Subjective Logic Based Trust Model for Mobile Ad hoc Networks

Venkat Balakrishnan
Vijay Varadarajan
Uday Tupakula

Information and Networked Systems Security (INSS) Research Group
Department of Computing, Macquarie University
Sydney, Australia 2109
{venkat, vijay, uday}@ics.mq.edu.au

ABSTRACT

In last five years, several trust models have been proposed to enhance the security of Mobile Ad hoc Networks (MANET). Nevertheless, these trust models fail to express the notion of ignorance during the establishment of trust relationships between mobile nodes. Furthermore, they lack a well-defined approach to defend against the issues resulting from recommendations. In this paper, we propose a novel subjective logic based trust model that enables mobile nodes to explicitly represent and manage ignorance as uncertainty during the establishment of trust relationships with other nodes. Our model defines additional operators to subjective logic in order to address the ignorance introduced between mobile nodes (which have already established trust relationships) as a result of mobility-induced separation. Second, we demonstrate on how mobile nodes formulate their opinions for other nodes based on the evidence collected from the benign and malicious behaviors of those nodes. We then describe on how mobile nodes establish trust relationships with other nodes using the opinions held for those nodes. Depending on the policies defined, these relationships are then used by our model to enhance the security of mobile communications. Third, we propose a novel approach to communicate recommendations by which no explicit packets or additional headers are disseminated as recommendations. This allows our model to defend against recommendation related issues such as free-riding, honest-elicitation, and recommender’s bias. Finally, we demonstrate the performance of our model through NS2 simulations.

Categories and Subject Descriptors

General Terms
Security, Algorithm, Design

Keywords
Trust, Reputation, Subjective logic, Security, and MANET

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright © 2008 ACM ISBN # 978-1-60558-241-2...$5.00.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a self-configuring network in which nodes rely on other nodes for communications. Security poses some fundamental challenges in such networks as they are not conducive to centralized trusted authorities. Although several secure routing protocols [1,2] have been proposed to defend against predefined attacks, they are vulnerable to new and dynamically changing attacks. Often the vulnerability results from the fact that the design of secure routing protocols does not take the trustworthiness of nodes into account. This has led to the development of several trust models [3-17], in which mobile nodes capture evidence of trustworthiness of other nodes to quantify and represent their behavior, and then to establish trust relationships with them. Trust models vary in their properties and also from the way they make trust enhanced decisions based on those established relationships and specified policies.

Perhaps at a more fundamental level, there is a lack of consensus on the definition of trust between the models. Furthermore, most if not all such models used in MANETs often fail to represent the aspect of ignorance during the establishment of trust relationships. Hence, a trust relationship between two nodes may not always reflect the actual relationship and consequently the executed decision may not always be accurate. For instance, existing nodes in a network may not have a record of past evidence to trust or distrust a newly joining node. Assigning an arbitrary level of trust for the new node poses several issues. The trust models address this issue either by pessimistically assigning a low [18] or neutral level of trust [9] or by optimistically assigning a high level of trust [6] to the new node. The purpose of pessimistic approach is to compel the new node to exhibit a consistent benign behavior from the point of entry. However, in some of these models, it is not always clear as to how the less trusted new node is selected for communications when nodes with high trust values exist. With the optimistic approach, the aim is to promptly identify whether the new node exhibits malicious behavior from the point of entry. Prompt identification is feasible because the high level of trust assigned for a new node decreases rapidly as malicious behavior increases. However, the optimistic approach fails to discriminate a new node from existing nodes, whose dynamically changing selective behavior has warranted the same level of trust. All these result from the fact that existing nodes fail to explicitly represent their ignorance of a newly joining node’s behavior. It also extends to nodes that have already established trust relationship with one another. For example, when a node moves away from a neighbor (due to mobility), it is unclear whether to consider the neighbor with the same level of trust or distrust during next interaction (when the neighbor
returns). It may be that the neighbor could retain its current behavior which may be either benign or malicious. Considering the neighbor to be benign, there is a chance for the neighbor to be compromised prior to next interaction. Alternatively, if the neighbor is considered to be malicious, then it may be repenting and expecting for an interaction to improve its relationship. These issues are often addressed by either increasing or decreasing the trust value of nodes in proportion to the duration for which they are out of communication. The main problem with this approach is that a node’s ignorance of other nodes is represented by either increasing or decreasing its trust value for them, which actually should denote to their benign or malicious behavior respectively. Hence, failing to explicitly represent the notion of ignorance and thereby uncertainty has fundamental impact on trust relationships.

In this paper, we present on how our novel subjective logic based trust model facilitates mobile nodes to explicitly represent and manage ignorance as uncertainty in their trust relationships with other nodes. Furthermore, we demonstrate on how our trust model allows mobile nodes to formulate their opinions for other nodes from the evidence of trustworthiness collected for those nodes. In our model, direct opinion is formulated from the evidence captured from the one-to-one interactions with neighbors, and it enables mobile nodes to classify their neighbors as either malicious or benign. Similarly, observed opinion is formulated from the evidence captured by observing the interactions of neighbors. It enables mobile nodes to identify malicious neighbors even before interacting with them. We assume that our model contains some monitor mechanism such as those in [9-12] to capture evidence for both direct and observed opinions. The evidence captured from derived recommendations is formulated into recommended opinion, and subsequently utilized by mobile nodes to identify and establish trust relationships with other trustworthy nodes. We then describe on how mobile nodes build trust relationships with other nodes using the opinions held for them, and also on how they communicate recommendations that are free from recommender's bias, honest-elicitation\(^1\), and free-riding\(^2\). The most important feature in our model is that every mobile node takes subjective decisions since it primarily believes in its opinions.

The paper is organized as follows. In Section 2, we discuss the characteristics and limitations of important related models. We then outline our assumptions and establish the context for subjective logic in Section 3. Section 4 presents our trust model and describes its operation in detail. We demonstrate the efficient performance of our trust model based on NS2 simulations in Section 5. Section 6 presents the concluding remarks.

