This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2005 proceedings.

Trust Modeling and Evaluation in Ad Hoc Networks

Yan Sun*, Wei Yu†, Zhu Han†, and K. J. Ray Liu†

† Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20740
Emails: weiyu, hanzhu, kjrliu@glue.umd.edu

* Department of Electrical and Computer Engineering
University of Rhode Island, Kingston, RI 02881
Email: yansun@ele.uri.edu

***Abstract*— The performance of ad hoc networks depends on the cooperative and trust nature of the distributed nodes. To enhance security in ad hoc networks, it is important to evaluate the trustworthiness of other nodes without central authorities. In this paper, we present an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks. In the proposed information theoretic framework, trust is a measure of uncertainty with its value represented by entropy. We develop Axioms that address the basic rules for trust propagation. Based on these Axioms, we present two trust models: entropy-based model and probability-based model, which satisfy all the Axioms. The proposed trust evaluation method and trust models are employed in ad hoc networks for secure ad hoc routing and malicious node detection. Simulations show that the proposed framework can significantly improve network throughput as well as effectively detect malicious behaviors in ad hoc networks.** [1]

I. Introduction

An ad hoc network is a group of mobile nodes without requiring a central administration or a fixed network infrastructure. Due to their distributed nature, ad hoc networks are vulnerable to various attacks [1]–[3]. One strategy to improve security of ad hoc networks is to develop mechanisms that allow a node to evaluate trustworthiness of other nodes. Such mechanisms not only help in malicious node detection, but also improve network performance because honest nodes can avoid working with untrustworthy nodes. The focus of this paper is to develop a framework that defines trust metrics and develop models of trust propagation in ad hoc networks. The proposed theoretical models are then applied to improve the performance of ad hoc network routing schemes and to assist malicious node detection.

The problem of defining trust metrics and trust relationship has been extensively studies for public key authentication [4]–[8], electronics commerce [9], as well as in P2P networks [10]. In these schemes, trust is evaluated in very different ways. Some schemes employ linguistic description of trust relationship, such as in [5], [11]–[13]. Based on the linguistic descriptions of trust, decisions can be made based on linguistic trust policies or fuzzy logic [9]. In some other schemes, discrete or continuous numerical values are assigned to measure the level of trust [6], [7], [14]. For example, in [6], an entity's opinion about the trustworthiness of a certificate is described by a continuous value in $[0, 1]$. In [7], a triplet in $[0, 1]^3$ is assigned to measure trustworthiness, and the elements in the triplet represent belief, disbelief, and uncertainty, respectively. In [14], discrete integer numbers are used.

Before we can compare different trust evaluation methods or discuss trust models for ad hoc networks, a fundamental question needs to be answered first. What is the physical meaning of trust? The answer to this question is the critical link between observations (trust evidence) and the metrics that evaluate trustworthiness. In ad hoc networks, trust relationship can be established in two ways. The first way is through direct observations of other nodes' behavior, such as dropping packets etc. The second way is through recommendations from other nodes. Without clarifying the meaning of trust, trustworthiness cannot be accurately determined from observations, and the calculation/policies/rules that govern trust propagation cannot be justified.

Previous work on trust management in ad hoc networks focuses on trustworthiness evaluation process after initial trust relationship has been established. They do not, however, address how to obtain initial trust relationship partially because the meaning of the trust metrics is not clearly defined. In this paper, we propose an information theoretic framework of trust modeling and evaluation. In this framework, trust is a measure of uncertainty, as such trust values can be measured by entropy. From this understanding of trust, we developed axioms that address the basic rules for establishing trust through a third party (concatenation propagation) and through recommendations from multiple sources (multipath propagation). Based on these axioms, we develop techniques that calculate trust values from observations and design two models that address the concatenation and multipath trust propagation problems in ad hoc networks. The proposed models are applied to improve network performance and security of ad hoc routing protocols. Simulations are performed to demonstrate the effectiveness of the proposed models.

