Using Node Accountability in Credential Based Routing for Mobile Ad-Hoc Networks

Erman Ayday and Faramarz Fekri
School of Electrical and Computer Eng. Georgia Institute of Technology Atlanta, GA 30332-0250, USA
Email: {erman, fekri}@ece.gatech.edu

***Abstract*—We propose a secure and efficient routing scheme using a game theoretical approach and trust relationships between the nodes. We assume a "Bayesian Game" model [1] among the nodes to find the optimal behavior of legitimate and malicious nodes. Moreover, using a "watchdog" mechanism and an "acknowledgement" mechanism (ACK), we construct trust relationships between the nodes.**

I. Related Work

Building trust values by relying on the direct or indirect measurements and using the watchdog mechanism is proposed in [2]–[4]. However, relying on the watchdog mechanism to obtain the direct measurements has many shortcomings. The monitoring node hearing the transmission of its next hop does not mean that the following node in the path actually receives the packet. Besides, when there are consecutive malicious nodes in the path, it becomes very easy to cheat a monitoring node and gain credit for a malicious node. Recently, researches started to use game theory to analyze wireless networks. Especially Bayesian game theoretical model [1] is commonly used to analyze wireless networks with selfish/attacker nodes.

II. Description of the Scheme

In our model, the source node encodes its packets before sending them to the destination using rateless codes [5]. The rational for this is to avoid retransmissions, decrease total latency and increase availability at the destination. We divide the time into time slots of length $slot_T$. At the beginning of each time slot, each node selects its max_n neighbors to use as its potential receivers during that time slot. This neighbor selection is based on the credentials of the neighbor nodes and their distances to the destination node. A sender node i calculates the metric for one of its 1-hop neighbors j as $M_j^i = \frac{min[dist]}{dist(j)} \times \frac{cred(j)}{max[cred]}$. Legitimate nodes use the ACK from the destination to built the trust values (credentials) and determine their optimal behaviors. ACKs are sent by the destination node with a specific period which is ACK_T. We note that ACK is sent for the block of packets that the destination has received between two ACK periods. When the ACK is received from the destination, a legitimate node first determines the packet with the maximum ID (max_{ID}) that is received by the destination. The credential for the neighbor node i is calculated based on the Beta distribution $cred(i) = \frac{\alpha}{\alpha+\beta}$ as in [6]. Here, β stands for the number of packets sent to node i by the sender that has IDs smaller than or equal to max_{ID} and α stands for the number of packets that are included in the ACK message among those β packets.

During the packet forwarding, each node chooses its next move to maximize its benefit in the game. A legitimate node just forwards the packets and chooses to use its watchdog mechanism or to stay passive depending on the trust value (credential) of its receiver.

A malicious node, on the other hand, decides to attack or not based on the watchdog mechanism of its previous hop. For simplicity of discussion, we illustrate the dynamic Bayesian game between the sender s and the receivers a and b (when $max_n = 2$). We introduce the notations we use in the following.

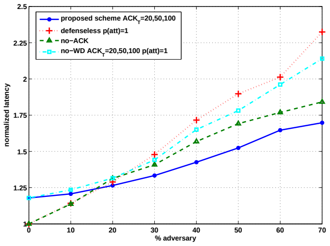


Fig. 1. Comparison of latency versus fraction of malicious nodes for four different schemes.

W_s^i	The event, node s uses watchdog for node i
$\overline{W}_s^i$	The event, node s does not use watchdog for node i
A_i	The event, malicious node a misbehaves
$\overline{A}_i$	The event, malicious node a does not misbehave
C_{WD}	Cost of using watchdog mechanism per packet
C_a	Cost of attacking per packet
G_{ch}	Gain of a malicious node when it succeeds to cheat a legitimate node
G_{ca}	Gain for a legitimate node when it succeeds to detect a misbehavior

Based on the previous observations of the sender s (ACKs received from the destination), the probabilities of node a and node b being malicious are ${P_s}^a$ and ${P_s}^b$, respectively. We also note that a node being malicious does not imply that it will behave maliciously all the time. Hence, given a and b are malicious, we define the attacking probabilities for nodes a and b as P_{att}^a and P_{att}^b, respectively. Moreover, we define f_a (forwarding probability for node a) and f_b (forwarding

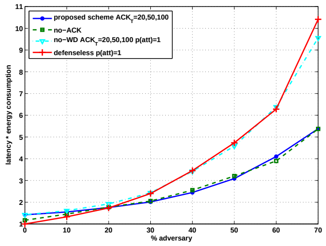


Fig. 2. $latency \times energy\ consumption$ versus fraction of malicious nodes.

1-4244-2575-4/08/$20.00 ©2008 IEEE

probability for node b) as the probabilities that s will choose node a and b to forward a packet, respectively.

Sender s initially determines the forwarding probabilities of nodes a and b based on ${P_s}^a$ and ${P_s}^b$, respectively. Furthermore, when a node is detected by the sender upon misbehaving, its forwarding probability is decreased by ϵ, and this decrease is rewarded proportionally to other nodes depending on their credentials.

max_n	2
$slot_T$	100 time units
ACK_T	$20, 50, 100$ time units
ϵ	0.1
G_{ch}	50 units
G_{ca}	50 units
C_a	1 unit
C_{WD}	10 units

TABLE I
SIMULATION PARAMETERS.

