Maslow's Pyramid of basic human needs [11]. Fig. 1 illustrates their model.

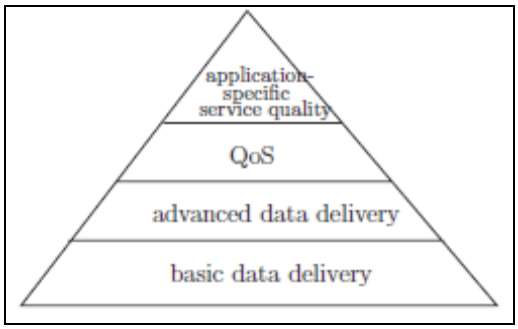

Figure 1 Pyramid of user's needs in computer networks.

At the bottom and most basic level, basic data delivery is all that is required. A simple example of this would be the delivery of email. On the second level, advance data delivery is required. This means that basic two-way communication is possible, for example the interaction with the WWW, where data is received and transmitted among participating agents. The third level, introduces quality of service, this includes real-time streaming of video and audio data. The final level is a

more specialized level which not only provides the service at the required quality levels but also requires each user of the application equal opportunity to the application resources. Examples of these type of systems would be e-trade, e-voting and large scale online gaming.

The work done in [10] states that the bottom three levels serve as prerequisite for fair network behaviour as it is forms the basis for data communications. Their paper further introduces several mechanisms to monitor misbehaviour and award fair network usage.

Within wireless networks the problem is slightly more complex. Wireless networks are not only limited by the same fairness constraints of physical networks, they also have a limited battery-life, limited computing power, a shared communication medium, connectivity issues and, in the case of MANETs, they also have no centralized control within the network to regulate and monitor data flow.

In the work done by [9], it can be seen that trust management can act as an incentive for fair agent behaviour in online trade systems. Reference [9] describes trust as an iterative prisoner's dilemma, whereby agents receive improved payoffs if they collaborate. Reference [9] proves that by simply introducing a tit for tat trust system, fairness emerges within the online trading system. Similarly trust can be used by MANET networks which operate in the same setting of uncertainty and mistrust [5] [6] [7].

Reference [12] describes a mechanism used to determine an agent's trustworthiness in a purely distributed system without the aid of a centralized control. Reference [12] builds on the work done earlier by [9] in attempting to illustrate fairness emergence through trust management. Both these models are based on online trading reputation systems and the author's attempt to identify misbehaving agents and by introducing a new reputation algorithm which promotes fair behaviour among nodes.

A trustworthy agent might not just be mistreated by misbehaving agents. According to [13] reputation management systems themselves can also be a barrier to fair agent treatment. In [13], six problems with current reputation systems where identified:

- Equations that do not accurately identify the current reputation of agents.
- Starting reputation is set too low, which acts as a barrier to new entries into the network.
- There is no incentive to rate peers.
- There is no ability to filter or search by reputation score.
- Use of a single general reputation system.
- Most systems have an unlimited memory.

The problems identified by [13] are targeted at online trading systems specifically, but in Section V, we will adapt these problems to be more suited for MANET networks. By using the newly formulated problems, we will evaluate the performance of well known MANET trust based protocols against these problems as criteria for fairness evaluation.

In the next Section we review some related protocols and protocol addendums.

III. Related Protocols.

It has been suggested that Public Key Encryption (PKI) could solve the current trust issues in MANET networks as well as serve as a mechanism to increase trust within the network [14] [15] [16]. Reference [17] produced a report comparing cryptographic MANET protocols to trust based protocols. Based on the report, cryptographic techniques often require a third party certificate authoring and authentication service or a pre-deployment sharing of public keys. This contradicts the ad hoc nature of MANET networks and limits the application of the network. Furthermore result also indicated that secure routing requires more overhead per-packet. Secure Ad hoc On Demand Distance Vector Routing (SAODV) had 2.125 times more per-packet overhead than Trust based AODV, and 2.35 times more overhead than standard ADOV. The additional overhead caused increased battery usage and reduces the overall lifespan of the agent. Decreasing agent lifespan might lead to targeted Denial of Service (DoS) attacks. Hence higher security via cryptography might result in a higher risk of DoS attacks. Reference [18] and [19] describes cryptographic systems which are scaleable to the specific security versus risk of DoS trade-offs expected within the network.