The rest of the paper is organized as follows. The understanding of trust and basic axioms are presented in Section II, and trust models are presented in Section III. Section IV addresses how to establish trust relationship based on observations. In Section V, the proposed models are applied in ad hoc networks to assist route selection in on-demand routing protocols and malicious node detection. Simulation results are shown in Section VI, followed by the conclusion in Section VII.

[1]This work was supported in part by the Army Research Office under Award No. DAAD19-01-1-0494 and by NSF ADVANCE program at the University of Rhode Island.

II. Basic Axioms

In this section, we will explain the meaning of trust and present axioms for establishing trust relationship. In this work, we relay trust as a level of uncertainty and the basic understanding of trust is summarized as follows.

1) Trust is a relationship established between two entities for a specific action. In particular, one entity trusts the other entity to perform an *action*. In this work, the first entity is called the *subject*, the second entity is called the *agent*. We introduce the notation $\{subject : agent, action\}$ to describe a trust relationship.
2) Trust can be measured by uncertainty. Here are three special cases. (1) When the subject believes that the agent will perform the action for sure, the subject fully trusts the agent and there is no uncertainty. (2) When the subject believes that the agent will not perform the action for sure, the subject fully distrusts the agent and there is no uncertainty either. (3) When the subject has no idea about the agent at all, there is the maximum amount of uncertainty and the subject has no trust in the agent. Indeed, trust is built upon how certain one is about another on whether some actions will be carried out or not. Therefore trust metrics should describe the level of uncertainty in trust relationship.
3) Trust is not necessarily symmetric. The fact that A trusts B does not necessarily means that B also trusts A, where A and B are two entities.

Trust Metrics

How to measure uncertainty in trust relationship? Information theory states that entropy is a nature measure of uncertainty [15]. We would like to define a trust metric based on entropy, while it gives trust value 1 in the first special case, -1 in the second special case, and 0 in the third special case.

Let $T\{subject : agent, action\}$ denote the trust value of the trust relationship $\{subject : agent, action\}$, and $P\{subject : agent, action\}$ denote the probability that the agent will perform the action in the subject's point of view. We define the entropy-based trust value as:

$$T\{subject : agent, action\} = \begin{cases} 1 - H(p), & \text{for } 0.5 \le p \le 1; \\ H(p) - 1, & \text{for } 0 \le p < 0.5, \end{cases} \quad (1)$$

where $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the entropy function and $p = P\{subject : agent, action\}$.

This definition considers both trust and distrust. In general, trust value is positive when the agent is more likely to perform the action ($p > 0.5$), and is negative when the agent is more likely not to perform the action ($p < 0.5$). This definition also tells that trust value is not a linear function of the probability. It is also noted that (1) is a one-to-one mapping between $T\{subject : agent, action\}$ and $P\{subject : agent, action\}$.

Necessary Conditions of Trust Propagation

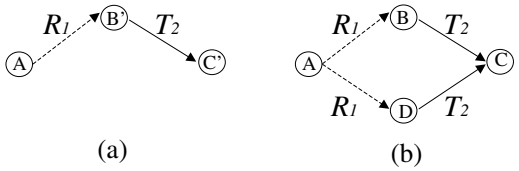

Fig. 1. Combing Trust Recommendations

Assume that A and B have established $\{A : B, action_r\}$, and B and C have established $\{B : C, action\}$. Then, $\{A : C, action\}$ can be established if

1 $action_r$ is to make recommendation of other nodes about performing $action$.
2 The trust value of $\{A : B, action_r\}$ is positive.

The first condition is necessary because the entities that perform the action do not necessarily make correct recommendations. The second condition is necessary because untrustworthy entities' recommendation can be totally uncorrelated with the truth. The enemy's enemy is not necessarily a friend. Thus, the best strategy is not to take recommendations from untrustworthy parties.

When the above two conditions are satisfied, we recognize three axioms for establishing trust relationship through recommendations without direct interaction between the agent and the subject. These axioms are originated from the understanding of uncertainty.

