Trust Is in the Air: A New Adaptive Method to Evaluate Mobile Wireless Networks

Alexandra-Elena Mocanu (mihaita), Bogdan-Costel Mocanu, Christian Esposito, Florin Pop

Trust is in the air: a new adaptive method to evaluate mobile wireless networks

Alexandra-Elena Mocanu (Mihaita)[1], Bogdan-Costel Mocanu[1], Christian Esposito[2], and Florin Pop[1,3]

[1] University Politehnica of Bucharest, Romania,
alexandra_elena.mihaita@cti.pub.ro, alexa.mihaita@gmail.com,
bogdan_costel.mocanu@cti.pub.ro, florin.pop@cs.pub.ro
[2] University of Salerno, Italy, esposito@unisa.it
[3] National Institute for Research and Development in Informatics (ICI), Bucharest, Romania, florin.pop@ici.ro

Abstract. During this new world pandemic, a lot of technical issues have come to life, forcing all industries to reinvent themselves and how the day to day operations are performed. Remote working has become not only a trend but a necessity. Starting from online lecturing to online meetings on a need to know basis, people are concerned about their privacy and security in the online environment. Thus, in this paper, we focus our attention to the concepts of trust and reputation models in Wireless Mobile Networks (WMN), Wireless Sensor Networks(WSN) more accurately, for secure routing of large data packets with respect to Quality of Service (QoS). This paper analyses the current context in wireless mobile networks, more specifically in wireless sensor networks, and proposes a novel adaptive method to evaluate it by defining a Markov based trust function and a new model to manage it.

Keywords: Trust · Reputation · Mobile wireless networks · Secure routing · Adaptive methods

1 Introduction

Nowadays, while all industries have tried to find a new way to perform daily operations remotely, the IT industry has been the one to offer the means to do. This goal has been able to be achieved through video conferences regardless of the geographical location of the parties involved. As the learning curve has adjusted, it has also brought to life multiple issues regarding user and data privacy. One of the most used conference applications, Zoom [18], has faced numerous damning issues: from scandals about sending data to third parties without user awareness, to the *lack of end-to-end encryption*. This type of problems had gathered more visibility than before and forced the authorities to take action [2], [10].

Another issue which has developed from the increased number of stay-at-home people, has been the increased usage of *video streaming apps* or *bandwidth hogs*, as the media has called them. According to their official statements,

HBO Now has reported an increase of 65% of binge-watching and 70% of movie viewing, Twitch an overall increase usage of 31%. In contrast, YouTube Games has reported an increase of 15% [3]. These significant numbers have translated into increased stress on the networks and forced major vendors like Netflix or YouTube to deliver their services at lower qualities to accommodate all the users [7] until better solutions can be found.

The day-to-day applications of security have become more relevant to the end-user and, hence, have enforced the need for research in securing WSN. The impact of privacy violations has made apparent the need for an added level of security when talking about mobile wireless networks. The desired effect is that even if the encryption element of the system is broken, there is still little-to-no-damage to be done on the user part. The extra layer of security mentioned previously can be represented by that of trust and reputation, taking into account the network's requirements for low latency and without increasing the network's offload and overhead significantly.

This paper presents a brief analysis of current research trends in Mobile Wireless Sensors Networks (Section 2). Second, we introduce a novel method for trust management of WSN based on Markov chains (Section 3) and an adaptive method trust management method with respect to QoS concerns (Section 4). Finally, we conclude this paper and present our experimental result in (Section 5).

2 Analysis is in our hands

The leading technologies which make the communication possible represent an integrated part of wireless sensor networks. A significant opportunity for scientific research has been brought forward towards the next generation of wireless communication systems of 6G by the last milestone of the 5G mobile communication standard worldwide release. According to the authors in reference [12], the technologies considered to be too immature for 5G networks will emerge for the upcoming 6G networks, improving the data transfer rates significantly. Therefore, researchers estimate that 6G networks will be faster than the 5G ones by up to 1000 times [14]. This next-generation communication standard will have to meet more requirements than the 5G technology, though, not necessarily, at the same time.

These requirements include a multi-band, high-spread spectrum beyond 300 GHz, allowing hundreds of Tbps links for the interconnection of trillion-level nodes with an undetectable human latency of less than 1ms. In [15], authors estimate that 6G networks will be developed in conjunction with the actual stringent network demands such as low latency, reliability, efficiency, and QoS for indoor and outdoor scenarios, taking into account the security constraints holistically. All these factors have a significant impact on WSN and their applicability.

