ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse48852019.pdf
https://doi.org/10.30534/ijatcse/2019/48852019

A Novel Opinion Computational model of multi path POR Routing Protocol based on subjective logic in Mobile Ad hoc Networks

Dr.A.Rajesh[1], R.Shankari[2]
[1]Associate Professor, Department of Computer Science Engineering, Vels University, Chennai.
[2]Assistant Professor, Velammal Engineering College, Chennai

ABSTRACT

We use the mobile ad-hoc network (MANET) to communicate to the mobile nodes that participate in the wireless network, wherein a new node is ready to advance their details to other nodes within the working environment. However, this allows every othernode, not just for the individual node, but the group of nodes, in an independent manner to share the exchange of information. In this paper is indicated, a novel opinion prediction model, which is to prevent selfish nodes,to ensure availability of trust value with subjective logic. In addition, this paper gives a novel subjective logic trust model to handle errors due toignorance of establishing a communication path between the nodes of a temporary network by a selfish node. The model of trust value acts as a key role in subjective logic. We use this type of model in multipath routing, which uses the subjective logic based trust model in distributed networks to determine the uncertainty between random nodes. There is not enough subjective logic to perform many tasks, so we add new technologies to expand it. For this, we place the new opinion associated with the subjective logic which is an indicator for route selection to the source node.Trust fusion is used to evaluate the relative basis of the application idea in subjective logic. Addition we used Bayesion theorem, evidence theorem and Dempster Shafer theorem. This results in a greater confidence assessment as the mutual trust based information exchange between the nodes. The confidence in the communication exchange mechanism reduces the additional routing overhead and computational overhead. Subjective Logic based Trust Fusion modelon Position based Opportunistic Routing (SLTF_POR) to test the results that are simulated with our proposed routing protocol,then the trial assessment by the use of Dempster Shafer theorem and trust fusion method areaccomplished to analyze a high level of trust and choice information. We analyze our sample results using ns2 simulations based on performance evaluation and compare with Context-Aware Security and Trust (CAST) framework, network performance amidst the different factors of impact. The results of simulation show that our model surpassed the pure subjective logic model and a 25% improvement on time combination.

Key words: Subjective logic, Dempster Shafer theorem, trust fusion, opinion computation, MANET, POR, multipath routing.

1. INTRODUCTION

The wireless ad-hoc network has many wireless nodes, and it is also a self-organized network, where the active nodes follow the dynamic hops, the mobile node does not follow the static infrastructure [1-4]. The node present in a wireless network works as follows: a node will communicate and send information to another node or send it through other methods.The mobile nodes behave differently, it sends information to the other node as a source node, or it may forward data packet to other nodes as a router. The most important advantages are the flexibility, the low cost and so on. However, it has more problems than the above benefits. The routing problem is to choose the best route on the way between the sender and the receiver [4]. Routing is a basic function in the network. The routing system is implemented on wired connectivity and does not use it on the wireless network. It is best designed for a wireless network because of their properties like dynamic infrastructure, transparency, and decentralized operations. [5][6] There are many effective routing algorithms used in MANETs for data exchange in the proposed work. Many efficient Routing algorithms are proposed on the wireless network, but some of them have been attempting to fix a new solution in our proposal, instead of some selfish node and malicious node processes,but they don't have the right solution for the problems that come at a certain time. For that, it is believed that the network will have basic trust when it occurs in the communication and that the information received on the network will increase as it is correct.As a solution, we are trying to get a better solution by subjective logic, opinion from other nodes and trust fusion methods which examining the communication path that has logical concepts in the research work.The routing is divided into three categories: they are proactive, reactive, and geographic positioning. These algorithms run on the nodes having occasional transmission of hello messages among their neighbors. [7][8] This information is used to create routing algorithms that run on the nodes and create ways to build and improve the routing nodes for neighboring schedule and maintenance. Proactive routing protocol: Before it sends the message, the

source node should consult with its neighboring node(s) and determine the path to a destination node. Reactive protocol: When it sends source node information, it finds its way through its nearest node. Geographic routing protocol:Participants on the network find its location information through GPS and share that information with the nearest nodes. The nodes participating in the wireless network need to create a trusted communication with the node to which they interact. In order to create this, each node communicates with its nearest node about the other node to which it is associated and evaluates it. The value is derived from this, as well as the additional consideration of trust fusion technology. The communication node received a higher value than the value assigned to that node. Doing so can sometimes lead to misinformation.

Opportunistic based routing protocol: This routing protocol comes under the geographical based routing protocol. [9-11] Proposed the concept of opportunistic based routing protocol with MANET as an extension and interpretation of Delay-Tolerant Network (DTNs). These networks are unpredictable and the current environment nodes of this network cannot predict the path of the informationand the manner in which that network operates cannot be predetermined. The way they operate is assumed to be hypothetical. In this case, the detail of the participating nodes becomes concealed, so there is no previous information between the nodes stored in any node.The network and nodes that participate in delay tolerance networks, most of which are caused by some problems in information transport, such as frequent spatial modification of movement nodes, periodic connectivity and end node disruption.These features will result in longer delays than existing Macy's regular networks [12]. The typical opportunistic-based routing protocol network and the nodes it operates on are often characterized by the inability of power control devices with interconnected, crowded mobile nodes, interconnected views, and decision paths [13].But the spatial-based comparability routing protocol causes a lot of power consumption. In the current period, most countries are unable to access the internet at all times, when connecting to the internet; they are more likely to spend money for the people. [14] But the number of people is very low. As a solution to this problem, in some rural areas where there is no internet connection, some countries use a rural Wireless Fidelity (Wi-Fi) to access and provide their information from people living in isolated and remote villages. The proposed researcher gave an idea which is used to establish an internet connection for village networks. This event has the following activities: An opportunistic basedrouting protocol and an interesting evolution of many hope networks emerged in that space. These functions are only allowed in such networks. Multiple hop communications are provided through opportunistic based links.