Axiom 1: Concatenation propagation of trust does not increase trust

It is well known that uncertainty does not decrease after processing. Thus, when the subject establishes a trust relationship with the agent through the recommendation from a third party, the trust value between the subject and the agent should not be more than the trust value between the subject and the recommender as well as the trust value between the recommender and the agent.

The mathematical representation of Axiom 1 is

$$|T_{AC}| \le \min(|R_{AB}|, |T_{BC}|), \quad (2)$$

where $T_{AC} = T\{A : C, action\}$, $R_{AB} = T\{A : B, action_r\}$ and $T_{BC} = T\{B : C, action\}$.

Axiom 2: Multipath propagation of trust does not reduce trust

If the subject obtains an extra recommendation, which agrees with the subject's current opinion, the subject will be more certain about the agent, or at least maintain the same level of certainty. Thus, if the subject receives the same recommendations for the agent from multiple sources, the trust value should be no less than that in the case where the subject receives less number of recommendations.

In particular, as illustrated in Figure 1, A establishes trust with C' through one concatenation path, and A establishes trust with C through two same paths. Let $T_{AC} = T\{A : C, action\}$ and $T_{AC'} = T\{A : C', action\}$. The mathematical representation of Axiom 2 is

$$T_{AC} \ge T_{AC'} \ge 0, \text{ for } R_1 > 0 \text{ and } T_2 \ge 0;$$
$$T_{AC} \le T_{AC'} \le 0, \text{ for } R_1 > 0 \text{ and } T_2 < 0,$$

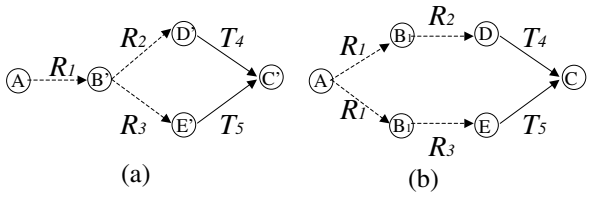

Fig. 2. One Entity Provides Multiple Recommendations

where $R_1 = T\{A : B, \text{making recommendation}\}$ and $T_2 = T\{B : C, action\}$. Notice that Axiom 2 holds only if multiple sources generate the same recommendations. This is because the collective combination of different recommendations is a problem in nature that can generate different trust values according to different trust models.

Axiom 3: Trust based on multiple recommendations from a single source should not be higher than that from independent sources

When the trust relationship is established jointly through concatenation and multipath trust propagation, it is possible to have multiple recommendations from a single source, as shown in Figure 2 (a). Since the recommendations from a single source are highly correlated, the trust built upon those correlated recommendations should not be higher than the trust built upon recommendations from independent sources. In particular, let $T_{AC'} = T\{A : C', action\}$ denote the trust value established in Figure 2 (a), and $T_{AC} = T\{A : C, action\}$ denote the trust value established in Figure 2 (b). The Axiom 3 says that

$$T_{AC} \geq T_{AC'} \geq 0, \text{ if } T_{AC'} \geq 0;$$
$$T_{AC} \leq T_{AC'} \leq 0, \text{ if } T_{AC'} < 0,$$

where R_1, R_2, and R_3 are all positive.

III. Trust Models

The methods for calculating trust via concatenation and multipath propagation are referred to as *trust models*. In this section, we introduce the entropy-based and the probability-based trust models.

A. Entropy-based Trust Model

In this model, the trust propagations are calculated directly from trust values defined in (1). For concatenation trust propagation, node B observes the behavior of node C and makes recommendation to node A as $T_{BC} = \{B : C, action\}$. Node A trusts node B with $T\{A : B, \text{making recommendation}\} = R_{AB}$. To satisfy Axiom 2, one way to calculate $T_{ABC} = T\{A : C, action\}$ is

$$T_{ABC} = R_{AB} T_{BC}. \quad (3)$$

Note that if node B has no idea about node C (i.e. $T_{BC} = 0$) or if node A has no idea about node B (i.e. $R_{AB} = 0$), the trust between A and C is zero, i.e., $T_{ABC} = 0$.