The remainder of the related protocols will be discussed use trust as the basis for security. The reason for this is primarily the high overhead requirements of cryptographic techniques and their reliance on third party certificate authoring mechanisms. We will specifically focus on the two trust algorithms that will be tested in Section V.

Trust based AODV, as proposed by [20], represents trust as subjective logic. According to subjective logic an opinion is comprised of a triplet that consist out of, Belief (*b*), Disbelief (*d*) and Uncertainty (*u*) as illustrated in Fig.2.

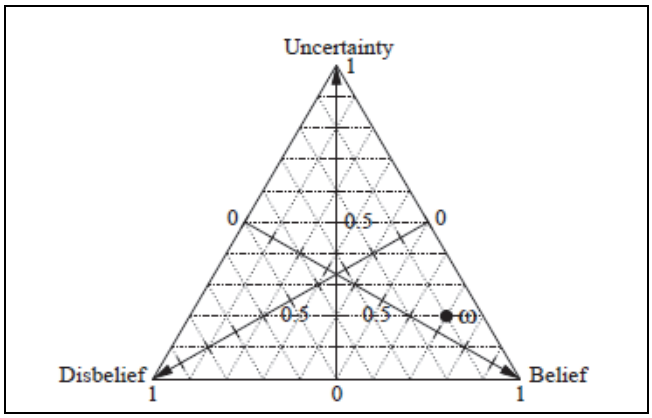

Figure 2 : Opinion triangle

$$Let\ \omega_B^A = (b_B^A, d_B^A, u_B^A) \quad (1)$$

Equation (1) describe

agent A's subjective opinion of agent B as the sum of its belief, disbelief and uncertainty in B based on prior experience with B.

$$\begin{cases} b_B^A &= \frac{p}{p+n+2} \\ d_B^A &= \frac{n}{p+n+2} \\ u_B^A &= \frac{2}{p+n+2} \end{cases} , where \quad u_B^A \neq 0. \tag{2}$$

Equation (2) illustrates how each of the values, within the opinion equation is determined. Let *p* and *n* respectively be the positive and negative evidence collected by A about B's trustworthiness.

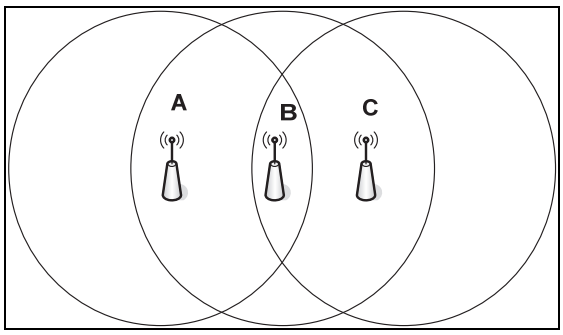

Figure 3 : Multi-hop connection

In the case of a multi-hop connection, as illustrated in Fig. 3, if A wants to communicate to C, A can only achieve this connection by first connecting to B and having B forward the message on A's behalf to C. A uses discounting combination, as defined by subjective logic [21], to combine its opinion of B with that of C, as illustrated in (3)

$$\begin{cases} b_C^{AB} &= b_B^A b_C^B \\ d_C^{AB} &= b_B^A d_C^B \\ u_C^{AB} &= d_B^A + u_B^A + b_B^A u_C^B \end{cases} \tag{3}$$

TAODV uses these triplets to make judgments about how it should respond to routing requests from various agents in the network. Table I, depicts the judgement criteria used in TAODV.

Table I : Criteria for judging trustworthiness

Belief	Disbelief	Uncertainty	Actions
		>0.5	Request and verify digital signature
	>0.5		Distrust agent for an expire time
>0.5			Trust agent and continue routing
≤ 0.5	≤ 0.5	≤ 0.5	Request and verify digital signature

During initial start-up A has no opinion of B and initializes its trust values to (0, 0, 1) as per (1).

TEA-AODV is an energy aware adaption of standard TAODV implementation, proposed by [22]. TAODV does not consider the energy level of agents within the MANET when judging an agent's trustworthiness. The battery life of an agent can adversely affect its capability to forward packets, as a result an agent's trustworthiness is negatively influenced. Reference [22] suggests that, by introducing a mechanism to combine energy levels and trustworthiness of a proposed route, in doing so they determine the reliability of the route.

