

FORBID: Cope with Byzantine Behaviors in Wireless Multi-Path Routing and Forwarding

Xueyuan Su^{*}, Gang Peng[†] and Sammy Chan[†]

^{*}Department of Computer Science, Yale University,
New Haven, CT 06511, U.S.A.

[†]Department of Electronic Engineering, City University of Hong Kong,
Tat Chee Avenue, Kowloon Tong, Hong Kong.

Email: xueyuan.su@yale.edu, gpeng2@student.cityu.edu.hk, eeschan@cityu.edu.hk

Abstract—Consider multi-path routing and forwarding scenarios in wireless ad hoc networks. Rational and Byzantine nodes both might deviate from the protocol. However, their intentions and behaviors are different. To extend our previous work on generalized second price (GSP) auction for stimulating rational nodes for cooperation, we propose FORBID mechanism in this work to cope with Byzantine behaviors. The core of the FORBID mechanism is a decentralized reputation system. Based on available evidence, each node relies on Bayesian inference to internally update its reputation beliefs that how reliable each other node is. Different from the passive overhearing techniques such as “watchdog”, each source node under FORBID actively triggers detection process to collect evidence towards Byzantine behaviors. In addition, FORBID includes a flocking algorithm to allow careful dissemination of reputation information and thus shortens the misbehavior detection time.

Index Terms—Wireless ad hoc networks, multi-path routing and forwarding, Bayesian inference, flocking algorithm.

I. INTRODUCTION

In a wireless ad hoc network, there is no central coordinator to manage communication among the nodes. Wireless devices rely on each other to forward packets to the destination. Initial protocol designs often assume that nodes will always follow the protocol. Such nodes are thus called *altruistic*. This kind of design worked well because such wireless devices were usually owned by a single entity and were supposed to cooperate with each other. However, due to the fast advancement of mobile communication and computing, numerous small and convenient mobile devices come into everyday life, such as smart phones, PDAs and so on. Such devices are owned by different individuals who may have various interests on deviating from the norm.

There are generally two kinds of misbehavior, *selfish* and *malicious*. In game theory literature, selfish nodes are often referred to as *rational* [16]; while in distributed computing literature, malicious nodes are often referred to as *Byzantine* [13]. A rational node behaves in such a way that its utility is maximized. For example, mobile devices usually have tight energy constraint as technological progress on batteries is much slower than on electronics [6], helping forward packets

introduces energy cost and thus selfish nodes are not likely to do the favor free of charge. On the other hand, a Byzantine node purposefully deviates from the protocol in order to disrupt the normal operation of a network. We can regard its utility function as unknown. In the literature, there are two main approaches to deal with misbehaving nodes: incentives to cooperation [1], [4], [5], [20], [21], [24], [25] or punishment to non-cooperation [2], [14], [15], [17], [22]. These approaches essentially treat selfish and malicious behaviors non-discriminatingly, but either one of them is not adequate to deal with both types of misbehaving nodes. For example, the mission of Byzantine nodes is to cause network disruption, no mechanism can encourage them to cooperate. On the other hand, the punishment based approach might be helpful for mitigating Byzantine behaviors, nevertheless it forces rational nodes to cooperate, which is not reasonable for some cases. Instead, we believe that rational and Byzantine behaviors need to be treated separately.

In [20], [21], we considered the problem of multi-path routing with selfish nodes. We proposed the generalized second price (GSP) auction to deal with rational behaviors, leading to Nash equilibria in which selfish nodes honestly participate in the routing process. However, even with GSP auction, it is expected that Byzantine nodes behave nicely in the routing stage to attract the routing protocol to select them. Once they are selected and asked to forward data packets, they will reveal their uncooperative nature such as not forwarding any data packets. In this paper, we extend our work to cope with Byzantine behaviors. We propose the FORBID mechanism for this purpose. The remainder of this paper is organized as follows. Section II formalizes the system model. Section III discusses the design of the proposed mechanism. Following that, Section IV evaluates its performance through extensive experiments. Section V reviews related work, and Section VI concludes the whole paper.