For multipath trust propagation, let $R_{AB} = T\{A : B, \text{making recommendation}\}$, $T_{BC} = T\{B : C, action\}$, $R_{AD} = T\{A : D, \text{making recommendation}\}$, $T_{DC} = T\{D : C, action\}$. Thus, A can establish trust to C through two paths: $A - B - C$ and $A - D - C$. To combine the different paths, we propose to use maximal ratio combining as:

$$T\{A : C, action\} = w_1(R_{AB} T_{BC}) + w_2(R_{AD} T_{DC}), \quad (4)$$

$$w_1 = \frac{R_{AB}}{R_{AB} + R_{AD}}, \text{ and } w_2 = \frac{R_{AD}}{R_{AB} + R_{AD}}. \quad (5)$$

In this model, if any path has trust value 0, this path will not affect the final result. We can prove that this model satisfies all axioms.

B. Probability-based Model

In the second model, we calculate concatenation and multipath trust propagation using the probability values of the trust relationship. The probability values can be easily transferred back to trust values using (1).

For the concatenation trust propagation, let p_{AB} denote $P\{A : B, \text{make recommendation}\}$, p_{BC} denote $P\{B : C, action\}$ and p_{ABC} denote $P\{A : C, action\}$. We also define p'_B as the probability that B will make correct recommendations, $p'_{C|B=1}$ as the probability that C will perform the action if B makes correct recommendation, and $p'_{C|B=0}$ as the probability that C will perform the action if B does not make correct recommendation. Then, A can calculate p_{ABC} as:

$$p_{ABC} = p'_B \cdot p'_{C|B=1} + (1 - p'_B) \cdot p'_{C|B=0}. \quad (6)$$

Although A does not know p'_B, $p'_{C|B=1}$ and $p'_{C|B=0}$, it is reasonable for A to estimate that $p'_B = p_{AB}$ and $p'_{C|B=1} = p_{BC}$. Therefore, (6) becomes

$$p_{ABC} = p_{AB} \cdot p_{BC} + (1 - p_{AB}) \cdot p'_{C|B=0}. \quad (7)$$

From Axiom 2, it is easy to see that T_{ABC} should be 0 when T_{AB} is 0. That is, p_{ABC} should be 0.5 when p_{AB} is 0.5. By using $p_{AB} = 0.5$ and $p_{ABC} = 0.5$ in (7), we can show that $p'_{C|B=0} = (1 - p_{BC})$. Therefore, we calculate p_{ABC} as

$$p_{ABC} = p_{AB} p_{BC} + (1 - p_{AB})(1 - p_{BC}). \quad (8)$$

For the multipath case, as shown in Figure 1, we obtain the probability value p_{ABC} through path $A - B - C$ and p_{ADC} through path $A - D - C$ using the concatenation model. The question is how to obtain the overall trust $p_{AC} = P\{A : C, action\}$. This problem has similarity as the data fusion problem where observations from different sensors are combined. Thus, we use the data fusion model [16] with the assumption that the recommendations are independent. So the probability p_{AC} can be calculated as follows:

$$\frac{p_{AC}}{1 - p_{AC}} = \frac{p_{ABC} p_{ADC}}{(1 - p_{ABC})(1 - p_{ADC})}. \quad (9)$$

In this model, if one path has probability value of 0.5 (i.e. trust value 0), this path does not affect the final result. We can prove that this model satisfies all axioms.