TEA-AODV alters the way in which trustworthiness is measured in TAODV. The new trust scheme is based on the number of packets received or sent to neighbouring agents. An agent is classified as a stranger (*S*), if the agent has never sent or received any packets from the neighbouring agents. An agent is classified as an acquaintance (*A*), if the agent has sent or received a few packets from the neighbouring agent. An agent is classified as a friend (*F*), if the agent has sent or received many packets from the neighbouring agent. The protocol does not specify a specific quantitative value for each of the qualitative statements many and few. It does suggest that these values are determined by the length of agent association and the number of packets sent during the association interval. For the purposes of this paper these values will be determined as per Table II.

Table II : trust estimation as defined by TEA-AODV

Trust Level	Num. Packets / Transmission Interval (*s*)	Trust Value
F	>0.7	0.7-1.0
A	≥ 0.3and ≤ 0.7	0.3-0.7
S	<0.3	0-0.3

TEA-AODV uses a second metric remaining battery power, to determine the reliability of suggested path. The power consumption is calculated as follows within TEA-AODV. Power consumed during transmission is calculated with (4), with P_t, the power required to transmit a single packet, and T as the transmission time. T can be calculated using (5). Power consumed during data reception can be calculated similarly with (6), with Pr being the power required to receive a single packet.

$$\text{Consumed Energy During Transmission} = P_t \times T \tag{4}$$

$$T = \text{Data size} / \text{Data rate} \tag{5}$$

$$\text{Consumed Energy During Reception} = P_r \times T \tag{6}$$

By combining these metrics a Reliability relation is derived as per Table III. If the reliability of the route request is lower or equal to 0, the route request is discarded. In the case of a multi-hop route, the reliability is determined by the sum of all agents within the route and divided by the number of hops taken, to form a combination reliability relationship.

Table III : Reliability value for each agent

Trust value	Remaining Energy %	Reliability	Reliability value
0.7-1.0	80-100	Very, very high	1.0
0.4-0.6	80-100	Very high	0.8
0.7-1.0	50-79	High	0.6
0.4-0.6	50-79	Medium	0.4
0.0-0.3	50-100	Low	0.2
N/A	0-49	Very low	0.0

In this section we discussed some of the current trust based MANET protocols. TAODV and TEA-AODV, were discussed in greater details as their fairness will be evaluated in Section V. The reason for specifically using these algorithms is because they rely purely on trust as the basis for secure communication. In the following Section, we discuss the criteria for constituting fair agent behaviour.

IV. Evaluation Criteria.

In Section II, we discussed some of the motivation for fairness in trust based reputation systems. Specifically we mentioned [13]'s problems identified with online trade systems. In this section we elaborate on these problems and tailor them to better fit the MANET domain. We also identify additional problems with trust based systems specific to the MANET domain. After describing each problem we propose a scenario based test to evaluate each trust based protocols performance against each problem identified.

A. Equations that do not accurately trustworthiness.

Due to the nature of wireless networks, connections are not always stable, they are affected by topology, geographic barriers, signal strength and temporal events [1], [3], [7], [19], [20]. Hence, it is fairly difficult to accurately measure misbehaviour if all of these parameters are not taken into account.

B. Starting reputation is too low and may act as a barrier to new agents.

In most trust based reputation systems, agents start with an initial trust value of 0 [4], [9], [10], [13], [22].This makes it difficult to improve gain trust if the agent is never permitted to engage in the network communications due to low trust.

C. No incentive to rate peers.

By transmitting one's opinion about neighbouring agents, limits ones own resources such as battery power and time to transmit. It would be better for agents to not advertise routing or trust information at the cost of their own battery power.

D. Inability to filter by reputation.

In Mobile networks there may be scenarios whereby there is only a single routing path. Trust based systems must strive to always use the most trusted path available, [10] describes basic data transfer as the most basic need of computer networks. Based on the urgency of a message it may, in certain scenarios, be acceptable to send data via a less trustworthy route. The routing protocol should be able to cater for such scenarios.

E. Use of a single general reputation system.

MANET routing is a multi-dimensional problem. As such an agent's trust can not fairly be judged by a single metric, which does not reflect the full situation of the agent.