Another critical use case of 6G networks resides in the evolution of both augmented reality (AR) and virtual reality (VR) with direct application in

e-Health and Smart Cities. The authors in reference [31] confirm that line of thought by stating that the bandwidth requirements for a full human 3D hologram are about 4.32 Tbps. This bandwidth is in the realm of the 6G networks. Even though the use cases mentioned above show a wide range of applications for the 6G networks, a new set of challenges emerges.

Besides the challenges that the 6G networks bring, the authors of [20] talk about the fact that user devices have started to carry more and more sensitive information. That information varies from banking data to actual data about the health of the user or the activity the user makes and when he does it. This information can be gathered and used directly or indirectly to damage the user, thus enforcing the idea of deploying an added level of security which can guarantee the data is unaltered and secure. Trust and reputation in WSN help a user know what elements of the network are to be trusted, including itself from the other's perspective.

In paper [5], the authors describe the concept of trust and reputation in WSN as depending on a set of attributes such as "reliability, scalability, and reconfigurability". Authors in reference [27] have emphasised three main goals for a trust and reputation model in a wireless communication network as follows:

- able to provide accurate information about the worthiness of the nodes, making it clear if they can be reliable or not;
- secure enough to encourage the nodes actually to try and cooperate and earn trustworthiness;
- dissuasive of untrustworthy nodes in the network.

Having spoken about the attributes of trust and reputation models, we also have to highlight their properties. In reference [1], the authors talk about those properties being asymmetry, context-sensitivity, subjectivity and partial transitivity. Asymmetry refers to the fact that: if node A trusts node B, then it is not mandatory that node B also trusts node A. Context sensitivity refers to the fact that node A might trust node B with respect to some tasks but not necessarily with all of them. Subjectivity refers to the fact that the trust each node can compute of any other nodes in the network depends on its perspective. For example, an öptimisticünode will have an average trust value more prominent than a pessimistic one with respect to the same tasks. Partial transitivity refers to the fact that if node A trusts node B and node B trusts node C, then it is not compulsory for node A to trust node C.

As stated by authors in reference [1], one of the main problems when dealing with WMN is the high computational cost of the nodes. This problem, along with their limited resources, leads to an increased level of vulnerability to attacks. Trust and reputation models can, therefore be a viable alternative to security through encryption in WSN. Based on the way that the network includes the trust and reputation model, we can split it into different categories as follows:

- security mechanisms like intrusion detection systems or dynamic access control policies. The role of trust and reputation, in this case, is that of detecting abnormal behaviour and then adjusting the level of trust of the nodes in the network;

- service management. Their use, in this case, can boost the solutions concerning multiple problems like routing and service provider selection;
- service provider(SP) selection. Their use, in this case, gives better performances according to reference [6];
- routing. In reference [9] authors have proved that trust and reputation models can be used for secure data-forwarding even through malicious isolating devices before making routes and finding the best and trustworthy route.

According to authors in reference [28], the trust and reputation models can also be classified according to the initial value that each node is given when entering the system, as follows:

- full trust. Each node is considered to be trustworthy and based on its malicious behaviour, that level of trust decreases. When the trust value drops under a fixed value named threshold, the node becomes untrustworthy. This approach is considered to be an optimistic one;
- no trust. Each node is considered to be untrustworthy and therefore has to prove its benevolence to become trustworthy. This approach is considered to be a pessimistic one;
- neutral value. Each node in the network is given a neutral value of trust and based on its actions that trust level can increase or decrease thus determining the trustworthiness of the node. This approach is considered, as the name suggests it, to be neutral.

According to the same paper [28], there are two possibilities for computing the trust and reputation values of the nodes. The first model is based solely on first-hand information, while the second one takes into account both first-hand information, as well as the second-hand information. If in the first case, each node takes into consideration only its experience to determine if a node is trustworthy, in the second case, it will base its trust and reputation value on its experience but also on the experience of its neighbours. Two systems, OCEAN [4] and Pathrater [22], have implemented both first hand and second-hand information and have shown that this model of computing the trust and reputation value is more robust.

Another interesting classification of trust and reputation models can be made according to the way that the trust and reputation value of the node in the network is updated. According to [19], the system can update the trust and reputation value either event-driven or time-based. Updating the value of the nodes in the system according to the first type of trigger is made after a transaction with the node has been completed. Updating the trust and reputation value in a time-driven system is made periodically by using an aggregation technique.