IV. Trust Evaluation Based on Observations

The problem we address in this section is to obtain the trust value from observations. Assume that A wants to establish trust relationship with X as $\{A : X, act\}$ based on A's previous observation about X. One typical type of observation is as follows. Node A observes that X has performed the action k times upon the request of performing the action N times. For example, A asked X to forward N packets, and X in fact forwarded k packets. For this type of observation, we define binary random variable $V(i)$, and $V(i) = 1$ means that X performs the action at the i^{th} trial. We also define random variable $n(N) = \sum_{i=1}^{N} V(i)$, which is the number of actions performed by X out of total N trials.

We assume that X's behaviors in the past N trials and in the future $(N+1)^{th}$ trial are independent but governed by the same Bernoulli distribution. Then, using Bayesian approach, we can prove that

$$Pr(V(N+1) = 1 | n(N) = k) = \frac{k+1}{N+2}. \qquad (10)$$

Here, $Pr(V(N+1) = 1 | n(N) = k)$ is a good estimate of the probability value of trust relationship $\{A : X, act\}$.

In practice, node A often makes observations at different times. Let t_j denote the time when A make observations of node X, where $j = 1, 2, \cdots, I$. At time t_j, node A observes that node X performs the action k_j times upon the request of performing the action N_i times. We propose to calculate the trust value as follows:

$$P\{A : X, action\} = \frac{1 + \sum_{j=1}^{I} \beta^{t_c - t_j} k_j}{2 + \sum_{j=1}^{I} \beta^{t_c - t_j} N_j}, \qquad (11)$$

where t_c represents the current time when this calculation is performed, and $0 \leq \beta \leq 1$ is referred to as the forgetting factor.

V. Trust Evaluation in Ad Hoc Networks

Securing routing protocols is a fundamental challenge for ad hoc network security [2], [3]. Currently, most schemes that aim to secure ad hoc routing protocols focus on preventing attackers from entering the network through secure key distribution/authentication and secure neighbor discovery. Those schemes, however, are not effective in situations where malicious nodes have gained access to the network, or some nodes in the network have been compromised. Therefore, it is important to develop mechanisms to monitor route disruption in ad hoc networks and adjust the route selection dynamically. In this section, we use the proposed trust models to improve ad hoc routing protocols and discuss their potential usage for malicious node detection.

In particular, for ad hoc routing, we investigate trust values associated with two actions: forwarding packets and making recommendations. Briefly speaking, each node maintains its trust record about other nodes associated with these two actions. When a node (source) wants to establish a route to the other node (destination), the source first finds multiple routes to the destination. Then the source tries to find the packet-forwarding trustworthiness of the nodes on the routes from its own trust record or through requesting recommendations. Finally the source selects the trustworthy route to transmit data. After the transmission, the source node updates the trust records based on its observation of route quality. The trust records can also be used for malicious node detection. All above are achieved in a distributed manner.

A. Obtaining Trust Recommendations

Requiring trust recommendation in ad hoc networks often occurs in the circumstance where communication channels between arbitrary entities are not available. We have designed a fully distributed trust recommendation mechanism for ad hoc networks.

Briefly speaking, node A generates a trust recommendation request (TRR) message, when node A wants to establish trust relationships with a set of nodes $\mathbf{B} = \{B_1, B_2, \cdots\}$ about action act but does not have valid trust record with $\{B_i, \forall i\}$. The TRR message has the format as

$\{\text{requestID}, A, \mathbf{B}, \text{act}, \mathbf{Z}, \text{Max\_transit}, \text{TTL}, \text{transmit-path}\}$.

Here, $\mathbf{Z}$ represents the IDs of the node from which A asks for recommendations, Max_transit is the maximum length of the trust transit chain, transmit-path records the delivery history of this TRR message. Node A sends the TRR to its neighbors and waits time TTL for replies. Upon receiving an unexpired TRR message, the nodes that are not in $\mathbf{Z}$ simply forward the TRR message to their neighbors; the nodes in $\mathbf{Z}$ either send trust values back to A or ask their trusted recommenders for further recommendations.

The major overhead of requesting trust recommendations comes from transmitting TRR messages in the network, which increases exponentially with Max_transit. Fortunately, Max_transit should be a small number due to Axiom 1, which implies that only short trust transit chains are useful.