When the path to a destination is not clear or during communication with other nodes, the node automatically retrieves the message. The nodes of these networks use the store concept to move forward and approach other nodes. The POR is not required to have a strong connection to data communication. It does not receive a stable route between two nodes for information traffic. The pathway is often shared with prolonged periods of time such as direct path, frequent deterioration, and long intervals. [15]An excellent example would be to have ad-hoc nodes with the soldiers in the battlefield and the helicopter carrying the communications plane. When the decision to send its data is unavailable, the alternative node will decide, for some reason, that a particular connection is not available, but opportunistic basedrouting protocolworks on all nodes, each node tries to detect the next link of each hop. Each node that has the role of opportunistic networks has its information and uses the local knowledge of its nearby nodes and determines the next hops between its neighbours. When there is no chance to transmit information to the intermediate nodes, a message is saved before the message is sent to a forwarder node about the current state of a node. The actions of an opportunistic based routing protocol with network should not be a clear source of consideration for later. The other reasons, based on the information currently stored in each node, is sent to the next node in the path.Figure 1 is shown the hierarchy of networks architecture with property of mobile node, in which the methods are set to MANET

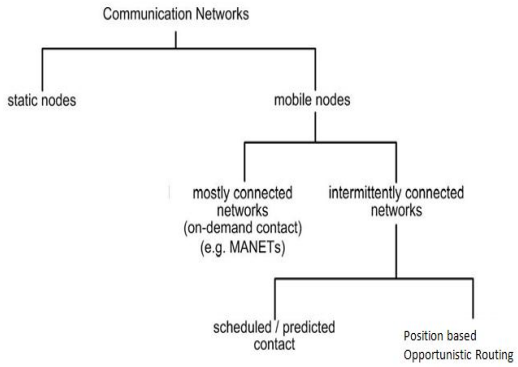


Figure 1: Hierarchy of Networks architecture, in which the methods are set to MANET

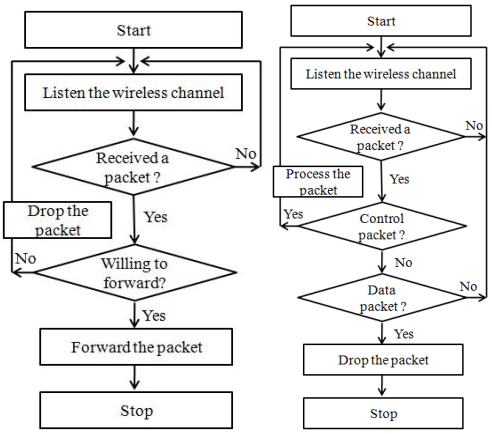
When the nodes of a network communicate with other nodes from where they are located, the network can be divided into several types based on the interconnected network and the alignment of the nodes. Nodes can be tabulated/calculated by their connection characteristics and are divided into two categories, For example, [16] Interconnect Internet network (IIN) or opportunistic network which can be divided into two classifications (e.g. Personal Area networks and vehicle Ad-hoc networks). Communication between the nodes of

some type of network and future connections is known early in the planned interactions, but no such information can be predicted in opportunistic based routing protocol network communications. However, these opportunistic routing communications are based on existing MANETs.If communication is ongoing between the two nodes, in the case of these, it is necessary to know that the other nodes will participate. The trust fusion method will be used to find out if any one of them is harmful to the node of contact between the two nodes. These are designed to be combined with the POR protocol, which is at the node.

The hazards of a malicious node in the communication path between the two nodes:

The POR protocol can be moved to a waiting node to obtain information via other channels, so that safe communication cannot be reported, in which case the attack nodes are not able to be predicted and then Since the node and its information have not been sent to its designated path, two major attacks occur selfish node attack and malicious node attack both attackers are participating in the network as normal nodes [9].The most difficult way to navigate the opportunistic based routing protocol is on nodes and networks, which are in good condition. The higher reliability of the persistent connections and its information between the nodes are more common, the routing protocol is shared between the nodes. The best and shortest route is to send information packets from the source, and packets are sent to this node. The shortest cost path of each path is computed based on possible routing and to select theoptimal route path from the best path list. On the other hand, the node connection is not common and is the next intermediate device (nodes) connection that connects them.The methods and path systems used by opportunistic-based routing protocol follow these definitions, in which some issues had been meted out following the POR such as selfish node and malicious node [17] [18].

The selfish node does not support the extension of the routing so it is considered as misbehaving node on the network.The nodes sometimes have certain properties, such as low battery power, and higher bandwidth utilization. In the rest of the areas, working policies that introduce the different malicious routing protocols like 1) Selfish Behavior and 2) Malicious Behaviour have been discussed.Figure 2 shows flow charts for selfish and malicious behaviours. The selfish node is called a selfish attacker, comes under a active attack and works in an offensive way with a selfish node to combat resource boundaries (such as low battery power, high bandwidth utilization). In Figure 2 (a), a selfish node is a part of setting up the path to take part and participate in the packet sharing. However, with selfish node contact, neighbors send the data it wants. Figure 2 (b) shows the malicious behavior of the selfish node.



(a) selfish behaviour(b) malicious behaviour

Figure 2 : Flow of process for the selfish behaviour and malicious behaviour nodes

Selfish Nodes Vs Malicious Node: Some nodes may come forward and share information with the other nodes of its memory but try to exploit the other nodes' memory location. Such nodes are called the 'selfish nodes'. A Selfish node does not show much interest in forwarding the packets of others nodes. Similarly, it is not interested in sharing its memory with other nodes. Selfish nodes can be divided into three categories. First category of selfish nodes:these nodes keep the memory within bounds and hold the duplicate as other nodes. The second kind of selfish node uses the energy to send its packets to other nodes without using the forwarded packet to detect the route. The third type of selfish node is having its energy,but even though, a node has its full state of energy level, it does not share information with other nodes. No node can predict when it works and when it isnot working. So it has contact with the nodes in other good positions and finds nodes insame level.