F. Unlimited memory.

Trust based systems use the full transaction history as basis of trustworthiness. Reference [4], [9] and [12], identified scenarios where agents would only misbehave for a small subset of transactions, but due to the reputation system's unlimited memory of transactions the average reputation would still reflect as trustworthy. Conversely if an agent seemingly misbehaved during initial interaction, it will remain accountable for these failed transactions for the remainder of its communications.

To evaluate the fairness based on the aforementioned criteria, three scenarios will now be described to test each of the protocols. The agents are simulated in NS-2.34. The agent setup can be seen in Table IV. Each scenario is simplistic and tries to determine the root cause of unfair treatment; hence we will simulate specific agent interactions without the clutter of a complex network setup.

Antenna model	Omni Directional
Propagation model	Two Ray Ground
Transmission range at full battery power	200 m
Distance between agents	180 m
Source packet rate	4 packets/s
Source data packet size	512 bytes
Initial battery power	3.6 Watts
Transmission power consumption	280 mA
Receiving power consumption	180 mA

Scenario 1 – Two agents will be placed within communication range of each other, as illustrated by Fig. 4. The agents will start continuous communication at t = 0s. All agents in this scenario act completely trustworthy to the best of its capabilities. The scenario will continue to run until one of the agents run out of battery power. The goal of this scenario is to show the initial ramp up time of each protocol as well as illustrate how they respond to ever decreasing transmission strength.

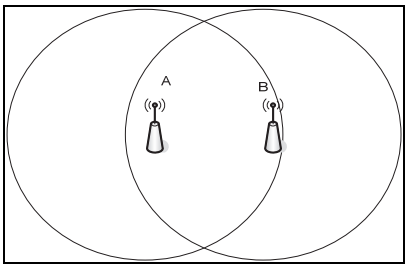

Figure 4 : Scenario 1

Scenario 2 – Three agents, A, B and C are placed within communication range, as illustrated in Fig. 5. At t = 60s a new agent, D, is introduced to the system.

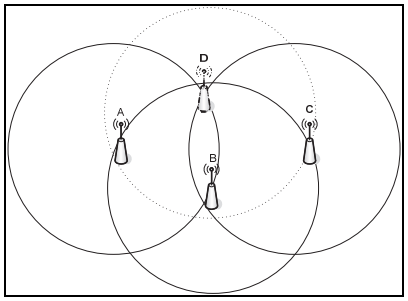

Figure 5 : Scenario 2

All agents within the system, except D, start communicating randomly to each other during the execution run, starting at t = 0s. At t = 60s, agent D joins the network, it does not transmit its own data but acts as a new source to route data from A to C. All agents in this scenario act completely trustworthy to the best of its capabilities. The goal with this scenario is to demonstrate the capability for a new agent to join the network.

Scenario 3 – Two agents will be placed within communication range of each other, as illustrated by Fig. 6. The agents will start continuous communication at t = 0s. In this scenario agent B has a 10% probability to misbehave. The scenario will continue to run until one of the agents run out of battery power. The goal of this experiment is to test how long it takes for the protocol to detect a partially misbehaving node.

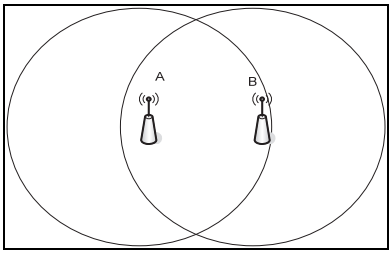

Figure 6 : Scenario 3

Each of these scenarios addresses a different aspect of the fairness of trust algorithm problem. In the next section we will evaluate the performance of TAODV and TEA-AODV in each of these scenarios.

It should be noted that these scenarios are rather basic in their design yet they are specifically designed to evaluate certain conditions within the MANET network. The results we aim to achieve by creating such basic scenarios often get obfuscated within very large simulations.

V. PROTOCOL EVALUATION

In this section each protocol will be run in each of the scenarios discussed in the previous section. The results will be presented and analysed according to the criteria specified in Section IV.

A. TAODV

1) Scenario 1

Fig. 7, depicts agent A's opinion of agent B in scenario 1, using TAODV. Table IV, compares the probability of packet delivery to the current belief in agent B.