Multiple scenarios of use-cases for WSN have been built based on each of the priory mentioned classifications and characteristics of trust and reputation models. Multiple models have been proposed and tested in WMN, each presenting their way of analysing the network, suggesting a formula for trust level estimation and results showing the advantages and disadvantages of the selected approach.

Authors in paper [17] have shown that several models can be implemented for wireless mobile networks. These models have applicability in fields like "cloud-computing, identity management and identity federation, web services and Internet of things".

Trust model	Description
ATRM [8]	This model of trust and reputation is carried out locally with low delays and overhead for the networks.
QDV [13]	Is an ant colony inspired model for trust and reputation with good results against packet injection by malicious nodes in a network.
ATSN [11]	Is a watchdog-based approach for trust and security in a network.
RFSN [30]	This is a reputation-table based approach for ensuring security.
CORE [24]	Measures trustworthiness in a network by its implications to common network operations.
DRBTS [29]	Is a two-level structure reputational model to assist user gather the best information available.
BTRM-WSN [23]	Represents another ant colony inspired trust and reputation model adapted to maintain a trace of its neighbors at all times.

Table 1. Proposed models for implementing trust in mobile wireless networks [21].

A novel trust model for Mobile Cloud computing [25] was developed by the Distributed Systems Laboratory from the Politehnica University of Bucharest. The authors proposed an adaptive trust management algorithm for structured overlay networks based on the honeycomb structure.

3 Trust is in the air

Trust model-based systems give the advantage of not using the classic approach of adding a level-upon-level of security but, instead, they enforce it from the beginning and the general level of protection of the network grows along with the system itself. Although the idea of an evolving trust is appealing, the accuracy of the computed value of the trust levels of a node in a WMN is rather difficult to ensure.

After analysing various models of trust and reputation in WMN, we want to set the premises for a new Markov based approach for trust and reputation in WMN. We consider a WMN with a number of N independent nodes whose trust values are dynamic, asymmetric, context-sensitive, subjective and partial transitive.

Almost all the trust and reputation model we have analysed have taken into consideration only the behaviour of the node and have ignored the wireless aspect of the network, therefore bypassing the importance of the link between two nodes.

We have proposed this model to help emulate the behaviour of the connection between two nodes, oversimplifying the problem into three states: the node has a stable connection and is available for tasks, is offline to the network or is in a volatile state in which it is online but not entirely open for tasks. The trust levels of the nodes in the proposed system are influenced by only one type of fault. That fault is that any given node can be offline for an undefined period. Each node fails according to a sum of exponentially distributed function with parameter α. In the system, each node can have one of three states: online and available for communication, offline and non-existing and volatile in which the node has recovered from an offline state, but it is still not available for communication. The volatile state can be assimilated to the error diagnosis state after a sudden shut down of a node.

The trust and reputation model we propose is implemented to help boost the routing of packets and to help find a reliable service provider, therefore being included in the system for service management.

The proposed model represents an optimist approach and therefore grants each node full trust when entering the system. The trust and reputation value of any node in the system, at the starting point, is 1.

The trust and reputation value of a node in the system for this proposed model is computed based solely on first-hand information. This model implies that each node computes the trust of the other nodes and the access points of the system are used for the data aggregation. The number of transitions of a node can be counted by the node itself upon unusual behaviour and also by the nodes and the access points in its surroundings by checking the node's status.Further work on the proposed model will include analysing if second-hand information adds robustness to the system, as references [4] and [22] suggest.

For this model of trust and reputation, we suggest using a hybrid approach of both event-trigger and time-based for updating the trustworthiness of a node. The event-trigger update refers to the oscillating state of the node between online and offline and between the states offline and volatile. The time-based aspect of the proposed model refers to the fact that, if a node is in the volatile state for a period of time larger than a set threshold τ, then it will be automatically placed in the online state again. Along with resetting the state of the node from volatile to online, the trust and reputation value of the node will be restored to 1, therefore allowing a node to redeem from bad behaviour. That bad behaviour in this proposed model is represented by a bad connection, either from subjective causes like battery drainage or objective one like weather events.

The time during which the node is offline is considered downtime. We assume that the downtime of a node is according to a sum of exponentially distributed function with parameter β.