The malicious nodes use the nearest nodes information to link the data to the other nodes. This will enable the network to transmit unnecessary and excessive communication. Finding such malicious nodes is not an easy task. Malicious nodes do not enforce their evil actions on the network at all times. To reduce the performance, all the nodes participating in the network will be divided into small groups as a cluster and set up a master node to manage them, and combine the POR protocol on all nodes, in addition to subjective logic. In addition, the proposed methods are determined by the merger, which determines the node at which the data is to be transmitted before it can be transmitted, can be removed from the transaction without use.

MANET has been very inefficient in the past few years because the collaboration of the nodes participating in the wireless network is very low. If there is cooperation, there is an underlying credibility within it too. We do not use this for many important security applications. Considering this, we present an opinion based subjective logic

theory to create a reliable wireless network. It is often difficult to predict. It is also a challenging task in designing a new concept of opinion based subjective logic that will keep us in the way of its functionality and facilitating routing in MANET.

Subjective logic:

Table 1: Binary logic with equivalent probabilistic logic

Binary Logic		Probabilistic Logic		
AND:	$x \wedge y$	Product:	$p(x \wedge y) = p(x)p(y)$	(1)
OR:	$x \vee y$	Coproduct:	$p(x \vee y) = p(x) + p(y) - p(x)p(y)$	(2)
XOR:	$x \not\equiv y$	Inequivalence:	$p(x \not\equiv y) = p(x)(1-p(y)) + (1-p(x))p(y)$	(3)
EQU:	$x \equiv y$	Equivalence:	$p(x \equiv y) = 1 - p(x \not\equiv y)$	(4)
MP:	$\{(x \rightarrow y), x\} \in y$	Deduction:	$p(y''x) = p(x)p(y\|x) + p(x)p(y\|x)$	(5)

Binary logic is a claim to all concepts in the world [20].Whether this statement is true or false, the assumption must be relevant to the world.It is a coincidence,finding this must be within the range of zero and one. We believe that if they are the source of information from the available information, or we conclude based on evaluated value as a true or a false statement.Subjective Logic and probabilistic logic, these two different operations are usually given as the truth table. Its main purpose is to handle opportunities with a binary logic capability, and the creation of a fear-free state from the structure. This structure provides a powerful theorem [19].

Subjective logic is derived from probability logic and uncertainty with subjectivity, and probability logic is derived from logic and probability [19]. When a source node communicates its information to another node, and it does not know the node, that source nodeknows about the unknown nodevia its trusted node. Then the node sends its message to a given event.

Table 2: relationship with belief and trust in subjective logic

Relationship type	Belief	Trust
Formal notation	[S,X]	[S,D]
Graph edge notation	S→X	S→D
Interpretation	Node S has an opinion about variable X	Node S has a trust opinion about node D

For the last 5 years, safety of mobile node technology has been proposed to provide many ideas and many solutions. But they are not considered as a permanent solution at the present time. Because when the nodes contact them, they share a lot of information, and they come to trust in ignorance.The basis of credibility between the basic level and its reliability is the fundamental principle of consensus.They fail to reflect the ignorance of their existence by creating and establishing credibility among these nodes.Therefore, friendship between the two nodes must always be realistic which is proven in table 2.

It is good to be always precise. For example, when a new nodejoins with thenodes in an existing network it reaches, the nodes with whom it has to establish a communicationwithreliability. When those nodes do not try, the disbelief is shown. Many problems occur by creating an autonomous reliability on a new node. The benefits can be classified in a number of different ways by having a low or neutral credibility of the model,(or) a higher level of trust,(or)based on various issues. This is a great way to connect a new node into existing network and create a contact with a steady, positive one, from a pole of faith. However, when this type of network is equipped with a higher confidence node, and a less reliable point is used to communicate then it causes some disruption.

Rest of this paper discussed, in the second chapter, we have analyzed all the information related work to this proposed work, the advantages and disadvantages of it, and the ideas that have been omitted from it, taking the information we need and combining it with a protocol and using it in a network. In the third chapter we have thoroughly discussed our proposed article. Chapter 4 simulates our proposed scheme, with the information available from it, proposed by someone else before it as a CAST routing protocol [21], and comparing it with our protocol-like SLTF_POR protocol and proposing the reasons for the differences.

2. RELATED WORK

We have focused on some reliability models of routing in MANET. This related work is based on whether a network provides a reliable routing and in guaranteeing it.Wireless Mobile adhoc network is a network that is used for emergency purposes. It automatically generates a wireless network, in a very short span of time. We are in the forefront of an urgent need. If the information is sent from one place to another and the information is sent for emergency purpose, then the nodes in this network play an important role. There is something called a selfish node or malicious node, and its reliability and urgency require both to be questionable. Therefore, we form a network routing protocol to send each safe information by realizing this significance.

MANET's security algorithm is not very easy to use, since it is a dynamic topology so it is very difficult to use. As a solution, the Trust Network has been created to establish a node's reliability between the nodes on the basis of trust, where the direct trust and indirect trust value are used to find trust value of each node. This is because some

malicious node works for of another node's recommendation for a false calculation of other nodes. A good node is a node that is converted to a node of negative thinking among other nodes. So subjective logic is proposed asa solution.Some problems keep arising during packet forwarding and we have researched and developed the opinion based subjective logic network.

While it is very difficult to calculate the reliability, the reliability is compared between the nodes, one of the most reliable node credits from the other nodes, and it self-examines and accepts if it is correct. If there is any mistake, it is mixed with other nodes. A simple solution for this is that a cluster has been created and a trusted one is appointed as the head and thereby using various methods. The reliability of the evaluation is assessed in two ways: functional reliability and suggestion reliability [22]. Depending on this reliability, packets are sent from one location to another. This route is based on the credibility and then packets are transmitted through the route.

Trust and Trust Management Systems: Developed through a belief in the foundations of traditional trust management systems, as well as mechanisms that rely on the uncertainty of its future interactions.This reduces confidence, which is beyond the control of loyalists, but whose beliefs and actions are believed and affected.In other words, nodes are believed, this balances the perceived risks and the principle of trust. A subjective logic begins with two nodes.Generally, all nodes are known risks, and that nature is considered an important concept, and this concept provides a direct relationship to a reliable node based on a kind of belief or experience.This reliability is the time and circumstances of other factors affecting the outcome of the decision i.e. the relationship between the reliability of the node or the nature of the confidence threshold and its application activities.In addition, the second trustee, on the basis of a direct relationship with the first trustee, has been named in a disguised relationship with his trust or second trustee.Allowing users to share their ideas with the network by allowing this process to be shared with the terminals of a network is in a good position [19].