We propose to equate the payoffs of sender s for the events W_s^i and $\overline{W}_s^i$ to use a mixed strategy. Hence we obtain

$$f_a P^a_{att} {P_s}^a + f_b P^b_{att} {P_s}^b = \frac{C_{WD}}{G_{ch} + G_{ca}} \qquad (1)$$

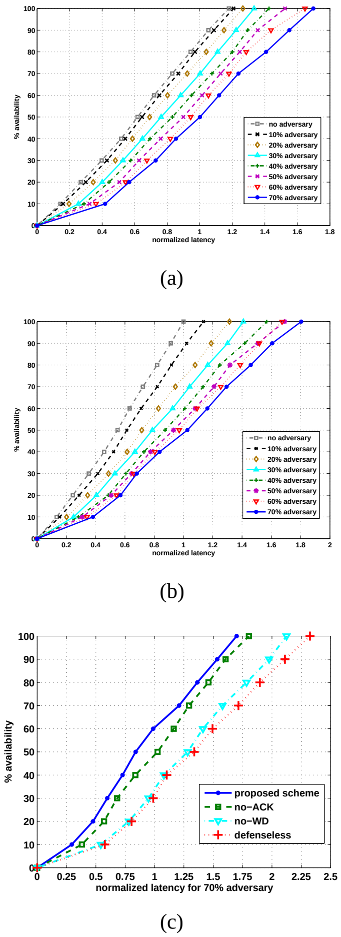
which illustrates the optimal attacking probabilities for nodes a and b (if they are malicious). This result can also be generalized to $max_n > 2$ easily. We also analyzed the communication from the receiver's side to determine the optimal watchdog probability of the sender s. We use a mixed strategy as we did before by equating the payoffs of node a for the events A_a and $\overline{A}_a$. After this calculation we come up with the watchdog probability of node s for node a as

$${P_{w_a}}^s = {P_s}^a \frac{-C_a + G_{ch}}{G_{ch} + G_{ca}} \qquad (2)$$

It is worth noting that the dynamic Bayesian game described throughout this section has a *Perfect Bayesian Equilibrium* (PBE) that is proved in [7].

III. Simulation

The main purpose of our simulations is to examine the latency, energy consumption and data availability in the presence of adversarial nodes. We consider the insider adversary who is allowed to do anything that a legitimate network node can do. Moreover, we consider that multiple malicious nodes may collaborate to achieve a common goal. As the mobility model, we assume nodes move inside a specific boundary based on the "random-way-point" (RWP) model (with a range of 0.3 units). We assume that there is no node in the network that is 100% trustworthy. Hence, we define a minimum value for ${P_s}^i$ as ${P_s}^{min}$ (0.1). Further, we define a minimum value for f_i as f_{min} (0.2). In our simulations, the network area is square shaped with an edge of 2 units.There are 100 nodes, we sweep the number of malicious nodes from 0 to 70. Furthermore, the communication range of each node is assumed to be 0.45 units. Number of encoded packets should be received by the destination for complete message recovery is 1000. Other parameters we use for the simulations are listed in Table I. Finally, we repeated each simulation 25 times to get an average. We compare our scheme with three different cases: 1) *defenseless* case, in which there is no mechanism against the malicious nodes, 2) *no-ACK* case, in which nodes just use the watchdog mechanism to observe and evaluate their next hop neighbors, and 3) *no-watchdog* case, in which nodes do not use the watchdog mechanism at all and solely use the ACK from the destination to evaluate the other nodes. In Figure I, we show the normalized latency versus different number of malicious nodes. As illustrated in Figure II, both the *proposed* and the *no-ACK* schemes have almost the same performances (However, the *no-ACK* scheme has serious drawbacks because of the dependency on the watchdog mechanism). In Figure 3(a) and Figure 3(b) the change in availability with the normalized latency is shown for the *proposed scheme* and the *no-ACK* scheme, respectively. Furthermore, in Figure 3(c), we show the change in availability of all schemes when 70% of the nodes are compromised.



(a)

(b)

(c)

Fig. 3. Availability versus latency: (a) *proposed scheme*, (b) *no-ACK* scheme, (c) comparison of all schemes when 70% of nodes are compromised.

References

[1] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: The MIT Press, 1991.

[2] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," in *Research Report cs.NI/0307012*, 2003.

[3] S. Buchegger and J. Boudec, "Performance analysis of confidant protocol (coorperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proc. IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, Jun. 2002.

[4] Y. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[5] M. Luby, "LT codes," in *Proc. IEEE Symposium on Foundations of Computer Science*. Vancouver: IEEE Comput. Soc., Nov. 2002, pp. 271–280.

[6] S. Buchegger and J. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in *Proc. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt '03)*, 2003.

[7] J. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in *Workshop on Game Thory for Networks (GameNets 2006)*, Pisa, Italy, Oct. 2006.