B. Trust Record Update

Trust record is updated before and after data transmission. Assume that node A would like to ask node C to transmit packets, while A does not have existing trust relationship with node C.

- Before data transmission, node A calculates the trust value $T^r_{AC} = T\{A : C, \text{forward packet}\}$ based on recommendation from node B.
- After data transmission, node A observes that C forwards k packets out of total N packets. This observation is made through a light-weight self-evaluation mechanism, which allows the source node to collect packet forwarding statistics and to validate the statistics through consistence check. More details of this mechanism is presented in [17]. Then, A calculates $T^a_{AC} = T\{A : C, \text{forward packet}\}$ based on observations. If $|T^a_{AC} - T^r_{AC}| \leq$ threshold, node A believes that B has made one good recommendation. Otherwise, node A believes that B has made one bad recommendation. Then, A can update the recommendation trust of B accordingly.

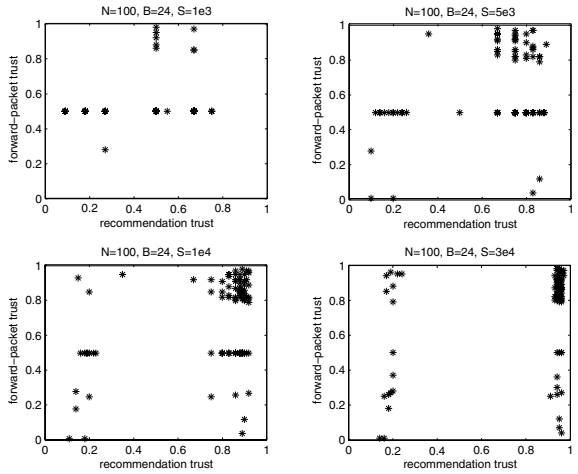

Fig. 3. Trust Record of a Good Node

C. Route Selection and Malicious Node Detection

Among all possible routes, node A chooses the most trustworthy route. The trustworthiness of a route is calculated as the product of the probability value of forward-packet trust of all nodes on the route.

In addition, node A performs malicious node detection based on the trust value of two actions: forwarding packet and making recommendations. The detailed method will be shown in the simulation section.

VI. Simulations

A. Malicious Node Detection

We first investigate the establishment of trust record in a simple system that reveals important insights of trust propagation and the effects of various attack models. The system is setup as follows. In each time interval, which is n time units long, each node selects another node to transmit packets. Assume that node A selects node X. If the trust value $\{A : X, \text{forward packet}\}$ is smaller than a threshold, node A will ask for recommendations about node X. Then, node A asks X to forward n packets and the data rate is 1 packet per time unit. In this system, if a malicious node decides to attack node A, it drops the packets from node A with packet drop ratio randomly selected between 0 and 40%, and/or sends recommendations to node A with trust values randomly picked from -1 to 1. Three types of malicious nodes are considered. Type 1 drops packets only, type 2 makes wrong recommendations only, and type 3 does both. Other simulation parameters are Max_transit $=$ 1, and the forgetting factor is $\beta = 0.999$.

In the first experiment, we have $N = 100$ total number of nodes. Among them, 24 nodes are malicious. 8 nodes for type 1, type 2, and type 3, respectively. In Figure 3, we show the trust record of one good node at different times. Here S is the simulation time. We plot the probability value of packet-forwarding trust vs. probability value of recommendation trust of all other nodes in this good node's trust record. When the number of observations is small, most of the nodes are with probability of 0.5 in either packet-forwarding trust or recommendation trust.