Trust management systems are evaluated by the following components: (a) a certified collector of nodes, (b) Policy manager decision policies for results and analysis.Depending on the expropriation of resources at one node, some other networks had other nodes at the same node as other networks, while others found the only source to take the idea from its first contact.You can also consider suggestions received from other nodes of the methods.Our model picture captures the first and second contacts between the two nodes, the evidence from other caregivers, and links with neighboring networks about the nodes.The models of trust obtained at one node, as well as the representation of the evidence captured at the other node, differ in the representation of the two sources.For example, you can specify the values of the expression that represents the data or node of the captured sources on a node.In our sample, trust is measured, resulting in my continuous throughput, which is represented by a series of values.In addition, establish trust relationships between the two nodes to compute the corresponding basic forms, such as map theory, entropy, and subjective logic, which are used to verify and number patterns.However, the great trust between the mobile nodes is established and reorganized, and we seek subjective logic to function properly and to manipulate ignorance [19].

Matters related to the recommendation between the nodes and their ignorance: the most important purpose of this study report is to be aware of some well-known concepts and the recently proposed Foundation models. We pay our debate and focus on ideas.Liu et.al.,.The researchers monitored and analyzed information from their neighbors' network behavior and proposed a decision, which created a source of reliability and basis [23].Researchers sometimes consider different approaches to distributing or receiving advice, and a neighbor may unload pockets to prevent their neighbors from engaging in inappropriate activities and making their performance less likely.However, it is slightly less to prevent his performance. As presented by researchers, the Dynamic Source Routing (DSR) proposed an approach to establishing trusted routes for routing. The types of trust approach are different.Determine the weight of the reliable node for each connection, as well as the information from another node, weighing the sum of the entire node reliability path, and then selecting a reliable path to the weight assigned to it. Basically perform the short path algorithm.In addition, they should use the hash function based legal node.However, the proposed approach to nodes fails to prevent their information from spreading in a single node network. [24]Ant-based Evidence Distribution (ABED) This type of protocol is implemented in the intelligence-based approach, distribute and discover the resources obtained from this Protocol modeling functionality from ant colonies And creates a network of nodes.The most interesting aspect of this protocol is that you can see that all the nodes are spread to routing information.A note, researchersare recommended to share its reputation with suggestions for a node and solve the problem of honesty, and a node derived from its experience must be evaluated honestly. This is a recommended node that shares its recommendations with only the nodes that share the honest recommendation.However, this kind of proposal has the potential for joint attack. According to Virender and et al., the researchers used the trust model to create a group using trusted key [25].He recommends and follows this five-step process that requires you to establish and maintain a trust relationship with his proposed node that accepts recommendations from a trusted neighbour.If they want to alleviate the consequences of dishonesty,

they can make recommendations and evaluate them based on the trust relations established by the node with their appointment and then the larger or average of their impossible suggestions Select.However, the proposed nodes approach cannot predict how to interact with the neighborhood side.

Cooperation of nodes: Evidence from canonical news and advice, as long as the nodes in dynamic networks are reasonably and credible.Then it unites all information, predicts resources, finds malicious nodes and makes good decisions, avoiding a good node path selection.This study is sponsored by researchers have proposed a breakdown of the nodes association and the networks, but thereby its core and its cosmic nodes are all running its sway, and thus all nodes are different from their trust.

But such an approach would suggest all the behaviors of the node's communication factors and the node's recommendations, which would be unusual for neighboring networks, and it is important to find compromise nodes.Furthermore, these types of policies are related to authentication recommendations.But they are not able to discriminate against the recommendation. Similarly, their mission is to recommend and disseminate information to the node of neighbours and its network.They recommend a set of peer-to-peer methods to detect the origins of these researchers and distribute them to other nodes.You will need to collect and review the evidence that activities have been collected between your suggested nodes.A clever approach has been created for finding new applications and dissemination of resources.

Uncertainty in trust relationships between nodes: On the one hand, Yan Lindsoo et al., the researchers proposed a model of entropy-based trust to measure the instability of trust between the nodes.Here hopeful model Liu Xiaoaki et al. It's very close to the work of our research because it uses logic to convey uncertainty between the nodes [26].However, when these two nodes move from one location to the other, the nodes fail to manage the instability, or the nodes may have no evidence of the damage and impact of the nodes.It is important to evaluate the relationship of nodes with those nodes and make accurate decisions.As far as recommendations are concerned, these optimistic models do not have a well-defined approach or are not well defined to protect them from honest stimulation.In addition, the pattern is distributed between the nodes of the recommendations and the information is operated independently, in which the possibilities for referral bias and higher secondary are taken into account. [27]Interestingly, in the process of observation-based cooperation and implementation between the nodes of the temporary networks (OCEAN protocol), researchers Bansal and Baker are concerned about the direct observation and dissemination Only solve problems that are collected from complications.Our self-confidence model is designed to adapt to the benefits of the node recommendations, even if it resembles the OCEAN, in solving the problems associated with the recommendations in our protocol.Our protocol differs from the OCEAN by using a new approach to get recommendations within the MANET controls that we have provided in detail.Zomlot, Loai, et al work is based on mathematical sound with subjective logic that handles activities and beliefs related to our work.Rooted in the Dempster-Schaffer theory, its apparent representation and ability to manage the ignorant rate of a single pancreas, the subjective logic arises, intrinsically, naturally, like MANET's, dynamic open and uncertain trust manipulation Networks that manifest as an attractive tool [28]. The author has introduced a Power-Aware protocol [29]. The author has implemented a Long Range WAN Routing Protocol for Vehicle Traffic handling in emergency situations [30].