II. THE SYSTEM MODEL

A. The Network Model

We focus on multi-path routing and forwarding in wireless ad hoc networks. A wireless ad hoc network is formed by a finite number of nodes, denoted by $\mathcal{V} = \{1, 2, \dots, n\}$. The existence of the directed edge $(i, j) \in \mathcal{E}$ between node i and

Xueyuan Su was supported by a Yale University Fellowship. Sammy Chan was supported by a grant from the Research Grants Council of the Hong Kong SAR, China [Project No. CityU 111208].

node j is dependent on the transmission power. We assume that each node i has a set \mathcal{P}_i of discrete transmission power levels. For any $i, j \in V$, there is a minimum power level P_{ij} at which node i could transmit packets to node j . If $P_{ij} \leq \max(\mathcal{P}_i)$, then we say node j is reachable from node i . In this way, the network could be represented by a weighted directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, \mathcal{W}\}$, where \mathcal{W} is the set of weights representing the cost on each edge.

Each node $i \in \mathcal{V}$ is assigned an inherent value $\gamma_i \in [0, 1]$, indicating the probability that a data packet will not be successfully forwarded by i if a path including i is chosen for packet forwarding. γ_i is private for each i . We set a threshold T . If $\gamma_i \leq T$, i is regarded as non-Byzantine and the possible packet loss is due to interference or link failures. If $\gamma_i > T$, i is regarded as Byzantine and the packet loss is due to malicious misbehavior. We accept that a non-Byzantine node could have non-zero probability of dropping a data packet, such that broader network scenarios are included in our model.

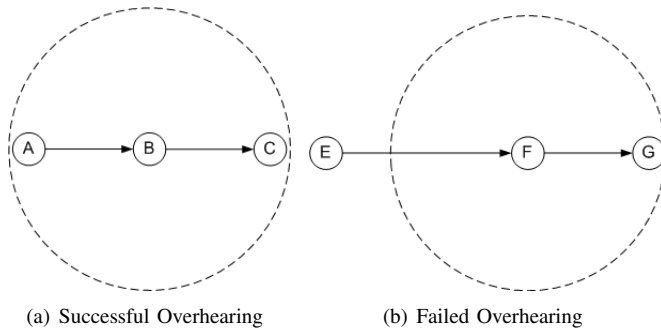


Fig. 1. Unreliable overhearing, the dashed circle represents the transmission range of the centering node.

In previous studies [2], [14], [15], [17], the most fundamental technique used to identify misbehavior is passive overhearing, or “watchdog” [14]. This technique works well assuming that wireless links are *symmetric*. As illustrated in Fig. 1(a), the idea is that when an intermediate node B is forwarding packets from the upstream node A to the downstream next hop C , A could monitor its behavior by overhearing the ongoing transmission. If no packets are forwarded by B or the forwarded packets are not the same as the original ones, A will suspect that B is misbehaving.

However, this passive overhearing technique is not always reliable. Asymmetric wireless links are quite common due to diverse channel conditions and dynamically adjusted transmission power. Take Fig. 1(b) for example. When node F is forwarding packets from E to the downstream node G , E is out of its transmission range. In this case, the overhearing technique fails and node F may be punished although it is innocent. In this paper, we take into account the *asymmetric* property of wireless links.

B. The Packet Delivery Model

When the source node S communicates with the destination node D , data packets might hop over several intermediate nodes. Transmitting a data packet introduces transmission cost to each intermediate node. From the system-wide perspective the goal is to minimize the total transmission cost.