2. BACKGROUND

Given that our focus is on the notion of ignorance, recommendation related issues, and the trust relationship itself, we first present the fundamental concepts of trust and trust management systems below. We then concentrate on the recommendation related issues in related trust models. In sequence, we discuss the incapability of those models to handle ignorance during the establishment of trust relationships between mobile nodes. Before summing up, we point to few models that attempt to address the notion of ignorance but however fail to handle the issues related to recommendations. To end with, we refer to how our trust model addresses those recommendation related issues by adopting a novel approach for communicating recommendations and a pointer to subjective logic based on which our work is built.

2.1 Trust and Trust Management Systems

In traditional trust management systems [19], trust enables a trustor to reduce uncertainty in its future interactions with a trustee, who is beyond the control of the trustor but whose actions are of interest to the trustor and affects the state of trustor. In other words, trust is a subjective probability which enables the trustor to take a binary decision by balancing between the known risks and the opinion held for trustee. In general, only known risks are considered, and the opinion presents trustee's direct relationship with the trustee based upon trustee's experiences. Other factors that influence the decision are time and context, where context accounts for the type of interaction between trustor and trustee, and the nature of application. Also, trustee's relationship with a second trustee based on its direct relationship with a first trustee and the first trustee's direct relationship with the second trustee is known as indirect relationship [20]. This is possible as nodes are allowed to share their opinions in the network, and typically it is achieved by disseminating recommendations.

In [21], trust management systems are characterized by the following components: (a) evidence manager to collect and classify evidence, (b) mathematical model to formulate evidence into opinion and then to use those opinions to predict the result of future interactions, and (c) policy manager to define decision policies for making decisions. With respect to capturing evidence, some models consider only the evidence from one-to-one interactions with other nodes [3], while some others may consider the recommendations received from other nodes [6-15]. As explained in Section 4, our model captures evidence from both one-to-one interactions and recommendations, and also by observing the interactions of neighbors. Related trust models also differ when it comes to the quantification and representation of captured evidence. For example, the captured evidence may be quantified and represented as either discrete [5] or continuous values [11]. In our model, trust is represented in continuous values since trust has been shown to evolve continuously over a period of time [11]. Also related trust models employ different mathematical models for establishing trust relationships between two nodes, such as graph theory [16], entropy [11], and Bayesian logic [17]. However, we resort to subjective logic in order to handle ignorance during the establishment of trust relationships between mobile nodes.

2.2 Recommendation Related Issues and Notion of Ignorance

For the purpose of this paper, we focus our discussion on the few well-known and recently proposed trust models [3-15]. Liu et al. proposed a trust model [5] in which evidence of trustworthiness is
collected by monitoring the behaviour of neighbours and recommendations received from them. Although they consider various approaches for distributing recommendations, they fall short to prevent a neighbour from maliciously reporting its next-hop neighbour as dropping or modifying packets. Pirzada et al. [6] proposed a similar approach for establishing trusted routes in Dynamic Source Routing (DSR) protocol [22]. They differ from the above approach by assigning trust weights to each link and then applying a shortest path algorithm based on the assigned weights to choose a trusted route. Also, they deploy hash function based proof-of-effort token to discourage a node from maliciously flooding a recommender with requests for recommendations. However, the proposed approach is unsuccessful in preventing a recommender from disseminating falsified recommendations. Ant Based Evidence Distribution (ABED) [7] uses a swarm intelligence based approach, which is modelled from ant colonies for distributing and discovering trust evidence. Interestingly, the approach assumes that all nodes would cooperate in disseminating and discovering evidence, which is unlikely in resource-constrained MANET.

To enforce reputation sharing through recommendations and to address honest-elicitation problem, Liu and Issarny [14] require a node to rate recommendations as either honest or dishonest after its experience with the recommended node. The node then shares recommendations only with nodes that have been sharing honest recommendations. Nevertheless, the proposal is vulnerable to collusion attack in which a colluding recommended node may exhibit benign behaviour to increase the reputation of a malicious recommender. Virendra et al. proposed a trust model [9] to establish group keys in MANET using trust relationships that exist among nodes. They adopt a five stage procedure to establish, and maintain trust relationship among nodes for which they accept recommendations from trustworthy neighbours. To lessen the effect of dishonest recommendations, they scale recommendations based on the trust relationships established with recommenders and then choosing either the largest or average of the scaled recommendations. However, it is unclear how the proposed approach enforces neighbours to communicate recommendations with other neighbours.

Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks (CONFIDANT) [13] collects evidence from direct experiences, and recommendations in the form of ALARM messages. Later it deploys the collected evidence to make trust decisions such as exclusion of malicious nodes and route selection. Rebah et al. proposed a trust model [10] similar to CONFIDANT, but their model primarily differs from CONFIDANT by enabling every node to broadcast its reputation to all neighbouring nodes. Analogous to [10, 13], Mundinger and Boudec [8] proposed a deviation test to accept only compatible recommendations and thereby to defend against honest-elicitation. However, such an approach is prone to overlook honest recommendations that would report unusual behaviour of neighbours, which is the key factor in detecting compromised benign nodes. Further, they are incapable of handling recommender's bias associated with the disseminated recommendations. Similar to [9], they are also ineffective in propelling neighbours to disseminate the recommendations. In [4], Eschenauer et al. recommend peer-to-peer based strategies for discovering and distributing evidence. Unlike related trust models, they define the requirements for mitigating recommender's bias and accepting recommendations in which the recommender has to collect and evaluate evidence for a recommended node in the same manner as the receiving node collects and evaluates evidence for the recommender. Alike [7], they adhere to swarm intelligence based approach for discovering and distributing evidence, and consequently inherit the corresponding vulnerabilities. Similar to our model, Ghosh et al. have proposed a framework [12] to empower mobile nodes to formulate their opinions for other nodes from the evidence collected from the benign and malicious behaviors of those nodes. In contrast to above models, the recommendations disseminated by mobile nodes not only contain their opinion for recommended nodes but also contain the digest of collected evidence. Nonetheless, the additional information falls short to alleviate the above-mentioned recommendation related issues. From our detailed study, we also observe that each of these trust models collectively fails to represent the aspect of ignorance, which is critical in evaluating the overall trustworthiness of nodes.

