Characterization and modeling of uncertainty intended for a secured MANET

Md. Amir Khusru Akhtar [#1], G. Sahoo [*2]

[#] Department of Computer Science and Engineering
Cambridge Institute of Technology
Ranchi, Jharkhand, India
[1] akru2008@gmail.com

[*] Department of Information Technology
Birla Institute of Technology
Mesra, Ranchi, India
[2] gsahoo@bitmesra.ac.in

***Abstract*— Mobile ad-hoc network is a chaos for decades due to its dynamic and heuristic base. It employs several forms of uncertainty such as vagueness and imprecision. Vagueness can be taken in terms of linguistic assumptions such as grading and classification for the acceptance. Imprecision on the other hand can be associated with countable or noncountable assumptions such as the weights of acceptance calculated by the members of the MANET.**

This paper presents "Certainty Intended Model (CIM)" for a secured MANET by introducing one or more expert nodes together with the inclusion of various theories (such as monotone measure, belief, plausibility, evidence). These theories can be used for the characterization and modeling various forms of uncertainty. Further, these characterizations help in quantifying the uncertainty spectrum because, as much information about the problem is available we can transform from one theory to another. In this work we have shown how these theories and expert opinion helps to identify the setback associated with the MANET in respect of trust management and finally, enhances the security, reliability and performance of the MANET.

Keyword- Selfish node, expert node, reputation values, vagueness, imprecision, uncertainty, focal element

I. INTRODUCTION

The Mobile Adhoc Network is the self organized and distributed networks that allow communication without any preexisting infrastructure. In a self organized and infrastructure less network nodes have dual tasks of forwarding and routing that needs a cooperative and trusted network. The infrastructure less environment is the only reason that creates the heuristic base of the MANET. Unlike the fixed wireless network we have radio towers and access points for linking the nodes. The fixed architecture creates a successful and robust platform and therefore extensively deployed all over the humanity and offering a range of voice and data services. But a fixed infrastructure is not only the complete solution for all scenarios. Some applications such as in disaster relief and battle fields when the fixed infrastructure is either destroyed or unavailable, then an infrastructure less network is the only solution.

A cooperative network is based on trust and reputation. Different frameworks as defined in [1] have been considered to model trust networks. Trusts are derived from personal and referrals and finally in collective measure make reputations of things. For a MANET the network nodes are trustor as well as trustee because of its self organization. We can associate a MANET with a human society in which social implies the association of give and take. Similarly, a MANET is also self organized in nature and based on give and take. A node is a trustor as well as trustee and on the basis of this fact only we make a foundation for establishing a secured, robust and reliable MANET. Lots of models and systems are proposed but they use linguistic, countable and noncountable assumptions and give results in terms right or wrong and perhaps forget the main cause that is the uncertainty. In this paper we have proposed a Certainty Intended Model in which we are focusing on belief, plausibility and evidence theories to predict and forecast the exact and natural behavior of the environment. Our certainty intended model gives a positive impact on the existing solutions [2-5]. A finer result is obtained by involving a variety of theories and inclusion of expert node decision in trust management and reputation. Here, we join various theories to generate the monotone measure. Monotone measures are helpful in quantifying uncertainty that is not easy to measure in terms of quantitative estimates. For example, in this paper we have defined the trustworthiness of a node in the MANET by involving plausibility and evidence theories. It will enhance the result because we have non quantitative estimates from experts; not only in terms of how many beliefs and disbeliefs we have. The expert opinion improves the fitness of the decision in routing and forwarding

because these opinions are qualitative not quantitative. These theories can be used for the characterization and modeling various forms of uncertainty to identify the problem associated with the MANET. Further, these characterizations help in quantifying the uncertainty spectrum because as much information about the problem is available we can transform from one theory to another.

The rest of this paper is organized as follows: Section II presents the related work, assumptions and the inclusion of expert nodes. Section III presents the Certainty Intended Model (CIM). Section IV discusses the experiments and results. Finally, Section V highlights the conclusion and the future work in this field.

II. RELATED WORK, ASSUMPTION AND INCLUSION OF EXPERT NODES

A. Related Work

Characterization and modeling of uncertainty are needed for MANET because of the infrastructure less environment in which nodes have the dual responsibilities of forwarding and routing. In such a network nodes drop packets of others either of its honest causes such as collisions, channel errors, buffer overflows or because of selfish causes such as to save its energy or bandwidth. Thus, the selfish activity degrades packet transfer rate, increases packet delivery time and packet loss rate eventually creates Network Partitioning.