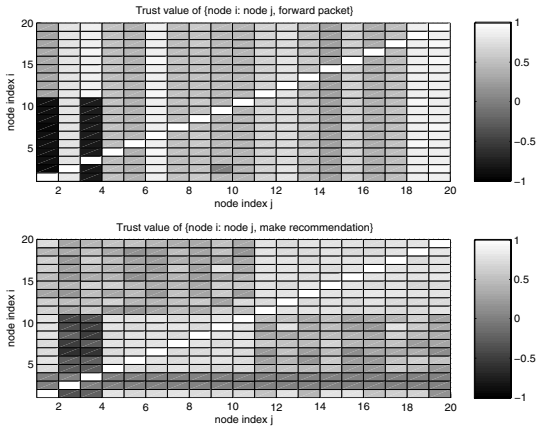

Fig. 4. Trust Records of 20 Nodes with 3 Malicious Nodes

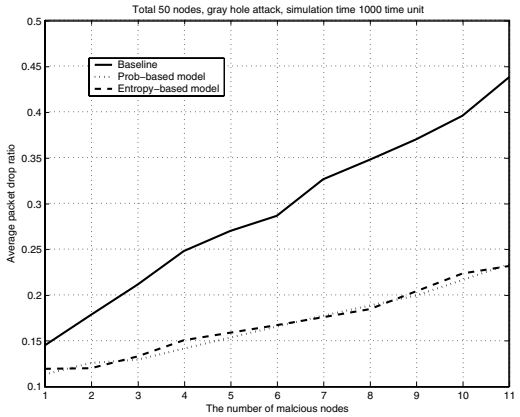

Fig. 5. Average Packet Drop Ratio with Different Number of Malicious Nodes

This is because this node has no experience with many others. With more observations, good nodes form a cluster that is close to the up-right corner and this cluster becomes tighter and tighter. In addition, three types of malicious behaviors are clearly shown and can be differentiated.

In the second experiment, we have a total of 20 nodes. Among them, 3 nodes are malicious. Specifically, node 1 drops packets only, node 2 provides bad recommendations only, and node 3 does both. In Figure 4, the element on the i^{th} row and j^{th} column represents the trust of the i^{th} user to the j^{th} user. The brighter is the color, the higher is the trust. Here, the bad nodes are only malicious to half of the users. It is seen that good nodes that are under attack develop negative packet-forwarding trust values for malicious nodes. However, when bad nodes only attack half of nodes, they can hurt good nodes' recommendation trusts. The node 1-10 think node 11-20 do not give good recommendations and vise versa. We can make two points here. First, the recommendation trusts of malicious nodes are still significantly lower than that of good nodes. We can still perform malicious node detection. Second, node 1-10 will not give higher weights to the recommendations from node 11-20, which has positive effects on improving network throughput.

B. Network Throughput Improvement

We use an event-driven simulator to simulate mobile ad hoc networks. The physical layer assumes a fixed transmission range model, where two nodes can directly communicate only if they are in each other's transmission range. The MAC layer protocol simulates the IEEE 802.11 Distributed Coordination Function (DCF). DSR [18] is used as the underlying routing protocol. The mobility model is random waypoint model [18] with slight modifications. We use a rectangular space of size 1000m by 1000m. The total number of nodes is 50, and the maximum transmission range is 250m. There are 50 traffic pairs randomly generated for each simulation. For each traffic pair, the packet arrival time is modelled as a Poisson process, and the average packet inter-arrival time is 1 second. The size of each data packet after encryption is 512 bytes. Among all the ROUTE REQUESTs with the same ID received by a node A, A will only broadcast the first request if it is not the destination, and will send back at most 5 ROUTE REPLYs if it is the destination. The maximum number of hops on a route is restricted to be 10.