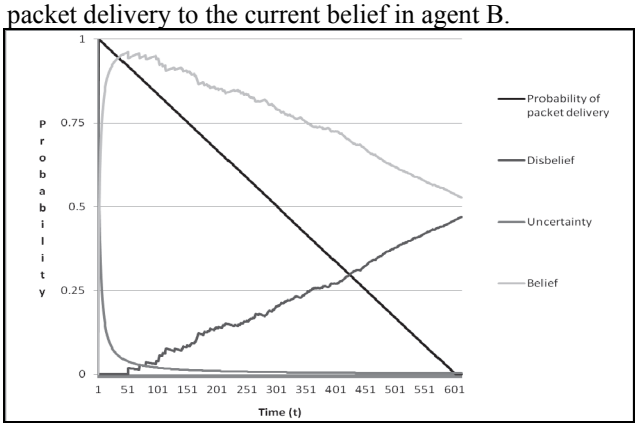

Figure 7 : Agent A's opinion of B in Scenario 1 using TAODV

Table IV : TAODV- Packet delivery Probability versus Agent Belief

Time (t)	Packet delivery probability	Belief value
1	1.00	0.333
153	0.75	0.901
298	0.50	0.788
443	0.25	0.689
601	0.0	0.536

As can be seen by Table IV, at initial packet transfer, t = 1s, agent A's opinion of B is lower than the required threshold of 0.5 to be trusted. According to Table 1, because the uncertainty level is greater than 0.5 the packet is not rejected but both agents are requested to verify their digital signatures. Within the first 3 packet transfers agent A's opinion of B becomes high enough to classify it as trustworthy and continues communication as normal. At t = 601s, both agents are at too low power to cover the communication distance of 180 meters. At t = 601s, A still has more than a 50% trust in agent B. According to Table VI, A's opinion of B does not accurately depict the true probability of packet delivery. Furthermore, A and B both act as honestly as possibly given their constraints, yet by purely judging the reputation values, it appears as if B acts increasingly dishonest. This is due to diminishing battery power and not due to any misbehaviour on B's part. By only taking successful communications into account A is unaware that the misbehaviour is due to diminishing battery power and as a result may unfairly judge the behaviour of B.

2) Scenario 2

Fig. 8 shows the results of scenario 2, while using the TAODV protocol. Agent D is only introduced at t = 60s. According to Table V, even though D is introduced to the network at t = 60s, it is not chosen as the routing agent

between A and C till, B has become untrustworthy, trust < 0.5, at t = 191s.At t = 60s, in a fair system D should have been selected as routing agent as it had the highest probability of successfully delivering the packet to C. Agent D was the more reliable routing option but was rejected by the trust algorithm due to the barrier of new entry. At t = 191s, D's probability of delivering the data has been reduced to just 0.767 due to agent D responding to route requests from A, which drained its battery power. This decrease in probability shows the price paid by D for acting trustworthy and advertising its ability to route the packets.

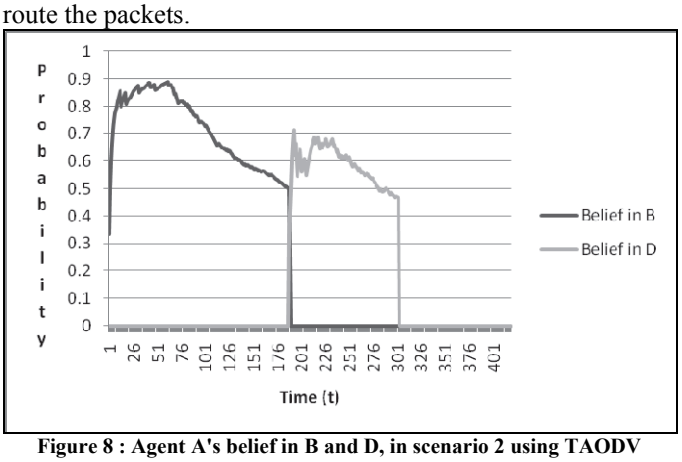

Figure 8 : Agent A's belief in B and D, in scenario 2 using TAODV

Table V: Scenario 2 test results using TAODV

Time (t)	Belief in B	Probability B	Belief in D	Probability D
60s	0.74	0.833	0.0	1.0
191s	0.494	0.0	0.333	0.767