2.3 Uncertainty in Trust Relationships

Nevertheless, Yan Lindsay et al. proposed an entropy based trust model [11] in which trust is measured as uncertainty. The trust model proposed by Xiaqii et al. in [15] is close to our proposal as it uses subjective logic to express uncertainty. However, both these models fail to manage uncertainty when a node moves away from other nodes or the node is deficit of evidence for the benign and malicious behaviours of those nodes. This is critical for the node to evaluate its actual relationship with those nodes and to make accurate decisions. Again with respect to recommendations, all these trust models [4-15] are either prone to or lack a well-defined approach to defend against honest-elicitation. Furthermore, the dissemination of recommendation in these models is also prone to free-riding, recommender's bias, and overhead. Interestingly, in Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) [3], Bansal and Baker address the issues associated with the dissemination of recommendation by considering only the evidence collected from direct observations. Although our trust model is synonymous with OCEAN in addressing the issues related to recommendations, we differ from OCEAN by considering the advantages of recommendations and deploying a novel approach to derive recommendations within the constraints of MANET, which we will explain in detail in Section 4.6

Our work builds upon Josang's work on subjective logic [23], which has sound mathematical foundation in dealing with evidential beliefs. Rooted in the Dempster-Shafer theory [24] and with the ability to explicitly represent and manage a node’s ignorance, subjective logic emerges as an attractive tool for handling trust relationships in inherently dynamic, open and uncertain networks such as MANET. Other extensions of subjective logic include applications in mobile agents [25] and grid computing [26]. The former utilizes subjective logic to model trust relationships between mobile agents and thereby makes trust enhanced security decisions for electronic transactions. The latter attempts to enhance grid security using trust management systems. Nevertheless to the best of our knowledge, subjective logic based trust management system are reasonably new to MANET and waits for an in-depth analysis. The context of subjective logic in our model is given in the following Section and a formal description of subjective logic is presented in the Appendix A.
3. CONTEXT FOR OUR MODEL

3.1 Assumptions

In our model, nodes are assumed to perform fixed range transmissions using Omni-directional antennas. Our model concentrates on enhancing the security of network layer and does not rely on any tamper proof hardware. In this paper, we address only the reactive routing protocols because of their ability to discover routes on demand. However, our model is applicable to both proactive and hybrid routing protocols with minor modifications, which we leave for future work. Amongst the reactive protocols, we have chosen the Ad-hoc On-demand Distance Vector (AODV) protocol [27] to present the details of our trust model. In order to take advantage of redundancy in MANET, we choose On-Demand Multi Path Distance Vector Routing in Ad Hoc Networks (AOMDV) [28], which is one of the extensions proposed for the AODV protocol.

We refer to the wireless range of a node as its environment. For ease of explanation, we define the sequence of a successful route discovery followed by data flow as a communication flow. Similar to other trust models [4,11], our trust model complements crypto-based secure routing models [1,2]. We refer to the nodes that either modify the routing information during route discovery and/or drop the packets intentionally to disrupt the data flow and/or selfishly save battery resource as malicious nodes; such behaviours are referred to as misbehaviours. In contrast, the behaviours that conform to the routing protocol specification are referred to as benign behaviours.

3.2 Subjective Logic

Subjective logic uses the term opinion (o) to represent evidential beliefs and the opinion itself has three dimensions: belief (b), disbelief (d), and uncertainty (u). Belief and disbelief are summarized from the evidence captured for benign and malicious behaviours respectively. Uncertainty represents the ignorance or level of confidence in a node’s knowledge. For instance, (1) presents an opinion (\(o_{b}\)) in which belief (\(b_{b}\)) gives the probability of node A’s trust on node B depending on B’s benign behaviour. Similarly, disbelief (\(d_{b}\)) presents the probability of A’s distrust on B depending on B’s malicious behaviour. Finally, uncertainty (\(u_{b}\)) represents the probability of A’s ignorance on B. In (1), ‘x’ denotes the mode (direct, observed, and recommended) through which evidence is captured. Belief, disbelief, and uncertainty satisfy (2). A formal description of subjective logic and our definitions of new operators to subjective logic are given in Appendix A.

\[
\begin{align*}
A_{ob} = \{ & b_{b}, d_{b}, u_{b} \} \\
& \left\{ b_{b} + d_{b} + u_{b} = 1, b_{b}, d_{b}, u_{b} \in [0,1] \right\}
\end{align*}
\]

(1)

(2)

As detailed in the next Section, every mobile node captures the evidence of trustworthiness to compute its opinion for other nodes in the following ways: (a) one-to-one interactions with neighbors (direct opinion), (b) observing the interactions of neighbors (observed opinion), and (c) recommendations derived from other nodes (recommended opinion). We have extended the evidence-to-opinion mapping operator of subjective logic in Appendix A.1, such that mobile nodes can represent ignorance during the establishment of trust relationships with other nodes and also when they move away from those nodes due to mobility. However, the evidence-to-opinion mapping operator holds only for direct and observed opinions, since mobile nodes collect evidence for these opinions literally from the other node’s benign or malicious response towards a request. In the case of recommended opinion, mobile nodes derive evidence from the opinion held by recommenders and amalgamate those evidence into recommended opinion using the discounting (\(\otimes\)) and consensus (\(\oplus\)) operators detailed in A.3. Unlike the evidence-to-opinion mapping operator of direct and observed opinions, the operators defined for recommended opinion fail to address the uncertainty introduced when nodes move away from each other. We have addressed this shortcoming by proposing a new operator known as fading operator (\(\ominus\)) in Appendix A.4. Furthermore, Appendix A.2 details on how a mobile node can combine direct, observed, and recommended opinions into a single opinion known as global opinion. Appendix A.5 then explains on how to classify a global opinion into trustworthy, uncertain, or untrustworthy.

4. OUR TRUST MODEL

In the following, first we present the formalisation of our trust model. Second, we discuss the operation of our trust model during a routing cycle to demonstrate its role in enhancing the security of communications using subjective trust decisions. We then describe the operation of trust evaluations that forms the basis for all subjective trust decisions. Finally, we describe the process of capturing evidence for different types of opinion (direct, observed, and recommended), which is then used in trust evaluations.