3. PROPOSED SYSTEM

The dense network has a lot of nodes that are very easy to access selfish node and malicious in this type of network are formed. We use the POR routing protocol for all nodes. Each time you send the message, the node is to find the forwarder node in a good state. For that, each node is to have an initial connection and become the nearest node, and the way in which it works is given below:

- The front node is sent to the request packets to the nearest nodes, where two types of information about the node.
- The first type of information is the reliability of the node, and the credibility of the nodes that are adjacent to it, and also, opinion on the destination node is sent.
- That node uses two types of theorems to analyze the information received first, the principle is used in Bayesian theorem and Evidence theorem.
- The Bayesian theorem is used to analyze the confidence of the forwarder node and to examine the value of the Evidence theorem or opinion theorem and the methods that are adjacent to the forwarder node.
- Then the node of transmission is using the Dempster-Shafer theorem and using the trust fusion method to choose which of the adjacent nodes is best.
- Similarly, it also studies the destination node.
- Each node is used in two different criteria to select the best forwarder node from the most optimistic nodes in the lane to send information from its standpoint to its destination node. This means that depth first path finding and heuristic search for near optimal algorithm is used.

In our model, a fixed range is transmitted using an omni-directional antenna.Our model is focused on improving the subjective logic based trust and does

not depend on any tamper-proof hardware.In this paper, we address only the POR routing protocols because of their ability to detect pathways in demand.However, our model applies to small changes in geographicand hybrid routing protocols, which we will leave behind for future work.In geographic protocols, we have chosen the POR protocol to present the details of our foundation model.Amongst the geographic protocols, we have chosen thePOR protocol to present the details of our trust model. In order to take advantage of redundancy in MANET, we choose Subjective logic is used with a trust Fusion on Position based Opportunistic Routing (SLTF_POR) , which is one of the extensions proposed for the POR which is compare with Context-Aware Security and Trust (CAST) protocol.

Trust Fusion: Combination of serial and parallel trust paths

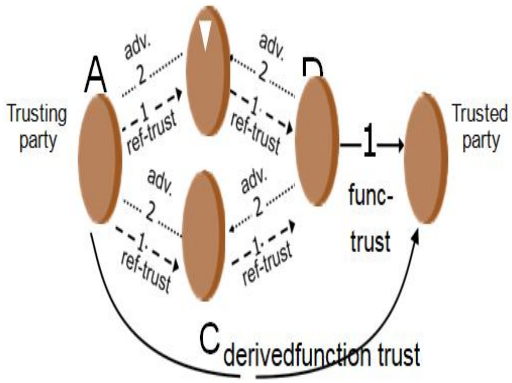


Figure 3: Interaction between the trusting party and trusted party

One node as a trusting node is to analyze the value of a trusted node by using the trust fusion system in a variety of ways before contacting other hopeful nodes. We have been showing this in two different ways figure 3 and Equation 6.

Dilution and Confidence value of trusted node

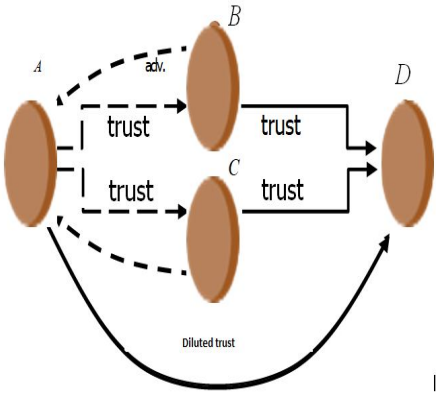


Figure 4: Trusting node obtain different values about the trusted node

Before a node can communicate with forwader nodes, it is necessary to analyze the value of a

$$\text{Graphnotation: } [A,E] = (([A;B] : [B;D]) \Diamond ([A;C] : [C;D])) : [D,E]$$

$$\text{SLnot.: } \square^{[A;B;D]\grave{a}[A;C;D]} \square((\square^{A}\ddot{A}\square^{B}) \mathring{A}(\square^{A}\ddot{A}|\square^{C}))\ddot{A}\square^{D\,E} \quad (6)$$

Dilution and Confidence value of trusted node

trusted node using a trust connection system in several ways. But the neighbour node has a lot of different opinion, but it gets the value of the node depending on the nature of the concept. We have given the Figure 4 shown.

We refer to the wireless range in a node as its context.For easy interpretation, we have a successful way of defining the discovery and flow of data continuously as a communication flow.Like other trust models, our trust fusion and Dempster-Shafer theoremmodels.You can find route and/or packets to deliberately disrupt the flow of data and/or save battery resources as malicious nodes. Such behaviors are referred to as abusive behavior. In contrast, the behaviors that comply with the routing protocol specification are referred to as optimal behaviors.Several routing solutions that have tried to cope with the MANETs challenge. Some of them include dynamic topology changes, interference losses, excessive movement of the nodes, results of individual autonomous nodes, connections and lack of structured security.From all these challenges, the decision of the node on a MANET will greatly affect the efficiency of communication.In view of this requirement, we focus on providing a node that will follow all the nodes to select the next hop to be able to routing the information on the network.The main contribution of this routing is two types. First, we evaluate the nodes of the universe in a dynamo to any current contact.Secondly, we propose a multi-path selection factor to be decided by the most selective multi-path POR protocol in MANET which is shown from figure 3 to figure 7.Position based Opportunistic Routing has major temptations for a multi-path POR format.The working strategy of POR is very efficient in providing routing to the network.The Route Request (RREQ) message is flooded, and then each node operates through the current, checking whether the path known to its destination is in the cache.Initially, the source node could send data to the sheltered member in its immediate search.This immediate sheltered level 1 is known as neighbour. Next, the neighbour is evaluated here before selecting the level 1 hop by using a multi selector factor. The data will not be sent to level 1 with the next connection until it is ready and trusted.