Parameter β, as well as α, can have either a fixed value for the lifespan of the node or a variable one, thus generating two different scenarios (Figure 1). We assimilate these two scenarios in real life to the power supply a node. For example, we can use the fixed-parameter to map, for instance, a node which is

constantly power plug and, thus, has little-to-no variations during its lifespan. In contrast, a battery-based node may vary according to the battery usage curve.

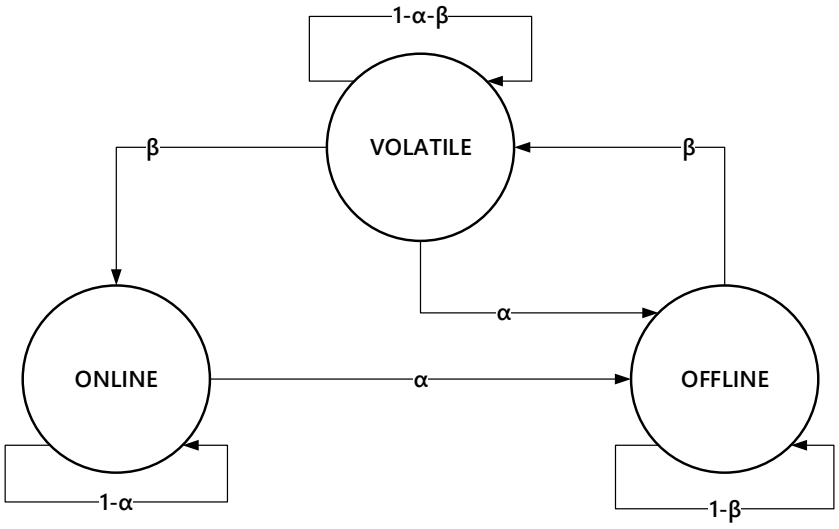

Fig. 1. Each node fails with a probability based on α parameter and recovers to an online state with a probability based on β parameter.

For research purposes, we consider that only one node recovers at a time as well as the fact that the nodes' variations between the state of online, offline and volatile are independently and that the state of one node does not influence that of those surrounding it. Therefore, for each node i from the N number of nodes existing in the network, there is a different α and β generically referred to as α_i and β_i. The premises previously stated represent an adaptation of a model presented in [16].

Given the previous premises, one of the main objectives of this paper is to discover what is the probability that a given number of nodes i, smaller than N, are online at any given time t in the WMN. To this respect, firstly, we modelled the proposed WMN as a Markovian system. We introduce

$$\gamma_i = \frac{\alpha_i}{\beta_i} \tag{1}$$

where α_i and β_i are the coefficients for the exponentially distributed functions which represent the states when a node is offline, respectively online.

Given the equation 1 and knowing the total number of nodes N in the network, we can state the probability that a given number i of nodes, smaller than

N, are online at any given time t, from balance equations of continuous-time Markov chain as follows in equation 2.

$$P_i = \frac{\gamma_i}{i! \sum_{j=1}^{N} \frac{\gamma_j}{j!}} \tag{2}$$

Another goal of this paper is to estimate what is the average downtime rate (i.e. the average number of nodes that breaks down per time unit) as well as the average failure rate for our given WMN.

Considering P_N the probability that all the nodes in the network are online, then we can state that the average downtime rate ($P_{down.rate}$) can be computed as the improbability of P_N happening. Knowing the value P_N, then the probability of the whole network to be down can be expressed in equation 3.

$$P_{down.rate} = 1 - P_N \tag{3}$$

In order to estimate the average failure rate ($\lambda_{fail.rate} \epsilon [0; 1]$) of a network with N number of nodes, we have to take into consideration both the downtime of each node in the system as well as the probability of having i nodes online in the WMN. To this respect, we use the conditional expectation calculation to compute equation 4.

$$\lambda_{fail.rate} = \sum_{i=1}^{N} i \times \alpha_i \times P_i \tag{4}$$

If we know the percentage of time when nodes are unavailable, then we can compute the average number of online nodes in the WMN as stated in equation 5.

$$N_{avg} = \sum_{i=1}^{N} i \times P_i \tag{5}$$

Trying to find the equation for the average downtime rate, a new challenge has arisen. If we can determine what the average number of online nodes is in a network, could we address the problem in reverse and find out what would be the minimum number of nodes that a WMN would have to have to ensure that at any given time there are at least N nodes online? The mathematical equation which can estimate the lowest number M of nodes which can guarantee at least N online nodes can be stated as follows $N_{avg}(M) \geq N$. The extended computation of that inequality can be observed in equation 6 .

$$\sum_{i=1}^{M} \frac{i \times \gamma_i}{i! \sum_{j=1}^{M} \frac{\gamma_j}{j!}} \geq N. \tag{6}$$

These equations have been tested and validates by considering a network with a number of $N = 10$ independent nodes whose values of the parameters α and β can be observed in Table 2.