3) Scenario 3

Fig. 9 shows the results of scenario 3, while using the TAODV protocol. Agent B misbehaved 10% of the time yet it was only detected as misbehaving, belief < 0.5, at t = 533s. In scenario 1, agent A's trust in agent B, which was acting 100% trustworthy, was only evaluated as 0.56 trustworthy. According to these finding the agents opinion of B was affected more by the loss of signal strength than by the deliberate misbehaviour of B. At t = 534s, the triplet is reset to (0,0,1) as per protocol specifications. At t = 546s, a single packet was successfully transmitted, which triggered the sudden spike between t = 546s and t = 549s. This solitary packet transfer was quickly deemed untrustworthy by the algorithm and the triplet was again reset to (0,0,1), where it remained till the battery power was deemed too low to cover the transmission distance, at t = 603s.

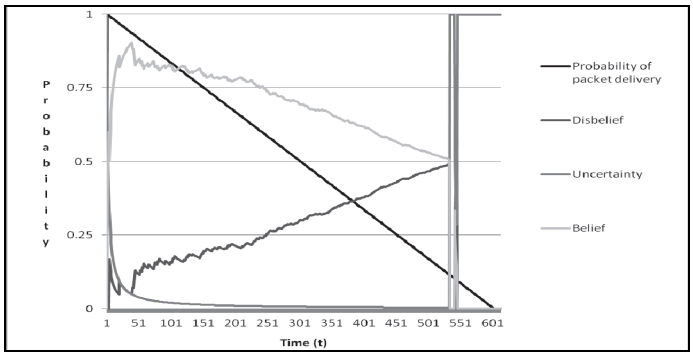

Figure 9 : Agent A's opinion of B in Scenario 3 using TAODV

B. TEA-AODV

1) Scenario 1

Fig. 10, depicts agent A's opinion of B's reliability in scenario 1. Table VI, compares the probability of packet delivery to the current reliability rating of agent B.

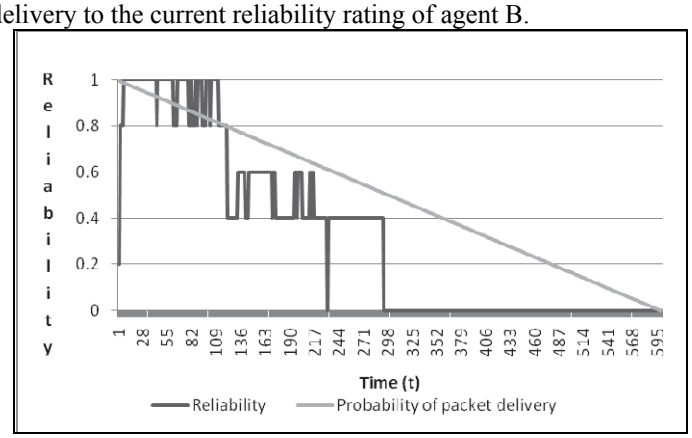

Figure 10 : Agent A's opinion of B in Scenario 1 using TEA-AODV

Table VI - Packet delivery Probability versus Reliability

Time (t)	Packet delivery probability	Reliability value
1	1	0.2
153	0.75	0.6
307	0.5	0
447	0.25	0
507	0.0	0

At t = 1s, the reliability of B is classified as *Low,* the battery power might be high but A views B as a stranger, due to the lack of prior knowledge. At t = 4s, B is classified as very, very highly reliable, due to high battery power and by having four successful communications without misbehaving B is classified as a friendly agent. At t = 298s, B is classified as having very, low reliability, this is due to low battery power and as a result low trust. After t = 298s. B is unable to re-establish connection to A, due to TEA-AODV protocol specifications. These specifications seem to be too strict, as at t = 298s, still had a probability of 0.48 of delivering the packet successfully, based on battery levels.

2) Scenario 2

Fig. 11 shows the results of scenario 2, while using the TEA-AODV protocol. Agent D is only introduced at t = 60s. According to Table V, even though D is introduced to the network at t = 60s, it is not chosen as the routing agent

between A and C till, B receives a reliability rating of low, at t = 101s. This adoption time is significantly less than that of normal TAODV. At t = 101s, D's only had a probability of 0.924, this is due to the power spent advertising its routing capabilities. Using TEA-AODV, D was also negatively affected for rating is routing capability, but to a lesser extent than standard TAODV. After t = 101s, B is no longer burdened by A and C's message relays and can use its remaining power for sending its own messages in the network, A and C will use, the more reliable, agent D to route messages amongst each other.