Packet delivery is divided into two consecutive stages, *routing* and *forwarding*. In the routing stage, S sends out route request (RREQ) messages to discover available node-disjoint paths to D . Intermediate nodes insert routing information into such RREQ messages and forward them to the next hop. The destination node collects routing information stored in RREQ messages and return it to S via route reply (RREP) messages. At the end of the routing stage, S selects multiple least cost paths (LCPs) and calculates the percentage of data traffic to be forwarded via each LCP. The payment for each intermediate node has also been determined by the mechanism in routing stage. Now the data packets are ready to be transmitted and we enter the forwarding stage.

For the sake of simplicity, we have two initial assumptions:

- There is no collusion among intermediate nodes.
- Either there are no rational nodes, or rational nodes have been stimulated for cooperation by auction mechanisms such as [1], [21], [24] during the routing stage.

III. FORWARDING STAGE MECHANISM DESIGN

We discuss our mechanism design for the forwarding stage here. We propose a reputation system called *FORBID*, standing for *Flocking ORiented Bayesian Inference with Detections*.

A. Packet Forwarding and Payment Realization

Similar to the *burst mode* with Cisco Aironet wireless adapter [18], we allow several data packets to chain together and be forwarded as a burst of block. The source S sends out each block with its digital signature and then waits for the confirmation from the destination before sending out the next block. In order to increase the efficiency of the digital signature scheme, one can use the hash-and-sign paradigm [19], in which each node signs the hash value of a block instead of the full block. Upon receiving each block from the upstream node, each intermediate node checks the validation of the block and then forwards it to its next hop at the computed power levels if the signature is valid. Upon successfully receiving each block, D sends a backward confirmation via multi-path back to S . All the intermediate nodes keep the appropriate confirmation as a means of getting payment. After checking the validation of the confirmation, S could make the corresponding payment or keep a record for this part of traffic. Then S sends out the next block. The whole procedure proceeds repeatedly until all data blocks are transmitted.

We adopt the same requirement in IEEE 802.11[11] that, each node must return a media access control (MAC) layer acknowledgement (ACK) to the upstream sender after correctly receiving a packet. The distinction is that such MAC layer ACKs should include some cryptographic information that cannot be forged by anyone else. After forwarding each packet, the intermediate node maintains the ACK from the next hop as a receipt. The function of these receipts is twofold. When the packet is lost due to downstream Byzantine nodes along the path, 1) receipt holders could use these receipts to get the deserved payment even if the block confirmation from D cannot arrive; 2) the reputation system could use this receipt to narrow down the suspects of Byzantine nodes. Note

that different from some previous schemes [9], [25], in our mechanism, an intermediate node can get its payment as long as it has forwarded the packets to the next hop, regardless of whether the packets finally arrive at D .

When an intermediate node cannot get ACKs from the next hop after forwarding data packets, it suspects that the downstream node is Byzantine and makes the corresponding note in its reputation record to be discussed later. In this case, the intermediate node cannot get the deserved payment or report the receipt of ACKs when the detection process is triggered. Then it will lose reputation among others. Therefore, we require this node to retransmit the packet with its highest transmission power level such that at least one upstream node can overhear the retransmission and act as witness during the detection process.

B. Detection: Identify Byzantine Behaviors

Data packets are forwarded through each LCP proportional to its allocated percentage. If packets along one of them, say LCP_k , do not get through to D , then S cannot receive backward confirmation of the packets that go through LCP_k . In this case, S reschedules the portion of data intended to be forwarded along LCP_k to other LCPs and recalculates the payments without directly performing the expensive rerouting procedure.

At the same time, S triggers a detection process which requires each intermediate node along LCP_k to report its receipt of ACKs from the next hop. If a node can neither report the receipt of ACKs nor have any upstream nodes as witness, then its reputation is degraded. In the worst case, if all the LCPs fail, then S needs to decide whether to reselect new LCPs from the previously excluded paths or to trigger rerouting.