We change the total number of malicious nodes from 1 to 11. In this implementation, the malicious nodes perform gray hole attack, i.e., randomly drop 65-75% packets passing through them. Three systems are compared: (1) baseline scheme that does not build or utilize trust record; (2) the system using entropy-based model for trust recommendations; and (3) the system using probability-based model for trust recommendations. Figure 5 shows the average packet drop ratios of good nodes. The simulation time is 1000sec. We can see that malicious nodes can significantly degrade the performance of the baseline system. Even with 4 attackers (8% of total nodes), the packet drop ratio can be as high as 25%. Obviously, using the proposed mechanism to build and utilize trust records can greatly improve the performance. In particular, it takes more than 11 attackers (24% of total nodes) to cause 25% average packet drop ratio. In addition, the performances of probability-based and entropy-based models are similar. It is important to point out that the results shown in Figure 5 is for a very short simulation time, where the trust records are built upon very limited observations. Within such as short simulation time, the good nodes and bad nodes are not well separated on the 2D trust plots, and malicious node detection mechanism is not activated yet. Even under this condition, the proposed scheme still shows performance gain in Figure 5, which is due to the route selection using trust values.

VII. Conclusion

In this paper, we present an information theoretic framework for trust evaluation in distributed networks. The proposed trust metric has clear physical meaning and the axioms are developed to govern trust establishment through third parties. Based on these axioms, the level of trustworthiness can be quantitatively determined based on observations and through propagation. Two models that govern concatenation and multipath trust propagation are developed. The proposed framework is suitable for a variety of applications in distributed networks. In this work, we demonstrate the usage of the proposed models in ad hoc network in malicious node detection and route selection. The simulation results show that the malicious nodes can be detected and the types of their malicious behaviors can be identified. In addition, with the trust recommendations and trust records, the chances of malicious node being on the routes are greatly reduced. As a result, the improvement in network throughput is observed. This work provides the theoretical bases of trust evaluation and addresses practical implementations when applying the theories in ad hoc networks.

References

[1] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.

[2] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of MobiCom 2000*, August 2000, p. 255265.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proceedings of MobiCom 2002*, Sep 2002.

[4] M. K. Reiter and S. G. Stubblebine, "Resilient authentication using path independence," *IEEE Transactions on Computers*, vol. 47, no. 12, pp. 1351–1362, December 1998.

[5] W. Stallings, *Protect Your Privacy, A Guide for PGP Users*, Prentice Hall, 1995.

[6] U. Maurer, "Modelling a public-key infrastructure," in *Proceedings 1996 European Symposium on Research in Computer Security(ESORICS' 96), volume 1146 of Lecture Notes in Computer Science*, 1996, pp. 325–350.

[7] A. Jsang, "An algebra for assessing trust in certification chains," in *Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium*, 1999.

[8] R. Levien and A. Aiken, "Attack-resistant trust metrics for public key certification," in *Proceedings of the 7th USENIX Security Symposium*, January 1998, pp. 229–242.

[9] D.W. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in *Proceedings of the 18th IEEE International Conference on Distributed Computing Systems*, May 1998, pp. 312 – 321.

[10] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of 12th International World Wide Web Conferences*, May 2003.

[11] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, May 1996, pp. 164–173.

[12] A. Herzberg, Y. Mass, J. Michaeli, D. Naor, and Y. Ravid, "Access control meets public key infrastructure or: Assigning roles to strangers," in *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, May 2000, pp. 2–14.

[13] D. Clarke, J.-E. Elien, C. Ellison, M. Fredette, A. Morcos, and R. L. Rivest, "Certificate chain discovery in spki/sdsi," *Journal of Computer Security*, vol. 9, no. 4, pp. 285–322, 2001.

[14] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in *Proceedings of 1997 New Security Paradigms Workshop, ACM Press*, 1998, pp. 48–60.

[15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience, 1991.

[16] D.L. Hall and S.A.H. Mcmullen, *Mathematical Techniques in Multisensor Data Fusion*, Artech Hous INC, 2004.

[17] Wei Yu, Yan Sun, and K.J. Ray Liu, "HADOF: Defense against routing disruptions in mobile ad hoc networks," in *Proceedings of IEEE INFOCOM'05*, March 2005.

[18] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks, mobile computing," *In Moible Computing, edited by Tomasz Imielinski and Hank Korth, Kluwer Academic Publishers*, pp. 153–181, 1996.