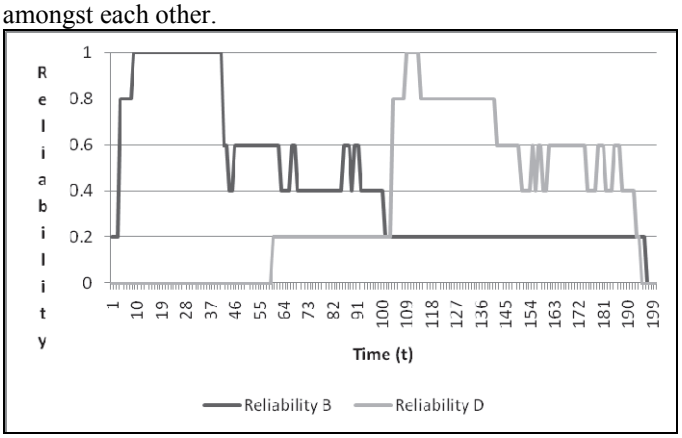

Figure 11 : Agent A's belief in B and D, in scenario 2 using TEA-AODV

Table VII: Scenario 2 test results using TEA-AODV

Time (t)	Reliability of B	Probability B	Reliability of D	Probability D
60	0.6	0.71	0.2	1
101	0.2	0.513	0.2	0.924

3) Scenario 3

Fig. 12 shows the results of scenario 3, while using the TEA-AODV protocol. In this scenario B misbehaves 10% of the time. Ironically, TEA-AODV rates the misbehaving agent with higher reliability than the trust worthy agent. This is due to the fact that by misbehaving slightly, B saves a lot of battery power, and by using TEA-AODV's weighting system B is viewed as more reliable because of this. By misbehaving, B is classified as having very low reliability at t = 379s, as opposed to t = 298s when acting completely trustworthy. [22] did mention the possibility of adjusting the weighting system or adding an additional weight to counteract this behaviour in the future work section of their paper.

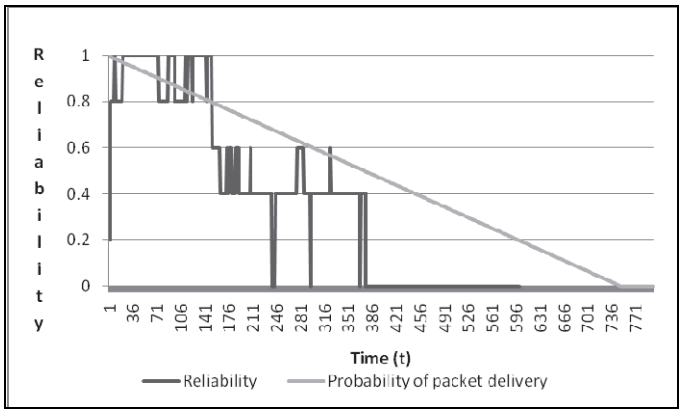

Figure 12 : Agent A's opinion of B in Scenario 3 using TEA-AODV

VI. CONCLUSION

In this paper we investigated some fairness problems identified in online reputation system. We then adapted the problems to fit the domain of wireless networks; we used the adapted problems as criteria for testing the fairness of two trust based routing protocols, namely TAODV and TEA-AODV.

Our results showed that trust based protocols can treat agents unfair in certain scenarios. In extreme cases such as scenario 3, using TEA-AODV, the trust based algorithm might even benefit a misbehaving agent.

A. Future work.

Identify more scenarios which may lead to unfair treatment of agents. Focusing specifically on the layout of the network. Simulation of large networks tend to hide scenarios within the network, which contribute to unfair treatment of nodes, such is suggested by [23].

Adapt the TEA-AODV protocol, to work with quantitative data rather than qualitative data. As well as, testing various weighting assignment applied to battery power versus trust.

After adjusting the protocols for enhanced fairness within these small isolated scenarios, we plan to test the scalability of the problems identified by increasing the network size and enhancing the realism of the scenarios.