Fusion strengthens trust confidence(Incorrect trust / belief derivation)

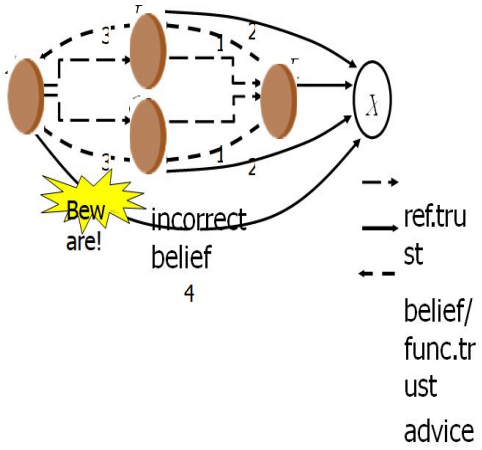


Figure 5: A fusion of trusted node strengthens confidence the confidence in it has been falsified

The trust value derived from other methods strengthens the reliance on trusted node or has falsified the confidence in it. We have been showing this in two different ways figure5 and Equation 7.

Perceived: $([A,B]:[B,X] \qquad ([A,C]:[C,X])$

Hidden: $([A,B]:[B,D]:[D,X])\ ([A,C]:[C,D]:[D,X])$ ..(7)

Hidden and perceived topologies: The trust value derived from my other nodes of trusting node strengthens the reliance on Trusted node or has been falsified by the belief in it. This may be the format of a network of two different networks, such as topology or hidden topology which is shown in figure 6 and equation 8.

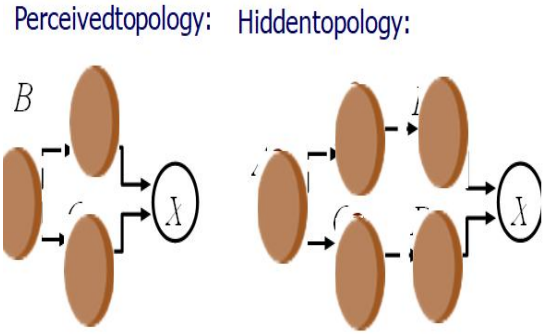


Figure 6 : Trusting node strengthens the reliance on Trusted node or has been falsified by the belief

$([A,B]:[B,X]) \Diamond ([A,C]:[C,X])$
$\square ([A,B]:[B,D]:[D,X]) \Diamond ([A,C]:[C,D]$

(D, E) is taken into account twice

(8)

Correct trust / belief derivation: By knowing the design of the network and the connections between the nodes of the system before you learn about the other method, you can avoid the hopelessness of a node that occurs which is shown in figure 7 and equation 9..

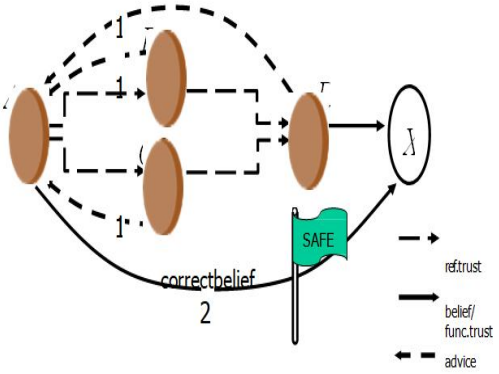


Figure 7: learning procedure of trusting node

Perceived and real topologies are equal: $(([A;B]:[B;D]) \Diamond ([A;C]:[C;D])):[D,X]$ (9)

4. MATHEMATICAL MODEL

The packet deliver ratio, packet loss, latency, and QOS are the four mechanisms that are used here for the next hop selection. In Figure 8 and figure 13 are representation to understand the work of the Multipath POR algorithm. The move displays 11 nodes, which set up a ad-hoc network. Each next hop is selected based on the best node selected from the best Hop selection factor expressed in equation (9). The hope Selection factor equation (10) is evaluated as rated by the matrix M.

$$M^j = \begin{bmatrix} D_{i,j} & 1-Q_j \\ Tr_j & L_{i,j} \end{bmatrix} \qquad (10)$$

$$HSF_j = |M_j| \qquad (11)$$

Here, Li,j is the connectivity, Di,j is the distance, Trj is the trust value, and Qj is the quality of service of the next hop j from the current node i respectively. Each node that you want to send is using this algorithm to continuously detect its next hop j. During such a next hop selection process, each node determines the following parameters in the timer.

5. SIMULATION AND ANALYSIS

Simulation and analysis we used NS2 to personify our research.It uses an uneven motion and a random channel model, where a node starts from a random point and its operation is waiting for a specific period of time. The same node chooses another random node without progressive thinking, and the node is moving to the new point with the selected velocity between the starting value 0 and the maximum faster ' Vmax '. The maximum message exchange velocity 250 for a node, and the approach used for information exchange, we have set up the Medium Access Control (MAC) protocol and routing protocol from the IEEE 802.11 which is implemented in SLTF_PORrespectively.We selected a ConstantBit Rate (CBR) traffic of 2Mbps data and a packet size of 512 bytes that allow for excessive data flow.The remaining parameters followed with the value are compressed in table 3.A mobile SLTF_PORis the basis of the protocol that they are designed to rely on it, and they are known as our model of trust.Our trust model is compared with exiting mode of the mobile nodes trust as aCAST protocol.

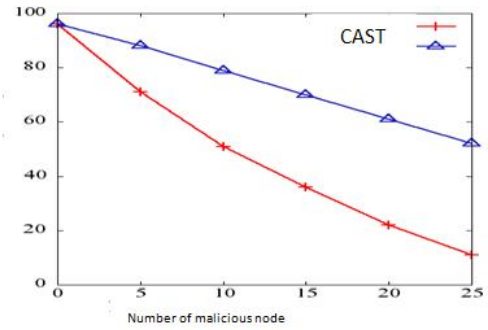


Figure 8: Number of malicious node Vs. PDR (%)

The malicious node of the dense network increases the number from 0 to 25, and when the information is transmitted from source to a destionation node, Figure 8 is shown in the difference between SLTF_POR and CAST routing protocol where two different protocols are made in the methods. The way in which information is reached varies, these two different protocols are shown to be the best.