4.1 Formal Trust Model

In our trust model, we consider the notion of trust described in [29]: “Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is not a fixed value associated with the entity but rather subject to its behaviour and applies only within the context and at a given time”.

Our trust model operates independently at every node. For instance our trust model at any node ‘i’ is represented using the following structure, \(T_{M_{i}} = (N_{i}, R_{i})\). If ‘N’ is the set of all nodes in network, then ‘N\(_{i}\)’ is the set of all nodes excluding ‘i’ such that \(N = N - \{i\}\). Finally, ‘R’ presents the set of trust relationships between ‘i’ and the list of nodes in ‘N\(_{i}\)’. Following expression presents the trust relationship ‘R\(_{ij}\)’ between nodes ‘i’ and ‘j’, which is a tuple of eight attributes:

\[
R_{ij} : \{T, \Omega, E, P, N, \sigma, \tau, \delta\}
\]

In the above expression, node i’s trust ‘T’ for node ‘j’ is given by its global opinion (\(o_{gb}\)) for ‘j’. Equation (A4) of Appendix A.2 presents the derivation of \(o_{gb}\), and \(\Omega\) contains the sub-opinions held for ‘j’ based on the evidence collected through various modes (direct, observed, and recommended). ‘E’ denotes the set of events (route request, route reply, route error, and data flow) from which the evidence for benign and malicious behaviours can be captured. Sets ‘P’ and ‘N’ contain the positive (p) and negative (n) evidence respectively (Appendix A.1), for both direct (\(o_{dir}\)) and observed (\(o_{ob}\)) opinions. ‘a’ is the set of timestamps indicating when the opinions (direct, observed, and
recommended) were initialized or last revised; hence ‘σ’ has a bijective relation with respect to ‘Ω’. The average duration taken for a communication flow by ‘i’ is given by ‘τ’. Recall that ‘τ’ is used to calculate the number of intervals for which there has been no update for each type of opinion (direct, observed, and recommended). Finally, ‘δ’ refers to <δ₀, δₜ>, where ‘δ₀’ denotes the name of cluster, and δₜ represents the type of cluster relationship (in the cluster-based MANET). The type of cluster defines whether it is an intra-cluster or inter-cluster relationship. In networks where there are no clusters, each node is treated as an individual cluster for simplicity.

4.2 System Operation

Our model assists AOMDV protocol in making decisions for the following cases, whether to - (a) accept or reject a route that is given by a forward-link (next-hop) towards the target, (b) record or discard a route that is given by a backward-link (previous-hop) towards the originator, (c) choose a route (forward-link) from available routes (forward-links) for the target, and (d) send a packet to the target or to forward a packet on behalf of originator. The decision for each of the above cases depends on the corresponding trust evaluation. In turn, trust evaluations rely on the opinions (direct, observed, and recommended) held for one or more nodes involved in the evaluated case.

Let us consider the scenario shown in Figure 1, where node S is the source and D is the destination for communication flow. Nodes A, B, I, X, and Y are the intermediary nodes that form the path from S to D. From here onwards, we will use this as the running scenario for explaining trust model's operations.

Whenever S wishes to send data packets to D, it initially checks for a route or a forward-link (next-hop) to D. On finding a route, S evaluates the route to decide whether the route can be trusted or not. Although S would have evaluated the route's trustworthiness before recording the route, it also continues to evaluate the route's trustworthiness prior to every deployment. This is due to the fact that trust is not monotonic; hence trust for a route may change anytime between its point of entry and deployment. Given that there is more than one route to D and many may be trustworthy, the route with highest trust is chosen for communication flow. If the trust evaluation asserts all available routes as uncertain, then the route or forward-link (next-hop) with lowest uncertainty is chosen for communication. This scenario arises during the initial stages of network deployment, as nodes are neither trusted nor distrusted. Alternatively, if only untrustworthy routes exist or there is no route available to D, then S initiates a new route discovery cycle to D. Prior to the initiation, S purges the untrustworthy routes from its route cache.

In our model, intermediary nodes perform the following trust evaluations. Let us consider the operation at node I in Figure 1. It evaluates the trustworthiness of previous-hop in order to set the previous-hop as the backward-link (or route) to S. This is in accordance with the expectation that the route is likely to be free from modification, only if the previous-hop is trustworthy. Also, it evaluates the trustworthiness of next-hop in order to set the next-hop as the forward-link (or route) to D. This is in accordance with the expectation that the route will be free from modification and the corresponding data packets will reach D, only if the next-hop is trustworthy. Finally, I evaluates the trustworthiness of packet by evaluating the trustworthiness of both S and D. This is because the intermediate nodes forward packets only for the sake of both S and D. Trust evaluations for both route (forward-link or backward-link) and packet (source and destination) are described in the following Section 4.3. An exception to the above set of evaluations at I is the route request event - for which the next-hop is unknown due to the broadcast nature. In such a situation, I evaluates the trustworthiness of previous-hop and packet. The trust evaluations are deemed successful, only if the evaluated opinion is asserted as either trustworthy or uncertain.

Similarly, D accepts its previous-hop as the backward link to S only after evaluating the trustworthiness of previous-hop. Otherwise, D may use an alternative trustworthy route to reach S or initiate a new route discovery cycle to S.

4.3 Trust Evaluation

Let us assume that every node sets its direct, observed, and recommended opinions for all other nodes to the default opinion, \( \omega_0 = (0.0, 0.0, 1.0) \), during the initial stage of deployment. Let us now consider the trust evaluation of a route. Node ‘i’ evaluates its trustworthiness for node ‘j’ (forward-link or backward-link) in two steps. As shown in (A4) in Appendix A.2, \( \mathcal{E} \) combines the opinions (direct, observed, and recommended) held by ‘i’ for ‘j’ into a global opinion \( \omega_{glo} \). Prior to the combination, direct and observed opinions are updated using evidence-to-opinion mapping operator (Appendix A.1), and recommended opinion is updated using \( \mathcal{O} \) (Appendix A.4) in proportion to the duration for which there has been no evidence. \( \omega_0 \) (Appendix A.5) is then applied to \( \omega_{glo} \) to evaluate the nature of trust relationship (trustworthy, untrustworthy, and uncertainty) ‘i’ holds with ‘j’. If the evaluation leads to either a trustworthy or uncertain relationship, then ‘j’ is recorded as the route, i.e., forward-link or backward-link to the target or originator respectively. Otherwise, the route is discarded along with the packet. As mentioned earlier, a route pertaining to an uncertain relationship is recorded to help the establishment of trust relationship during the initial stage of deployment and to meet the conditions when trustworthy routes are unavailable.