Because our work is based on uncertainty so, we enlighten the work done on trust management and reputation system. In a reputation system reputation values are taken into consideration to detect and classify selfish nodes in MANET. Different categories of the trust management system are proposed such as a centralized system in which the individual cooperates with the centralized system to manage the trust values but due to the self organized nature it is not practical. The second category involves global trust calculation for each node but it does not employ uncertainty. Finally, the third category describes the calculation of trust value maintained by each node in its own views of other nodes, and is suitable for our mobile adhoc network. The existing work such as CONFIDANT [2-3], CORE [4] and OCEAN [5] comes under the third category. Other works [6-7] Josang developed algebra in support of assessing trust relations. It uses a triplet of belief, disbelief, and uncertainty in each trust statement but, it fails to do so because a user cannot assign consistent values in all cases. The certainty-oriented reputation system proposed by Feng Li et. al [8] uses a triplet to represent a node's opinion (b, d, u) € $[0, 1]^3$: b+d+u =1. b, d, and u designate belief, disbelief, and uncertainty, respectively. When a new observation is made, if it is a successful forwarding, then α is updated. Otherwise, β is updated. Where α denotes successful forwarding and β denotes unsuccessful forwarding. It uses Beta distributions, Beta (α, β) for the Bayesian inference that accepts two parameters for continuous modification when new observations are made. The triplet (b, d, u) representing the node's opinion is derived from Beta (α, β). Still the work fails to describe the core dimension of trust. The authors concentrate on belief and disbelief. However, dividing trust into only belief or disbelief is not always appropriate. It is completely possible that $bel(\mathrm{S}) + bel(\bar{\mathrm{S}}) \neq 1$ and if it equals to 1 it is termed as a probability measure $prob(\mathrm{S}) + prob(\bar{\mathrm{S}}) = 1$. That's why, in this paper we have included plausibility and expert node opinion. We have taken monotone measures because it is valuable in quantifying uncertainty that is not easy to measure in terms of quantitative estimates.

The present status of reputation based systems is shown in the survey of trust and reputation management systems and reputation based schemes [9-10]. Several new works [11-13] shows the usage of reputation systems but uncertainty is still a major problem that reduces degree of confidence in trust information [8].

In this paper we have enhanced the reputation system by introducing one or more expert nodes opinion together with the inclusion of various theories and results shows the effectiveness of the proposed model.

B. Assumption

To enhance the reputation system various theories such as belief, plausibility and evidence theories and expert node opinion is incorporated. In this work we have taken a MANET without subnets and one having subnets or friendly groups [14]. The friendly group represents a group of cooperative nodes called regular nodes jointly with one expert node called border node having common objectives [14]. A node may be a member of one friendly group or more than one friendly group depending on the service requirements and reachability. We have involved one or more expert nodes whose opinion is essential to calculate uncertainty. The expert node is defined in section II-C.

C. Inclusion of Expert node

An expert node is defined in the literature [15-16], it represents an intelligent node of the Adhoc network, having a good knowledge of the network with the high computation capability to process and maintain the history of the transaction in the network. It could be a captain's Laptop in a combat zone or the device/devices having high processing power and battery lifetime.

In an Adhoc network to manage the trust and reputation expert node opinion is essential. That's why, we have introduced one or more expert nodes that maintain the history of trust and reputation because, it has good knowledge about the network. We have used the Friendly Group Model [14] to divide a MANET into more than

one friendly group which maximize the throughput and minimize the battery usage of the network. Fig. 1(a) shows a MANET without subnets with one or more than one expert nodes and Fig. 1(b) shows a MANET with subnets/friendly group having one or more than one expert nodes per subnets.