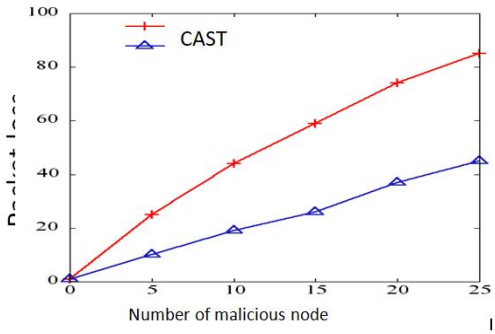


Figure 9: Number of malicious node Vs. Packet loss (%)

The loss rate of the data reaching the destination node decreases when it increases the number of malicious nodes, which gradually reduces the reach of information. The rate at which this information reaches is examined in two different protocols, while the SLTF_POR protocol follows a critical belief and the message loss is very low. Figure 9 is shown loss rate when the malicious nodes were increased.

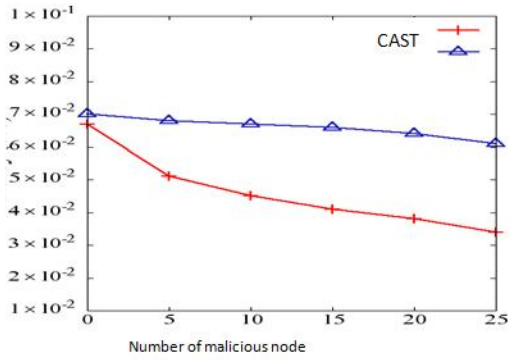


Figure 10: Number of malicious node Vs. Latency

The time it takes to arrive at the information is increasing when the network increases the malicious nodes. Subjective logic with trust fusion methods is selected on the basis of which the message is chosen before the information is sent to the other node. Figure 10 is shown the difference between SLTF_POR and CAST.

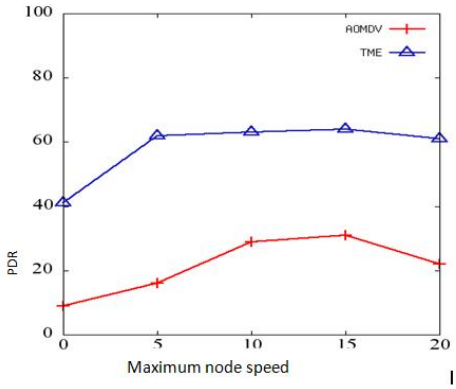


Figure 11: Maximum node speed Vs. PDR (%)

When you start finding ways to find reliable routes on a previously discovered route, it will be the malicious node (s). reliable routes are longer than optimal hop-length, and the time to build trust Every hope. In the case of information transport, the nodes are in mobility but their reach information is very limited and it will be difficult to analyze the nodes and trust of the nodes. Figure 11 is shown the maximum node speed Vs. Packet delivery ratio (PDR).

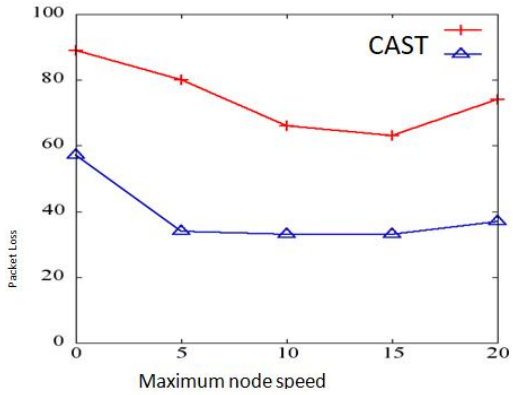


Figure 12: Maximum node speed Vs. Packet Loss (%)

The nodes are moving at maximum speed, but when the loss of a packet is compared with another protocol CAST, their data loss is very limited. Because of the primary reason for the trusted protocols being injected into the nodes. Figure 12 is shown the difference between SLTF_POR VS. CAST.

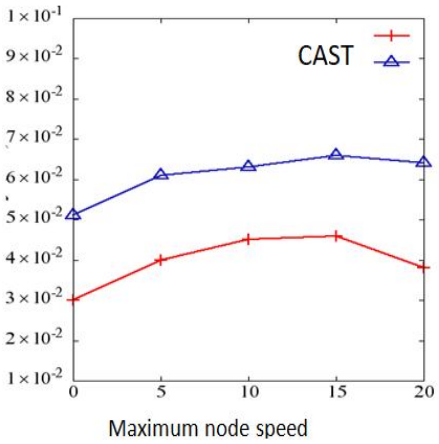


Figure 13: Maximum node speed Vs. Latency

When the nodes increase their speed, the time taken for each packet to come is greater than the other CAST protocol. Figure 13 is shown the difference between SLTF_POR VS. CAST.

6.CONCLUSION

In this research paper, we have an innovative subjective logic based trust fusion model, which they openly represents and manages ignorance that they are uncertain of their trust fusion relationships with other nodes. Our model does not only implement mobile nodes to distinguish new node from the nodes that have an existing network. But, It helped them to solve the ignorance that was occurring when mobile node moved far from exitingnodes.To achieve this right solution, we have embraced the mapping operator in between the evidence-opinion through subjective logic, as well as any new operators for internal logic such as fading and closing operators. Secondly, how our model can provide mobile nodes to formation their opinions to other nodes, depending on the authenticity of the evidence collected from the harmful and malicious behaviors of those nodes had helped. In our proposed model, direct and indirect opinion has been created from the evidence captured from an interactive with neighboring and neighbourhoods. In turn, it helped to classify mobile nodes as malicious or selfish node to their neighbours. Similarly, the observed view is generated from the captured sources by observing the contacts of neighboring node or itsnetwork. This helped to identify the mobile nodes and the malicious neighbour before interactive with them. The evidence captured from the received suggestions is used to establish the suggested concepts and then to identify and install trust relationships with other trusted nodes through mobile nodes. We describe how mobile nodes can be used to build trust relationships with existingnodes, using the feedback opinion that are being conducted for them.