Similarly, node ‘i’ evaluates the trustworthiness of a packet ‘pkt’ in two steps. Initially, ‘i’ uses \( \mathcal{O} \) to compute the global opinions \( \omega_{glo} \) and \( \omega_{glo}^{\text{pkt}} \) for the source S and destination D of packet respectively. Recall that ‘i’ updates its direct and observed (using the evidence-to-opinion mapping operator), and recommended (using \( \mathcal{O} \)) opinions for both S and D in proportion to the duration for which there has been no evidence. Node ‘i’ then computes its opinion \( \omega_{glob} \) for the packet ‘pkt’ by applying \( \mathcal{O} \) to \( \omega_{glo}^{\text{pkt}} \) and \( \omega_{glo} \), which is given in (3). Finally, ‘i’ evaluates its
trustworthiness for the packet by applying \( \sigma \) to \( \omega_{pk} \). Node \( i \) forwards the packet only if the evaluation leads to either a trustworthy or an uncertain relationship.

\[
\omega_{pk} = (\sigma_S \odot \sigma_D)
\]

4.4 Direct Opinion

We define node \( i \)'s direct opinion \( \omega_{dir} \) towards node \( j \) as its trust on \( j \) depending on the evidence collected from the one-to-one interactions with \( j \). The evidence is collected by forwarding a packet to \( j \) and then monitoring its successive forwarding of the same packet. The evidence captured for \( j \) is considered as benign behaviour, only if the packet has been forwarded without any modification. Alternatively, if the packet has been modified or intentionally dropped to disrupt the data flow, then the evidence is considered as a malicious behaviour. Further, \( j \) is excluded from corresponding communication flow until the completion of flow due to its malicious behaviour.

After capturing the recent evidence (benign or malicious), node \( i \) revises either \( p \) or \( n \) for next-hop \( j \) at \( P \) or \( N \) respectively, as mentioned in Section 4.1. Also, \( i \) revises \( k \), the duration for which there has been no interaction between \( i \) and \( j \). Finally, \( i \) updates its direct opinion \( \omega_{dir} \) for \( j \) by following the evidence-to-opinion mapping operator defined in (A1) of Appendix A.1.

4.5 Observed-Opinion

The notion of capturing evidence from the interactions of neighbours is inspired from social psychology, where an individual’s behaviour in a society is observed whenever the individual deviates from normal behaviour. In turn, it explains the psychology of observers, who are interested in remembering the individuals known for misbehaviours. From the perspective of observers, the objective is to take advantage of their observations, so that they can be cautious when they interact with the observed individuals in future, who are known for misbehaving. Note that the definition of a normal behaviour may be subjective from the perspective of an observing individual, though a generic definition may exist in terms of social laws. In addition, observers fail to consider the individual’s normal behaviours unless it is of direct benefit to them. However, it is noted that observers do consider an extraordinary behaviour of individual as a benign behaviour.

We consider node \( Y \) in Figure 1 to study the process of \( Y \) capturing evidence and updating its observed opinion \( \omega_{obs} \) for node \( X \). First, \( Y \) overhears the packet forwarded by node \( I \) to \( X \), and then the packet forwarded by \( X \) on behalf of \( I \). Node \( Y \) does not perform any further operations, if \( X \) has forwarded the packet without any modification. From the perspective of \( Y \), forwarding a packet by following the specification of AOMDV protocol is a normal behaviour. Further, it assists in counteracting colluding attacks. Otherwise, \( I \) and \( X \) may be exchanging dummy packets between them in order to increase their observed opinions at \( Y \). Alternatively, \( Y \) revises ‘n’ for \( X \) at its ‘N’ as mentioned in Section 4.1, only if \( X \) has modified the packet to disrupt the data flow. Node \( X \) is then excluded from the corresponding communication flow until the completion of flow. Node \( Y \) does not consider the evidence of \( X \) dropping \( I \)'s packet since it is hard for \( Y \) to ascertain the precise reason behind the packet drop. Interestingly, \( Y \) revises ‘p’ for \( X \) at its ‘P’ as mentioned in Section 4.1, only if \( X \) has reported a genuine broken link to \( I \). This is considered to be an extraordinary action in resource constrained MANET. Note that any falsified report on a link would be captured as an evidence for \( X \)'s malicious behaviour at its other-end neighbour, i.e. \( D \), and also at other observing neighbours.

Node \( Y \) then revises \( k \), the duration for which there has been no observation for \( X \). Finally, it updates its observed opinion \( \omega_{obs} \) for \( X \) by following the evidence-to-opinion mapping operator defined in (A1) of Appendix A.1. Note that \( X \) not only loses direct opinion \( \omega_{obs} \) at its previous-hop for modifying the packet, but also observed opinion \( \omega_{obs} \) at all its observing neighbours ‘j’.

4.6 Recommended Opinion

For ease of explanation, the node that provides a recommendation is referred as recommender and the recommended node is referred as recommendee. In [6-15], recommendations are communicated among nodes by disseminating explicit data packets or additional headers. In these models, the notion of disseminating recommendations corrupts trust decisions for the following reasons. First, they lack well-analyzed approaches to determine a recommender’s bias accompanied with the recommendation. Second, they fail to investigate whether the recommender exhibits free-riding and honest-elicitation. Even when these models do attempt to address these problems, they are unable to defend against those behaviours completely. In addition, the dissemination of recommendations increases the overhead and hence degrades the performance of network.