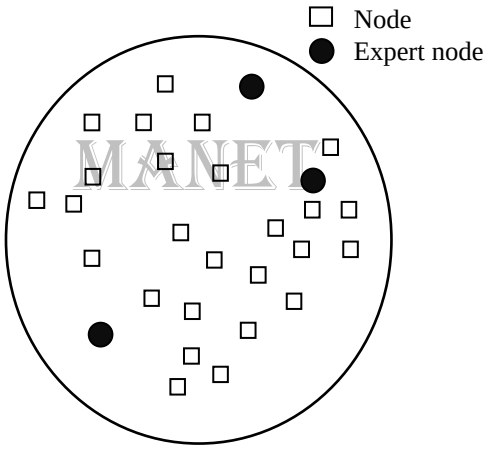

Fig. 1(a). Inclusion of expert nodes in a MANET without subnets

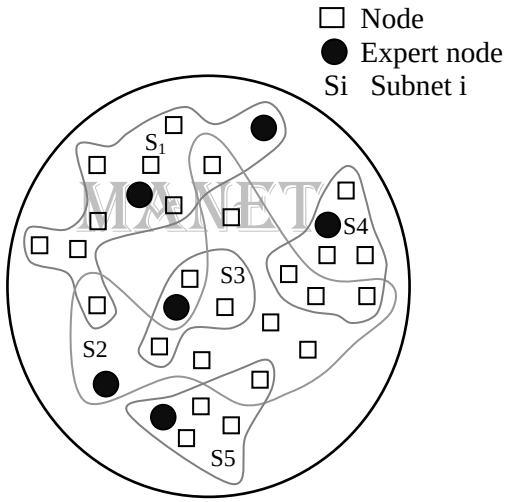

Fig. 2(b). Inclusion of expert nodes in a MANET having subnets/Friendly group

III. CERTAINTY INTENDED MODEL

This section presents how the vagueness and imprecision can be minimized using the proposed Certainty Intended Model (CIM) for a secured MANET. We have used various theories [17] to characterize and model diverse forms of uncertainty intended for a secured MANET. We have assigned values for membership to each crisp set that exists in the power set of universe, telling the degree of evidence or belief. The degree of belief and evidence are calculated on the basis of reputation values [2-5] and it shows that fuzziness is associated with our crisp values. The uncertainty associated with the boundaries of a regular and selfish class in form of belief and evidence is called a fuzzy set.

A. Evaluating basic evidence assignment (bea)

We have taken the concept of belief, plausibility measure and evidence theory from Fuzzy Logic with Engineering Applications [17]. To determine belief and plausibility measures a function m(S) can be defined on the subnet $(S \in P(N))$ where $P(N)$ is the power set, N is the mobile Adhoc network and S denotes the number of subnets in the MANET. The measure m (S) also shows a mapping of the power set to the unit interval,

$$m : P(N) \rightarrow [0, 1] \quad \ldots (1)$$

with the boundary conditions

$$m(\phi) = 0 \quad ...(2)$$

$$\sum_{S \in P(N)} m(S) = 1 \quad ...(3)$$

where ϕ shows no evidence about the subnet. The measure m(S) denotes the degree of belief of node i, of subnet S belonging to network N. The boundary condition is defined in Eqs. 2 & 3 in which value 0 means no evidence and 1 means complete evidence.

Now we can assign the belief measure using basic evidence assignment and it is

$$bel\ (S) = \sum_{O \subseteq S} m\ (O) \quad ... (4)$$

where O denotes all subsets of subnet S and m(S) define the degree of evidence for S while bel(S) is the total evidence in set S and its all subsets. Similarly the plausibility measure can be defined using measure m(S) as

$$pl\ (S) = \sum_{O \cap S = \phi} m\ (O) \quad ... (5)$$

The plausibility measure given in equation (5) describes the plausibility on the subnet S by combining total evidence in subnet S and the intersection of all evidences of subset S. The relationship between belief measure and plausibility measure is the joining of belief measure and the intersection of all evidences of set S.

B. Computing combined evidence using Dempster's theorem

We have obtained the combined monotone measure from more than one expert using Dempster's theorem [18]. In a noncooperative network we have defined two or more expert nodes to gather evidence on the basis of trust and reputation of all nodes lying in the network. Let the symbols m_1 and m_2 denotes the evidence calculated by two expert nodes on the power set P(N). The joint basic evidence assignment m_{12}(S) is obtained by combining evidence m_1 and evidence m_2 using the Dempster theorem as given in equation (6).

$$m_{12}(S) = \frac{\sum_{P \cap Q = S} m_1(P) \cdot m_2(Q)}{1 - F} \qquad \text{for } S \neq \phi \quad ...(6)$$

and the denominator F showing the normalizing factor defined as

$$F = \sum_{P \cap Q = \phi} m(P) \cdot m(Q) \quad ...(7)$$

where P and Q are the observed collection of nodes of subnet S measured by two expert nodes and these collections of nodes shows the same set of nodes.

IV. Experiments and Results

Experiments are performed on the discussed theories of section III to obtain the results. It shows the efficiency of the proposed Certainty Intended Model (CIM) in respect of the degree of confidence in trust information. The measures of evidence are provided by the expert nodes on the basis of reputation values. Reputation values are taken from the literature [2-5, 15-16, 19]. In this experiment the reputation values are taken in the range from 0 to 1 instead of 0 to 100 as defined in [19]. For example if the reputation value is 47.5 then we have taken 0.47. The reputation values are processed by the expert node as defined in [15-16].