α	β
0.20	0.99
0.14	0.72
0.20	0.86
0.11	0.97
0.21	0.87
0.11	0.85
0.21	0.81
0.11	0.43
0.10	0.88
0.20	0.98

Table 2. Values of α and β for the test network formed by 10 nodes.

During the validation we have observed that a low rate a failure, stated by a low value of parameter *alpha*, along with a high recovery rate, translated in a high value of parameter *beta*, increase the probability of i number of nodes to be online in the network. These simulation results can be observed in Figure 3.

In Figure 2 we show the dependency of the probability of having a certain number of nodes online in the network according to the existing number of failed nodes. As seen, the value of the probability P is decreasing significantly with the number of offline nodes.

4 Adaptive method bases on probabilities

Given the WMN described in the previous section, with N number of nodes which can switch their state between online and offline independently, we consider each of the node's initial trust to be 1 ($T_0 = 1$). That is to say that all the nodes start from the presumption of being fully reliable, with capabilities to be a part of the network (online). Each transition to offline and online again affect the reliability of the node and therefore it's trust.

We choose the variable w to express the probability that an offline node can not go online immediately, thus remaining in the volatile state. It's value can be computed as the ratio of the rate of node break-downs that can not go online immediately, over the total average rate of node break-downs as shown in equation 7.

$$w = \frac{\sum_{j=1}^{N-1} \alpha_j \times P_j}{\sum_{j=1}^{N} \alpha_j \times P_j}. \tag{7}$$

We can define the trust of a node i in a WMN with M nodes, an average number of N_{avg} online nodes with a probability w that after a break down they cannot become immediately online, after k number of transitions as follow in equation 8.

$$T_i^k = \frac{1}{k} \times \left((1 - w) \times T_i^{k-1} + w \times \frac{N_{avg}}{M} \right) \tag{8}$$

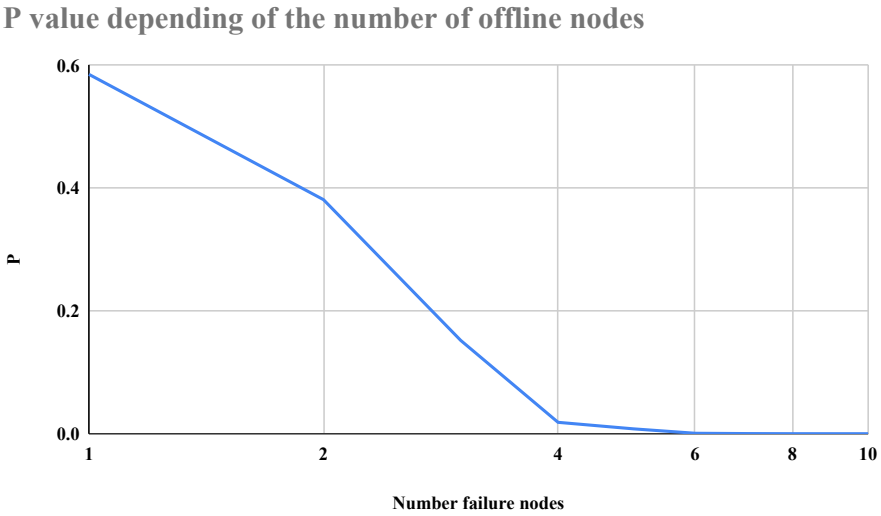

Fig. 2. Values of the probability P of having a certain number of online nodes in the network with respect to the number of failed nodes.

Translating this formula for the trust and reputation level computation into pseudo-code can be observed in algorithm 1. Considering that when a node is going offline is it not voluntarily, then when it is rebooting it will have a system error to detect the abnormal behaviour.

Furthermore, we evaluate the proposed trust method using the same sample values of the parameters of the network, as shown in Table 2. In Figure 4 we show the obtained results where it can be seen that the trust value for each node decreases in the same manner as the value of the probability P of having a certain number of nodes online in the network.