In general, a recommender’s opinion for a recommendee can be deduced from the disseminated recommendation. Given that there has been no change in the deduced opinion, it is then possible to determine whether the recommender will forward or discard a subsequent packet received from the recommendee. The reasoning holds as long as the context for both disseminated recommendation and deduced opinion is the same. In our model, we reverse the above reasoning to derive recommendations for a recommendee, rather than requesting the recommenders to disseminate recommendations as explicit messages or additional headers. In other words, a node deduces its previous-hop’s intention to forward or discard an upstream packet received from the originator as previous-hop’s opinion for the originator. The node then derives the deduced opinion as previous-hop’s recommendation for the originator. Here, the previous-hop is the recommender and the originator is the recommendee. The node derives such recommendations from the route (forward-link or backward-link), only if the received packet is considered as trustworthy for forwarding. Recall from Section 4.3 that a node forwards a packet only if it trusts its previous-hop (backward-link), next-hop (forward-link), source (originator), and destination (target). Similar condition also applies to the previous-hop and to all upstream intermediate nodes until the originator of packet. Also in our model, recommendations are derived only once for a communication flow, especially during the data flow. This enables our model to derive recommendations only from trustworthy routes as both direct and observed opinions would capture the evidence for malicious behaviours during route
discovery and accordingly prevent the establishment of malicious route.

Let us again consider the scenario shown in Figure 1, where X receives a data packet from I, whose origin is S. As mentioned earlier, X prepares to forward the received data packet, only if the packet satisfies all the trust evaluations mentioned in Section 4.3. Subsequent to successful evaluations, X deduces node I’s (backward-link) intention to forward the packet in favour of S, as node I’s opinion for S. As discussed earlier, X then derives the deduced opinion as node I’s recommendation for S. This is based on X’s inference that node I should have either a trustworthy or uncertain relationship with S in order to forward the packet originated by S. From this inference, X postulates I’s global opinion for S as $\omega_{X}^{\text{infer-glo}} = (\text{Threshold}, 0, (1-\text{Threshold}))$, where node I’s belief $\omega_{X}^{\text{infer-glo}}$ and uncertainty $\omega_{X}^{\text{infer-glo}}$ for S is set to Threshold and (1-Threshold) respectively. Given that X’s global opinion $\omega_{X}^{\text{glob}}$ for S using the inferred recommendation $\omega_{X}^{\text{infer-glo}}$ and its global opinion $\omega_{X}^{\text{glob}}$ for I. The operation is achieved by applying $\otimes$, such that $\omega_{X}^{\text{all-rec}} = \omega_{X}^{\text{glob}} \otimes \omega_{X}^{\text{infer-glo}}$ which is given in (A5) of Appendix A.3. Finally, X updates its overall recommended opinion $\omega_{X}^{\text{all-rec}}$ for S by applying $\otimes$ according to (A7) of Appendix A.4, and then integrates the result with $\omega_{X}^{\text{rec}}$ using (A6) of Appendix A.3. The same set of operations is then applied by D to derive X’s recommendation for S.

In summary, the proposed approach prevents a node’s opinion from being corrupted by the recommender, and this in turn facilitates the node only to believe in its opinions. Hence, the node better resolves the issues concerned with the recommender’s bias. Since recommenders do not forward their opinions explicitly, they are prevented from exhibiting both honest-elicitaction and free-riding behaviours.

5. SIMULATION AND ANALYSIS

We have used NS2 for our simulations. It uses random waypoint model for mobility, in which a node starts from a random point, waits for a duration determined by pause time, then chooses another random point, and moves to the new point with a velocity uniformly chosen between 0 and maximum velocity $V_{\text{max}}$. We fixed the transmission range for a node to 250m, and the Medium Access Control (MAC) protocol and routing protocol to IEEE 802.11 and AOMDV respectively. We selected Constant Bit Rate (CBR) traffic with a data rate of 2Mbps and packet size of 512 bytes. Remaining parameters are summarized in Table 1. Mobile nodes which do not have trust model are called as AOMDV nodes and mobile nodes with our trust model enabled are known as TME nodes. Nodes that perform either modification or packet dropping attacks are called as malicious nodes. We analysed our trust model for mobility, in which a node starts from a random point, and moves to the new point with a velocity another random point, and moves to the new point with a velocity.

<table>
<thead>
<tr>
<th>Simulation Parameters</th>
<th>Parameter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total simulation time</td>
<td>500 s</td>
</tr>
<tr>
<td>Total number of nodes</td>
<td>50</td>
</tr>
<tr>
<td>Max number of malicious nodes</td>
<td>25</td>
</tr>
<tr>
<td>Max velocity ($V_{\text{max}}$)</td>
<td>20 m/s</td>
</tr>
<tr>
<td>Max pause time</td>
<td>10 s</td>
</tr>
<tr>
<td>Simulation area</td>
<td>1200x1200 m2</td>
</tr>
<tr>
<td>Total constant bit rate connections</td>
<td>10</td>
</tr>
<tr>
<td>Packet rate</td>
<td>4 packets/s</td>
</tr>
<tr>
<td>Threshold</td>
<td>0.60</td>
</tr>
<tr>
<td>Default values</td>
<td>$\omega_{S} = (0.0, 0.0, 1.0)$; p = 0, n = 0, and k = 1</td>
</tr>
</tbody>
</table>

5.1 Scenario 1

As shown in Figure 2(a), the PDR for AOMDV nodes fall steeply with increasing number of malicious nodes. This is due to the characteristic of AOMDV nodes not being able to distinguish between benign and malicious behaviours. As a result they are prone to select modified routes with either shortest hop-length or lowest sequence number, which consequently disrupts the data flow. However, TME nodes perform better due to their ability to make subjective decisions as mentioned in Section 4.2. This is because TME nodes are able to manage ignorance as uncertainty in their relationship with other nodes, and hence make better decisions. The enhanced efficiency of TME nodes in differentiating malicious nodes from benign nodes originates from their direct, observed and recommended opinions. Observed opinion enables TME nodes to short-list malicious neighbours even before interacting with them. This leaves TME nodes to classify only a lesser proportion of neighbours as either benign or malicious based on direct interactions. On the other hand, recommended opinion increases the probability of TME nodes to establish trustworthy relationship with other TME nodes. Further Figure 2(a) confirms that TME nodes do not incur overhead, as the PDR for both TME and AOMDV nodes is same in the absence of malicious nodes. This is due to the ability of TME nodes to capture evidence within the constraints of MANET without incurring additional overhead.