A. Measures of evidence for MANET using one expert node

We have involved belief, plausibility and expert opinion in the calculation. The network is categorized in malicious and regular node, consisting of the singleton nodes R (regular node class) and M (selfish node class). The power set has $2^2 = 4$ elements having one null set as given in Eq. 2 i.e., ($m(\phi) = 0$) showing no evidence about the nodes, two singletons (R and M) and one ($R \cup M$) union of these two. The class ($R \cup M$) defines that the node has 50 % evidence in set R and 50% in set M. These classes are called focal elements. Let us assume that the measures of evidence provided by the expert node on the basis of reputation values for each one of the focal elements is shown in the 2nd column of Table I. Using Eqs. 4 & 5 gives the degrees of belief and plausibility for this evidence set as given in Table I.

TABLE I
Measures of evidence for a MANET

Focal element, Node$_i$	**Expert**		
	m(S_i)	**bel(S_i)**	**pl(S_i)**
ϕ	0.00	0.00	0.00
R	0.35	0.35	0.70
M	0.30	0.30	0.60
R∪M	0.35	1.00	1.00

Through these results we consider that the evidence supporting set R is at least 0.35 and possibly as high as 0.7 (plausibility), and believes the evidence supporting set M is at least 0.25 and possibly as high as 0.6 (plausibility). The union of set R and set S finally shows that the evidence supporting either of these sets (R∪M) is complete (i.e., bel = pl = 1). Finally, the true focal element can be obtained using the said theories because, dividing trust into only belief or disbelief are not always appropriate.

Through this result nodes cooperation can be measured and cooperating range can be defined for the cooperating nodes. Further, the obtained result can be used in the existing reputation based mechanisms [2-5] to isolate correct node from the routing paths. Thus, it enhances security by minimizing misbehaves and increases node strength in the network. The network performance and reliability will automatically increase when we have higher node strength in a network.

B. Combined evidence using Dempster theorem

We can join more than one expert node opinions using Dempster's rule of the combined evidence to enhance the degree of confidence in trust information. In this experiment two expert nodes having different opinions are employed to enhance the detection efficiency of selfish nodes on the basis of reputation values. Each expert is permitted to carry out tests and maintain history to collect information (evidence) about each of the nodes in a MANET.

Let us assume that a network has three types of selfish nodes and classified as High, Medium and Low selfish nodes called H, M and L respectively. The power set has 2^3 =8 elements consisting of eight focal elements. They are H, M, L, (H ∪ M), (H ∪ L), (M ∪ L), and (H ∪ M ∪ L) together with the null set having no evidence. We have not taken null set in our combined evidence because it gives only 0 values.

Let us assume that the measures of evidence provided by the expert nodes for each one of the focal elements is shown in the 2nd and 4th column of Table II. The combined evidence (m_{12}) measure is calculated using Eqs. 6 & 7 as shown in Table II. In order to calculate combined evidence first normalizing factor (F) is calculated using Eq. 7.

TABLE III
Combined evidence for a MANET

Focal elements, Node$_i$	**Expert node1**		**Expert node 2**		**Combined evidence**	
	***m_1*(Si)**	***bel_1*(S_i)**	***m_2*(S_i)**	***bel*(S_i)**	***m_{12}*(S_i)**	***bel_{12}*(S_i)**
H	0.00	0.00	0.00	0.00	0.01	0.01
M	0.05	0.05	0.10	0.10	0.21	0.21
L	0.10	0.10	0.10	0.10	0.10	0.10
H∪M	0.15	0.20	0.05	0.15	0.12	0.32
H∪L	0.05	0.15	0.05	0.15	0.12	0.15
M∪L	0.15	0.30	0.20	0.40	0.14	0.50
H∪M∪L	0.50	1.00	0.50	1.00	0.30	1.00

Then, the obtained result can be used in the existing reputation based mechanisms [2-5] to isolate correct node from the routing paths.

Thus, the proposed method helps to identify the setback associated with the MANET in respect of trust management and finally, enhances the security, reliability and performance of the MANET.

C. Advantage/Application of 'Certainty Intended Model' in trust management reputation systems

The Certainty Intended Model can be used in trust management reputation systems for the following reasons

- Measuring trust and reputation in terms of belief and disbelief is not always suitable.