If after a certain number of transitions during the volatile state, a node will remain stable, the trust and reputation model allows the possibility of redemption by reinstating its trust value to the initial one, $T_0 = 1$. Further work will determine how long does the time τ has to be to represent that a node has become stable and available properly.

One of the possible applications of this adaptive method for trust and reputation in WMN is to ensure secure routing of video streams taking into account QoS over a number of N online nodes.

The authors of [26] present a novel lightweight trust decision-making framework named LEACH (Low Energy Adaptive Clustering Hierarchy) for secure video streaming. The stakeholders of this protocol are master nodes, member nodes, and base station, where sensor nodes are organised in small clusters. The base stations are power-plugged nodes, while the master nodes are chosen by taking into consideration the largest battery life of sensors. The low probability

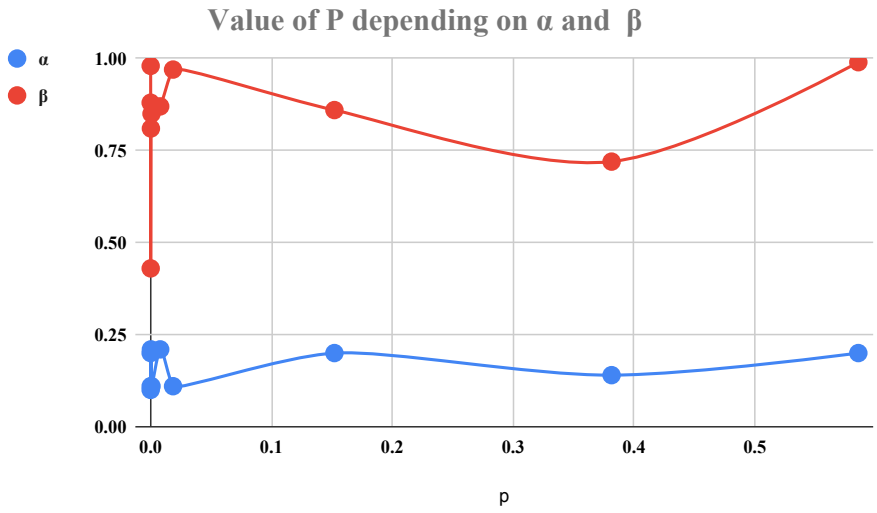

Fig. 3. Values of the probability P of having a certain number of online nodes in the network with respect to the α and β parameters.

of being offline of the master nodes ensures a high level of trust, which is to be expected due to their high availability in the system.

Other applications of this adaptive trust model can be ubiquitous systems.

5 Conclusions

Taking into consideration the heterogeneous devices in a network along with the different operating systems and all-changing topology, it becomes difficult and consuming in terms of resources (time, money etc.) to implement classical security models with respect to QoS.

In this paper, we have proven that the trust and reputation based new paradigm of security may be able to solve these issues efficiently. The Markov based approach for trust and reputation in WMN proposed in this paper manages to compute trust values of the nodes that are dynamic, asymmetric, context-sensitive, subjective and partial transitive.

Each node in the system can have one of three states: online and available for communication, offline and non-existing and volatile in which the node has recovered from an offline state, but it is still not available for communication. The volatile state can be assimilated to the error diagnosis state after a sudden shut down of a node.

The trust and reputation model proposed represents an optimist approach and therefore grants each node full trust when entering the system. The trust and reputation value of any node in the system, at the starting point, is 1. Each

Algorithm 1 Calculate the trust and reputation level of a node

M the number of nodes in the network
Require: $M \geq 0$
for $i < M$ **do**
  Compute for each node its γ_i and probability to be i nodes online at any given time in the network with M nodes
  $\gamma_i \leftarrow \frac{\alpha_i}{\beta_i}$

  $P_i \leftarrow \frac{\gamma_i}{i! \sum_{j=1}^{M} \frac{\gamma_j}{j!}}$

end for
$N_{avg} \leftarrow \sum_{i=1}^{M} i \times P_i$

$w \leftarrow \frac{\sum_{j=1}^{M-1} \alpha_j \times P_j}{\sum_{j=1}^{M} \alpha_j \times P_j}$

for $i < M$ **do**
  update the trust and reputation value for all the nodes in the network
  if node is recovering after being offline **then**
    if time recovering $> \tau$ **then**
      change node state to online
      $T_i = 1$
    else
      node state is considered volatile with k_i transitions
      $T_i^{k_i} = \frac{1}{k_i} \times \left((1 - w) \times T_i^{k_i - 1} + w \times \frac{N_{avg}}{M} \right)$
    end if
  end if

end for

update of the trust and reputation value is computed based solely on first-hand information. This approach has managed to avoid single point of failure but presents less accuracy, each user being limited to its history when considering if trusting other nodes. Extending the model to aggregate data from both first-handed and second-handed data represents future work.