Figure 2(b) again confirms that TME nodes are successful in establishing valid routes despite the increasing proportion of malicious nodes. However as the proportion of malicious nodes increases, the packet loss for TME nodes also increases. The reason rests on the decision to propagate only a trusted packet, and that too only through trustworthy previous and next hops. As expected, the latency for TME nodes is marginally greater than
the latency of AOMDV nodes in Figure 2(c) for the following reasons: (a) initiation of route discoveries to find trustworthy routes when previously discovered route contains malicious node(s), (b) the likelihood of trustworthy routes being longer in hop-length than the optimal hop-length, and (c) the time taken for making trust decisions at every hop. Note that the latency corresponds to the PDR in which high PDR attributes to routes with variable lengths, while low PDR predominantly attributes to routes with shorter hop-length.

5.2 Scenario 2

In Figure 2(d), PDR for both TME and AOMDV nodes is low at 0m/s. The decreased performance is due to the nodes not being able to establish a valid route when they are positioned in a malicious environment. In the case of TME nodes, observed opinion prevents the routes from being established through malicious neighbours. However, the PDR increases for both TME and AOMDV nodes as they become mobile, which can be confirmed by the reduced packet loss in Figure 2(e). The PDR then decreases as the velocity increases beyond the optimal value 15m/s. The reduction results from broken links, which is the root cause for loss of data packets and increased route discoveries.

Similar to Figure 2(c), the latency for TME nodes is higher than the latency of AOMDV nodes (Figure 2(f)). At low velocities, latency results from the time taken for making trust decisions at every hop. At high velocities, latency results from the increased route discoveries and trusted routes being longer in hop-length than the optimal hop-length.

In summary the simulation results confirm that TME nodes make better routing decisions due to their ability to differentiate benign nodes from malicious nodes, and to better represent their trust relationship with other nodes by managing ignorance as uncertainty. In addition, they also do not incur overhead and perform better by eliminating the issues related to recommendation (such as recommender’s bias, honest-elicitation, and free-riding) and operating within the constraints of MANET.

6. CONCLUSION

In this paper, we have proposed a novel subjective logic based trust model for mobile nodes through which they explicitly represented and managed ignorance as uncertainty in their trust relationships with other nodes. Our model not only enabled mobile nodes to distinguish new nodes from existing nodes, but
also facilitated them to address the ignorance that resulted when they move away from other nodes. To achieve this, we have adapted the evidence-to-opinion mapping operator of subjective logic and also defined new operators to subjective logic such as the fading and decision operators.

Second, we have shown how our model has facilitated mobile nodes to formulate their opinions for other nodes depending on the evidence of trustworthiness collected from the benign and malicious behaviors of those nodes. In our model, direct opinion is formulated from the evidence captured from the one-to-one interactions with neighbors. In turn, it enabled mobile nodes to classify their neighbors as either malicious or benign. Similarly, observed opinion is formulated from the evidence captured by observing the interactions of neighbors. It enabled mobile nodes to identify malicious neighbors even before interacting with them. The evidence captured from derived recommendations is formulated into recommended opinion, and subsequently utilized by mobile nodes to identify and establish trust relationships with other trustworthy nodes. We have then described on how mobile nodes can build trust relationships with other nodes using the opinions held for them. We have specified decision policies to demonstrate on how trust relationships can be used to enhance the security of communications by isolating malicious nodes and selecting only benign nodes for communications.

Third, we have deployed a novel approach to communicate recommendations in which mobile nodes did not disseminate explicit packets or additional headers as recommendations. This feature enabled our model to defend against free-riding, and allowed it to operate within the limitations of MANET. Furthermore, it defended against honest-elicitation and recommender's bias, since nodes did not exchange their ratings for communicating recommendations. The most important feature in our model is the capability of mobile nodes to take subjective decisions since they primarily believes in their opinions. We have confirmed the effectiveness of our trust model using NS2 simulations.

7. ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers for valuable comments and also Pekka Nikander for his suggestions in preparing the final version of the paper. Also, we would like to thank Defence Signals Directorate (DSD), Australia for their financial support of this research project under Security in National Information Infrastructure Program (SNIIP).

8. REFERENCES

APPENDIX A

It has been shown in [30] that the probability density over binary event spaces can be expressed as beta Probability Density Function (PDF), denoted as ‘beta (α,β)’. Furthermore, it has been shown in [23] that the subjective logic’s opinion (ω) can be bijectively mapped onto beta PDF parameters. A number of operators have been defined for subjective logic [23]; some represent generalisations of binary logic and probability calculus operators, while others are unique to belief theory because they depend on belief ownership. We inherit only the consensus (⊗) and discounting (⊕) operators, where ‘⊗’ is used to combine different types of opinion (direct, observed, and recommended) into a single opinion so that mobile nodes can make an objective judgement about another node’s trustworthiness, and ‘⊕’ is used by mobile nodes to derive recommended opinion for another node using the recommender’s opinion. We also extend the evidence-to-opinion mapping operator of subjective logic, so that mobile nodes can represent ignorance during the establishment of trust relationships with other nodes and also when they move away from those nodes due to mobility. However, evidence-to-opinion operator holds only for direct and observed opinions for the reasons explained in Section 3.2. Since recommended opinion does not account for the uncertainty introduced when nodes move away from each other, we address this by proposing a new operator known as fading operator (⊙). Lastly, we propose another new operator known as comparison operator (◻) so that mobile nodes can make trust enhanced decisions using the opinions held for other nodes.

A.1. Evidence-to-Opinion Operator

For either direct or observed opinion, let ‘p’ and ‘n’ express the number of evidence captured for benign and malicious behaviours respectively. We have extended ‘k’ to express the count of interval for which the mobile nodes are out of communication with each other. The interval is defined as the average time taken for a communication flow by the node. Equation (A-1) presents the mapping of evidence to opinion, where node A derives its direct or observed opinion (ω_y) for node B, where ‘y ∈ {direct, observed}’.

\[ A_b^{\omega_y} = \left[ p / (p + n + k) \right] \]
\[ A_d^{\omega_y} = \left[ n / (p + n + k) \right] \]
\[ A_u^{\omega_y} = \left[ k / (p + n + k) \right] \]

\[ A^{\omega_y} = \left( A_b^{\omega_y}, A_d^{\omega_y}, A_u^{\omega_y} \right) \] (A1)

A.2. Consensus Operator

In our trust model, ‘⊗’ is used to combine different types of opinion (direct, observed, and recommended) into a single opinion known as global opinion.