REFERENCES

[1] K. Balakrishnan, J. Deng and P. K. Varshnet. "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks",Wireless Communications and Networking Conference, IEEE, pp 2137-2142, Vol 4, 2005.

[2] B. Wu, J. Chen, J. Wu. and M. Cardei. "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks". In Signals and Communication Technology. 1st ed. Springer USA. pp.103-35. 2007

[3] D. Umuhoza, J. I. Agbinya, C.W. Omlin. "Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms" In Proceedings AUSWIRELESS '07: Proceedings of the The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Washington, DC, 2007, pp 80-85

[4] C. Dellarocas and C. A. Wood. "The sound of silence in online feedback: Estimating trading risk in the presence of report bias". Robert H. Smith School for Business, Leaders for the digital Economy, 2006

[5] H. Miranda, L. Rodrigues. "Preventing selfishness in open mobile ad-hoc networks". 2000

[6] T. Ghosh, N. Pissinou and K. S. Makki. “Towards designing a trusted routing solution in Mobile Ad hoc Networks”, Springer Netherlands, vol. 10, pp 985-995. 2005.

[7] J. Cho and A. Swami. “Towards a trust based cognative network: A survey on trust management for Mobile Ad hoc Networks”, 14th ICCRTS, “C2 and Agility”. 2009

[8] Y. Lin. “QoS issues using probabilistic non-reputation protocol in Mobile Ad Hoc Network environment”, Unpublished

[9] A. Wirzbicki. “The case for fairness of trust management”, ENTCS, vol. 197, Issue 2, pp. 73-89, 2008.

[10] R. Denda, A. Branchs and W Effelsberg. “The Fairness Challenge in Computer networks”, LNCS, vol. 1922, pp. 208-220, 2000.

[11] A Maslow. “Motivation and Personality”, Harper & Row, New York, pp. 20-37, 1954.

[12] T. Kaszuba, K. Rzadca and A Wierzbicki. “Discovering the most trusted agents without centralized control”, Embedded and Unbiquitous Computing, EUC ’08, pp. 616-621. 2008.

[13] E. A. Malaga. “Web-based reputation system amanagement: Problems and suggested solutions”, Electronic Commerce Research, Vol. 1, Number 4, pp. 403-417. 2001.

[14] M. Wang, L Lamont, P. Mason and M Gorlatova. “An effective intrusion detection approach for OLSR MANET Protocol”, 1st IEEE ICNP Workshop on Secure Network Protocols, pp. 55-60. 2005.

[15] D.Glynos, P.Kotzanikolaou, C. Douligeris. “Preventing Impression Attacks in MANET with Multi-factorAuthentication”, Third International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks, pp.59-64. 2005.

[16] G. Hahn, D. Nyang, J. Song, J. Lee and B. Park. “Secure cluster based routing protocol incorporating the distributed PKI mechanism”. Proceedings of the 12th IEEE Mediterranean Electronical Conference, pp. 787-790. 2004.

[17] J. Cordasco and S. Wetzel. “Cryptographic vs. Trust-Based methods for MANET Routing Security”, DIMACS Technical Report, pp. 1-20. 2007.

[18] L. Eschenauer, V. Gligor and J. Baras. “On Trust Estimation in Mobile Ad-hoc Networks”, Technical report, MS 2002-10, Institute for research, University of Maryland, 2002.

[19] C. Zouridaki, B. L. Hejmo and R. K. Thomas. “A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs”, In proceedings of the 3rd ACM workshop on Security of Ad hoc and Sensor Networks (SASN ‘05), pp. 1-10, 2005.

[20] L. Xiaoqi, “TAODV: A Trust based AODV Routing Protocaol for Mobile Ad Hoc Networks”. GiGi, pp. 57-83. 2004.

[21] A. Josang, “Artificila Reasoning with Subjective logic”, Proceedings of the Second Australian Workshop on Communication Reasoning, Perth, pp. 34-53, 1997.

[22] M. Pushpalatha, R. Vankataraman and T. Ramarao, “Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks”, Enginering and technology, Vol. 56, pp. 16-19, 2009.

[23] Marias, G. F., Georgiadis, P., Flitzanis, D., Mandalas, K., “Cooperation enforcement schemes for MANETs: a survey,” Wireless Communications and Mobile Computing, Vol 6, Issue 3, pages 319 – 332, 2006.