This information is gathered using a hybrid approach of both event-trigger and time-based for updating the trustworthiness of a node. The obtained results of the proposed trust and reputation model present great potential regarding further simulations and determining the accuracy of the proposed algorithm.

Multiple challenges need to be addressed in terms of heterogeneous devices in a network. The first set of challenges addresses the hardware design, especially in the microcircuits and microprocessors manufacturing areas to deal with high propagation loss, especially in terahertz frequencies. Beyond the hardware implementation, the use of distributed user-centric architectures means a significant challenge in the distribution of data to the end-points in a secure and trustful manner. Another issue is creating an efficient and trusted system based

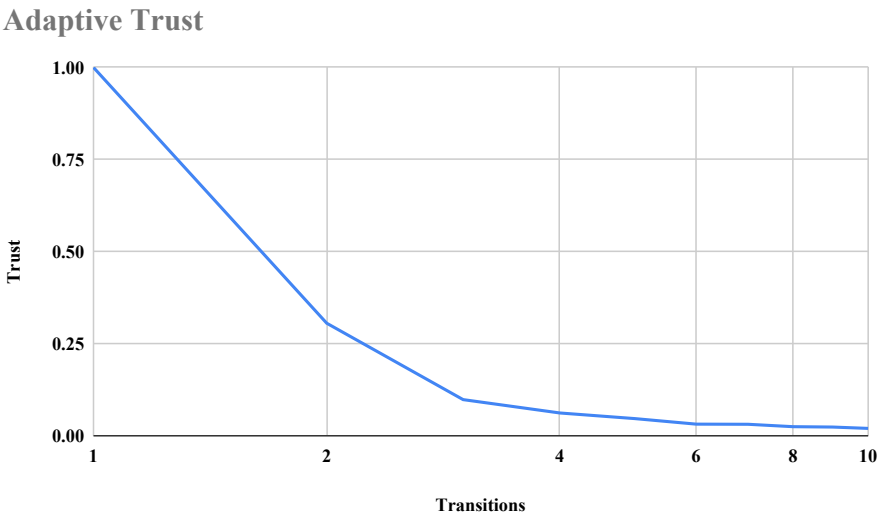

Fig. 4. Evolution of trust with respect to the number of failed nodes in the network

on the next-generation 6G networks taking into consideration energy efficiency. Another challenge in these networks is the modelling and optimisation of the network topology for the scheduling of tasks.

One of the use cases involves the concept of unmanned mobility that will evolve to fully autonomous transportation systems with high efficiency, taking into consideration traffic safety and infrastructure management in a green manner.

Our statements are as follow: the trust model is defined and theoretically proved considering the probabilistic model presented in Section 3. The adaptive model (see Section 4) considers that adaptive factor, w, is changing over time, and that fact is reflected in the trust computation of a node. Further work will present the level of trust that the Markov based security approach which has been discussed in Section 3 can offer concerning similar other techniques presented in Section 2.

References

1. Ahmed, A.I.A., Ab Hamid, S.H., Gani, A., Khan, M.K., et al.: Trust and reputation for internet of things: Fundamentals, taxonomy, and open research challenges. Journal of Network and Computer Applications **145**, 102409 (2019)
2. Aiken, A.: Zooming in on privacy concerns: Video app zoom is surging in popularity. in our rush to stay connected, we need to make security checks and not reveal more than we think. Index on Censorship **49**(2), 24–27 (2020)
3. Alexander, J.: The entire world is streaming more than ever - and it's straining the internet: Governments and isps are trying to manage strain (2020)