Let us assume that node A’s direct opinion for node B is based on B’s response to its requests and is denoted as \( \lambda_{0b}^{dir} = (\lambda_{0b}^{dir}, \lambda_{0b}^{obs}, \lambda_{0b}^{dir obs}) \). Similarly, its observed opinion for node B is based on B’s response to the requests received from A’s neighbours and is denoted as \( \lambda_{0b}^{obs} = (\lambda_{0b}^{obs}, \lambda_{0b}^{dir obs}, \lambda_{0b}^{obs dir obs}) \). The combined opinion, \( \lambda_{0b}^{dir obs} = (\lambda_{0b}^{dir obs}, \lambda_{0b}^{dir obs}, \lambda_{0b}^{dir obs}) \), is then referred as the consensus between \( \lambda_{0b}^{dir obs} \) and \( \lambda_{0b}^{dir obs} \). Thus we get \( \lambda_{0b}^{dir obs} = \lambda_{0b}^{dir obs} \oplus \lambda_{0b}^{obs} \). Note that ‘⊗’ decreases uncertainty and thereof increasing the confidence.

Case I: \( A_{u_b}^{\omega} + A_{u_b}^{\omega} - A_{u_b}^{\omega} - A_{u_b}^{\omega} \neq 0 \)
A.4. Fading Operator

Recall that the evidence-to-opinion mapping operator defined for direct and observed opinions not only maps benign and malicious behaviours, but also accounts for the uncertainty introduced when nodes are out of communication with each other. In other words, the operator also responds to the duration for which there has been no evidence for either benign or malicious behaviour. Although '⊗' derives recommended opinion, it lacks provision to respond to the duration for which there have been no recommendations. Hence, we have proposed a new operator known as fading operator (⊗) to account for the duration for which recommendations are unavailable.

Let us consider the overall recommended opinion held for C by A to be \( A_{\text{all-rec}}^{\text{rev}} = (b_{c}^{\text{all-rec}}, b_{c}^{\text{rev-all-rec}}, u_{c}^{\text{all-rec}}) \). Let ‘\( \mu \)’ represent the count of interval for which recommendations are unavailable to update the overall recommended opinion, where an interval is equal to the average duration taken for a communication flow. Equations (A-7) and (A-8) present the effect of applying ‘⊗’ to \( A_{\text{all-rec}}^{\text{rev}} \) to arrive at the revised overall recommended opinion, \( A_{\text{rev-all-rec}}^{\text{all-rec}} = (b_{c}^{\text{rev-all-rec}}, b_{c}^{\text{rev-all-rec}}, u_{c}^{\text{rev-all-rec}}) \). Later, the revised overall recommended opinion \( A_{\text{rev-all-rec}}^{\text{all-rec}} \) emerges as the overall recommended opinion \( A_{\text{all-rec}}^{\text{rev}} \) for future computations and referred as \( A_{\text{all-rec}}^{\text{rev}} \) for simplicity.

\[
A_{\text{all-rec}}^{\text{rev}} = A_{\text{all-rec}}^{\text{rev}} \circ (A_{\text{all-rec}}^{\text{rev}} \circ A_{\text{all-rec}}^{\text{rev}})
\]

(A7)

A.5. Comparison Operator

One of the main objectives of a trust model is to make decisions for the system. In other models [4, 9–11, 13, 15], this is achieved by evaluating the opinions held for concerned nodes against a predefined threshold. We follow this conventional approach and for that reason, we propose a comparison operator (\( \geq \)) so that a global opinion (trust relationship) can be classified as trustworthy, uncertain, or untrustworthy.

Let us assume that node A’s global opinion for node B is denoted by, \( A_{\text{glo}}^{\text{b}} = (b_{a}^{\text{b}}, d_{a}^{\text{b}}, u_{a}^{\text{b}}) \), and node B’s global opinion on node C’s behaviour be denoted as \( b_{b}^{\text{glo}} = (b_{b}^{\text{glo}}, b_{b}^{\text{glo}}, u_{b}^{\text{glo}}) \). Here, A derives its recommended opinion for C by following its global opinion for B and B’s global opinion for C. Equation (A-5) presents the derivation of A’s recommended opinion for C based on B’s recommendation, which is denoted by, \( A_{\text{rec}}^{\text{glo}} = (b_{c}^{\text{glo}}, b_{c}^{\text{glo}}, u_{c}^{\text{glo}}) \). Thus we get \( A_{\text{rec}}^{\text{glo}} \) for simplicity.

The above presents the scenario where A takes B’s recommendation for its recommended opinion \( A_{\text{rec}}^{\text{glo}} \) towards C. However, in reality A may be considering recommendations from many other nodes for its recommended opinion towards C. Let us assume A’s overall recommended opinion for C to be \( A_{\text{all-rec}}^{\text{glo}} \), which represents the summary of past recommendations received for C. Then A’s latest overall recommended opinion \( A_{\text{all-rec}}^{\text{new-all-rec}} \) for C including B’s recommendation is given by applying '⊗' as shown in (A-6). The latest overall recommended opinion \( A_{\text{all-rec}}^{\text{new-all-rec}} \) then becomes the overall recommended opinion \( A_{\text{all-rec}}^{\text{all-rec}} \) for future reference and referred as \( A_{\text{all-rec}}^{\text{all-rec}} \) for simplicity. Recall that the process of deriving recommended opinion has been described in Section 4.6.

\[
A_{\text{glo}}^{\text{new-all-rec}} = A_{\text{glo}}^{\text{glo}} \circ A_{\text{glo}}^{\text{glo}} \circ A_{\text{glo}}^{\text{glo}}
\]

(A6)