- The monotone measure has been taken because it is valuable in quantifying uncertainty that is not easy to measure in terms of quantitative estimates.
- This model introduced one or more expert nodes to maintain the history of trust and reputation values of all nodes lying on the network. The expert nodes have good knowledge about the network and its opinion enhances the results. The opinion given by expert node are qualitative not quantitative.
- This model incorporates a plausibility measure because it is possible that the $bel(S) + bel(\bar{S}) \neq 1$ and if it equals to 1 it is termed as a probability measure $prob(S) + prob(\bar{S}) = 1$. Plausibility measure is associated with information that is more likely, or plausible.
- The proposed model gives more evidences for focal elements that can be used to characterize the true class. It enhances nodes strength in a network because it gives a better degree of confidence in trust information and excludes only correct selfish nodes from the routing paths.
- The proposed method helps to identify the setback associated with the MANET in respect of trust management and finally, enhances the security, reliability and performance of the MANET.

V. Conclusion and Future Work

A cooperative network is based on trust and reputation that is why the uncertainty reduction is important. In this paper, we have proposed "Certainty Intended Model (CIM)" for a secured MANET by incorporating various theories (such as monotone measure, belief, plausibility, evidence) and expert nodes opinions. The obtained result shows that the proposed model enhanced the trust management and reputation system and on that basis it surely enhances the security, reliability and performance of a MANET. The future work includes the inclusion of probability, possibility and necessity theories in our model to predict and forecast the exact and natural behavior of the network environment.

References

[1] A. Josang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[2] S. Buchegger and J. Y. Le-Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)", In Proceedings of MobiHOC'02, June 2002.

[3] S. Buchegger and J. Y. Le-Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks", In Proceedings of EUROMICRO- PDP'02, 2002.

[4] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce cooperation in Mobile Ad-hoc networks", in CMS'2002, Communication and Multimedia Security 2002 Conference, September 26-27, 2002, Portoroz, Slovenia / Also published in the book : Advanced Communications and Multimedia Security /Borka Jerman-Blazic & Tomaz Klobucar, editors, Kluwer Academic Publishers, ISBN 1-4020-7206-6, August 2002 , 320 pp, August 2002.

[5] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Report cs.NI/0307012, Stanford Univ., 2003.

[6] A. Josang, S. Marsh, and S. Pope, "Exploring Different Types of Trust Propagation," Proc. Int'l Conf. Trust Management, 2006.

[7] A. Josang and S. Pope, "Normalising the Consensus Operator for Belief Fusion," Proc. Int'l Conf. Information Processing and Management of Uncertainty, July 2006.

[8] Feng Li, Jie Wu, "Uncertainty Modeling and Reduction in MANETs", IEEE transactions on Mobile Computing, vol. 9, no. 7, july 2010.

[9] Han Yu, Zhiqi Shen, Chunyan Miao, C. Leung, and D. Niyato. "A survey of trust and reputation management systems in wireless communications", Proceedings of the IEEE, 98(10):1755 –1772, Oct 2010.

[10] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones, "A Survey of Reputation Based Schemes for MANET", The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK, 21-22 June 2010.

[11] E. Hernández-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog", IEEE Communications Letters, 16(5):642--645, 2012.

[12] Enrique Hernández-Orallo, Manuel D. Serrat Olmos, Juan-Carlos Cano, Carlos T. Calafate, Pietro Manzoni, "Evaluation of collaborative selfish node detection in MANETS and DTNs", MSWiM '12 Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, pp 159-166, 2012.

[13] Chun–Ta Li, Chou–Chen Yang, Min–Shiang Hwang, "A secure routing protocol with node selfishness resistance in MANETs", International Journal of Mobile Communications, Vol 10, pp 103-118, 2012.

[14] Md. Amir Khusru Akhtar and G. Sahoo, "A Novel Methodology for Securing Adhoc Network by Friendly Group Model", The Fourth International Conference on Networks & Communications (NetCoM) Chennai, LNEE, Springer, Sep, 2012.

[15] N.H. Saeed, M.F. Abbod, H.S. Al-Raweshidy, "IMAN: An Intelligent MANET Routing System", 17th International Conference on Telecommunications, 2010.

[16] Nagham Saeed, "Intelligent MANET Optimisation System", Ph.D. Thesis, School of Engineering and Design, Electronic and Computer Engineering Department, Brunel University, Brunel University, Feb 2011.

[17] Timothy J. Ross, "Fuzzy Logic with Engineering Applications", John Wiley and Sons (Asia) Pte. Ltd., Singapore 2007.

[18] Shafer, G., "A Mathematical Theory of Evidence", Princeton University Press, Princeton, NJ, 1976.

[19] Aruna Balasubramanian, Joy Ghosh, Xin Wang, "A Reputation Based Scheme for Stimulating Cooperation in MANETs", Proceedings of The 19th International Teletraffic Congress, Beijing 2005 (August).