REFERENCES

1. Meghanathan, Natarajan. “Impact of Static Nodes and Pause Time on the Stability of Connected Dominating Sets in a Mobile Ad Hoc Network.” International Journal of Wireless & Mobile Networks 7.4 (2015): 1–18. Crossref. Web.
2. Williams, Brad, and Tracy Camp. "Comparison of broadcasting techniques for mobile ad hoc networks." Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002. https://doi.org/10.1145/513824.513825
3. Cho, Sungsoon, and John P. Hayes. "Impact of mobility on connection in ad hoc networks." IEEE Wireless Communications and Networking Conference, 2005. Vol. 3. IEEE, 2005.
4. Stojmenovic, Ivan, Mark Russell, and Bosko Vukojevic. "Depth first search and location based localized routing and QoS routing in wireless networks." Proceedings 2000 International Conference on Parallel Processing. IEEE, 2000.
5. Martinelli pinto, rafael. “exact algorithms for arc and node routing problems.” n. pag. Crossref. Web.
6. Mishra, Dinesh, Yogendra Kumar Jain, and Sudhir Agrawal. “Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET).” 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies (2009): n. pag. Crossref. Web.
7. Dhumane, Amol, Rajesh Prasad, and Jayashree Prasad. "Routing issues in internet of things: a survey." Proceedings of the international

multiconference of engineers and computer scientists. Vol. 1. 2016.

8. Medhi, Deep, and Karthik Ramasamy. Network routing: algorithms, protocols, and architectures. Morgan Kaufmann, 2017.
9. Zhang, Xinming, et al. "A street-centric opportunistic routing protocol based on link correlation for urban VANETs." IEEE Transactions on Mobile Computing 15.7 (2015): 1586-1599. https://doi.org/10.1109/TMC.2015.2478452
10. Jadhav, Payal, and Rachna Satao. "A survey on opportunistic routing protocols for wireless sensor networks." Procedia Computer Science 79 (2016): 603-609.
11. Rathee, Priyanka. "Semantics for Delay-Tolerant Network (DTN)." Emerging Wireless Communication and Network Technologies (2018): 101–123. Crossref. Web. https://doi.org/10.1007/978-981-13-0396-8_6
12. Park, Patrick, Ingmar Weber, and Michael Macy. "The mesh of civilizations in the global network of digital communication." PloS one 10.5 (2015): e0122543.
13. Baek, Kyung Min, Dong Yeong Seo, and Yun Won Chung. "An Improved Opportunistic Routing Protocol Based on Context Information of Mobile Nodes." Applied Sciences 8.8 (2018): 1344. Crossref. Web.
14. Haywood, Maurice, Dewayne Brown, and Derrek Dunn. "Implementation of Wireless-Fidelity (Wi-Fi) Instruments for Rural Areas of North Carolina." Proceedings 2007 IEEE SoutheastCon (2007): n. pag. Crossref. Web. https://doi.org/10.1109/SECON.2007.342979
15. Natu, M., and A.S. Sethi. "Adaptive Fault Localization in Mobile Ad Hoc Battlefield Networks." MILCOM 2005 - 2005 IEEE Military Communications Conference n. pag. Crossref. Web.
16. Nage, Tebatso. "TCP-Aware Network Coding with Opportunistic Scheduling in Wireless Mobile Ad Hoc Networks." n. pag. Crossref. Web.
17. Ciobanu, Radu Ioan et al. "SPRINT-SELF: Social-Based Routing and Selfish Node Detection in Opportunistic Networks." Mobile Information Systems 2015 (2015): 1–12. Crossref. Web.
18. Gupta, Ganesh. "Identification Of Malicious Node In Dynamic Source Routing Protocol." Computer and Network Technology (2009): n. pag. Crossref. Web.
19. Jøsang, Audun. "Principles of Subjective Logic." Subjective Logic (2016): 83–94. Crossref. Web.
20. Uzunoğlu, Bahri. "An Adaptive Bayesian Approach With Subjective Logic Reliability Networks for Preventive Maintenance." IEEE Transactions on Reliability (2019).
21. Li, W.; Joshi, A.; Finin, T. CAST: Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies. // ACM transaction on distributed and parallel databases. 31, 2(2013), pp. 353-376. https://doi.org/10.1007/s10619-012-7113-3
22. "Reliability Evaluation of a Two-Unit Unrepairable System." Microelectronics Reliability 21.4 (1981): 615. Crossref. Web.
23. Liu, Shuai, Lihua Xie, and Frank L. Lewis. "Synchronization of Multi-Agent Systems with Delayed Input Information from Neighbors." 49th IEEE Conference on Decision and Control (CDC) (2010): n. pag. Crossref. Web. https://doi.org/10.1109/CDC.2010.5716980
24. Jiang, Tao, and John S. Baras. "Ant-based adaptive trust evidence distribution in MANET." 24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.. IEEE, 2004.
25. Virendra et al: Quantifying trust in Mobile ad hoc networks, in Proc. of KIMAS, 2005, April 18-21, 2005, Waltham USA.
26. R.B. Bobba, L. Eschenauer, V.D. Gligor, W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks", Proc. IEEE Global Telecomm. Conf. (Globecom), Dec. 2003.
27. Outola, Iisa, et al. "Optimizing standard sequential extraction protocol with lake and ocean sediments." Journal of radioanalytical and nuclear chemistry 282.2 (2009): 321-327. https://doi.org/10.1007/s10967-009-0183-7
28. Zomlot, Loai, et al. "Prioritizing intrusion analysis using Dempster-Shafer theory." Proceedings of the 4th ACM workshop on Security and artificial intelligence. ACM, 2011. https://doi.org/10.1145/2046684.2046694
29. Pooja Singh *et al.*, A Secure and Power-Aware Protocol for Wireless Ad Hoc Networks, International Journal of Advanced Trends in Computer Science and Engineering, 8(1), January – February 2019, 34 – 41. https://doi.org/10.30534/ijatcse/2019/07812019
30. Varun Chand H *et al.*, A Novel Approach using LoRaWRP for Emergency Vehicle Traffic Management, International Journal of Advanced Trends in Computer Science and Engineering, 8(3), May - June 2019, 349 – 353. https://doi.org/10.30534/ijatcse/2019/03832019