4. Bansal, S., Baker, M.: Observation-based cooperation enforcement in ad hoc networks. arXiv preprint cs/0307012 (2003)
5. Baras, J.S., Jiang, T.: Managing trust in self-organized mobile ad hoc networks. In: Proc. 12th Annual Network and Distributed System Security Symposium Workshop (2005)
6. Billhardt, H., Hermoso, R., Ossowski, S., Centeno, R.: Trust-based service provider selection in open environments. In: Proceedings of the 2007 ACM symposium on Applied computing. pp. 1375–1380 (2007)
7. Blose, T., Umar, P., Squicciarini, A., Rajtmajer, S.: Privacy in crisis: A study of self-disclosure during the coronavirus pandemic. arXiv preprint: 2004.09717 (2020)
8. Boukerche, A., Li, X.: An agent-based trust and reputation management scheme for wireless sensor networks. In: GLOBECOM'05. IEEE Global Telecommunications Conference, 2005. vol. 3, pp. 5–pp. IEEE (2005)
9. Brenner, M.: Classifying itil processes; a taxonomy under tool support aspects. In: 2006 IEEE/IFIP Business Driven IT Management. pp. 19–28. IEEE (2006)
10. Chawla, A.: Coronavirus (covid-19) - 'zoom'application boon or bane. Available at SSRN 3606716 (2020)
11. Chen, H., Wu, H., Zhou, X., Gao, C.: Agent-based trust model in wireless sensor networks. In: Eighth ACIS international conference on software engineering, artificial intelligence, networking, and parallel/distributed computing (SNPD 2007). vol. 3, pp. 119–124. IEEE (2007)
12. David, K., Berndt, H.: 6g vision and requirements: Is there any need for beyond 5g? IEEE Vehicular Technology Magazine **13**(3), 72–80 (2018)
13. Dhurandher, S.K., Misra, S., Obaidat, M.S., Gupta, N.: Qdv: a quality-of-security-based distance vector routing protocol for wireless sensor networks using ant colony optimization. In: 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. pp. 598–602. IEEE (2008)
14. DOCOMO, N.: White paper 5g evolution and 6g. Accessed on **1** (2020)
15. Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., Zorzi, M.: Toward 6g networks: Use cases and technologies. IEEE Comm. Mag. **58**(3), 55–61 (2020)
16. Glaropoulos, I.: Queuing theory 2014-exercises (2014)
17. Gómez Mármol, F., Marín-Blázquez, J.G., Martínez Pérez, G.: Lftm, linguistic fuzzy trust mechanism for distributed networks. Concurrency and Computation: Practice and Experience **24**(17), 2007–2027 (2012)
18. Gray, L.M., Wong-Wylie, G., Rempel, G.R., Cook, K.: Expanding qualitative research interviewing strategies: Zoom video communications. The Qualitative Report **25**(5), 1292–1301 (2020)
19. Guo, J., Chen, R., Tsai, J.J.: A survey of trust computation models for service management in internet of things systems. Computer Communications **97**, 1–14 (2017)
20. Kambourakis, G., Gomez Marmol, F., Wang, G.: Security and privacy in wireless and mobile networks (2018)
21. Mármol, F.G., Pérez, G.M.: Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication systems **46**(2), 163–180 (2011)
22. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking. pp. 255–265 (2000)
23. Marzi, H., Li, M.: An enhanced bio-inspired trust and reputation model for wireless sensor network. Procedia Computer Science **19**, 1159–1166 (2013)

24. Michiardi, P., Molva, R.: Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Advanced communications and multimedia security, pp. 107–121. Springer (2002)
25. Pop, F., Dobre, C., Mocanu, B.C., Citoteanu, O.M., Xhafa, F.: Trust models for efficient communication in mobile cloud computing and their applications to e-commerce. Enterprise Information Systems **10**(9), 982–1000 (2016)
26. Ramesh, S., Yaashuwanth, C.: Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimedia Tools and Applications pp. 1–20 (2019)
27. Resnick, P., Zeckhauser, R.: Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system. The Economics of the Internet and E-commerce **11**(2), 23–25 (2002)
28. Sen, J.: A survey on reputation and trust-based systems for wireless communication networks. arXiv preprint arXiv:1012.2529 (2010)
29. Srinivasan, A., Teitelbaum, J., Wu, J.: Drbts: distributed reputation-based beacon trust system. In: 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. pp. 277–283. IEEE (2006)
30. Srinivasan, A., Teitelbaum, J., Wu, J., Cardei, M., Liang, H.: Reputation-and-trust-based systems for ad hoc networks. Algorithms and protocols for wireless and mobile ad hoc networks **375**, 375–404 (2009)
31. Xu, X., Pan, Y., Lwin, P.P.M.Y., Liang, X.: 3d holographic display and its data transmission requirement. In: 2011 International Conference on Information Photonics and Optical Communications. pp. 1–4. IEEE (2011)