C. Bayesian Inference: Update Internal Reputation

Each node i internally maintains a reputation list, which keeps the reputation record for other nodes in the network. Let α_{ij} be the number of occurrences of evidence available at node i that node j deviates from the protocol (called *negative evidence*), and β_{ij} be the number of occurrences of evidence available at i that j follows the protocol (called *positive evidence*). Every time when a data packet is successfully sent from S to D , β_{ij} is increased by 1 where $i \in \{S, D\}$ and j is in the set of all participating intermediate nodes. Every time when a node j is caught in the detection process, α_{ij} is increased by m where $i \in \{S, D\}$ and m is the number of lost packets.

Let random variable $X_{i,j}$ represent i 's belief that how likely j is Byzantine. Based on α_{ij} and β_{ij} , node i computes $E(X_{i,j})$ as the reputation value for j , or i 's evaluation of γ_j . We do not require all the non-Byzantine nodes in the network reach agreement on their beliefs, which is essentially the Byzantine generals problem [13]. Instead, each node maintains its own reputation beliefs and relies on them to make decisions.

Initially, this belief is neutral, i.e., node i regards node j as a Byzantine node with probability 50%. This belief will be continuously updated internally by node i when new evidence

becomes available. When such a belief exceeds the threshold T , it discards all the routing information that includes j . Node i will not ask j to forward packets until the belief becomes below the threshold.

We use Bayesian inference to perform such internal updates. There are two subactions by node j , either deviating from the protocol or following the protocol. Therefore, the family of binomial parameter distributions is a natural choice. Let $Y_{i,j}$ be the event that the number of negative and positive evidence are α_{ij} and β_{ij} , respectively. Given $X_{i,j} = \gamma_j$, the conditional probability is

$$\Pr_i(Y_{i,j}|X_{i,j} = \gamma_j) = \binom{\alpha_{ij} + \beta_{ij}}{\alpha_{ij}} \gamma_j^{\alpha_{ij}} (1 - \gamma_j)^{\beta_{ij}} \quad (1)$$

Since α_{ij} and β_{ij} are fixed as current available evidence and γ_j is unknown, (1) specifies a likelihood function for $X_{i,j}$. According to Bayes' theorem [10] and the continuous form of the law of total probability, we compute the posterior probability as

$$\Pr_i(X_{i,j} = \gamma_j|Y_{i,j}) = \frac{\Pr_i(Y_{i,j}|X_{i,j} = \gamma_j) \Pr(X_{i,j} = \gamma_j)}{\int_0^1 \Pr_i(Y_{i,j}|X_{i,j} = x) \Pr(X_{i,j} = x) dx} \quad (2)$$

For some special choices of the prior distribution, the integral can be easily solved and the posterior takes a convenient form. We propose to use the binomial parameter beta distribution [8]. This is a family of continuous probability distributions defined on the interval $[0, 1]$ parameterized by two positive shape parameters. Assume X is a random variable of the beta distribution with parameters (α, β) , then the probability density function is

$$f(x; \alpha, \beta) = \frac{1}{B(\alpha, \beta)} x^{\alpha-1} (1-x)^{\beta-1},$$

where $B(\cdot)$ is the beta function.

Two special properties of the beta distribution makes it quite convenient for the use here. First, the expectation is

$$E(X) = \frac{\alpha}{\alpha + \beta} \quad (3)$$

Second, if the prior distribution is a beta distribution with parameters α and β , after the calculation of posterior probability with new evidence α' and β' , the resulting distribution is still a beta distribution with parameters $(\alpha + \alpha', \beta + \beta')$.

Therefore, with the beta distribution, node i can easily perform internal updates and calculate the belief as

$$E(X_{i,j}) = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}} \quad (4)$$

In order to conform to the initial neutrality assumption, we set the initial condition at each non-Byzantine node i as

$$\alpha_{ij} = \beta_{ij} = 1, \quad \forall j$$

This leads to the initial belief $E(X_{i,j}) = \frac{1}{1+1} = 50\%$. When new evidence comes, say, α'_{ij} and β'_{ij} as the number of new negative and positive evidence respectively, node i updates the new parameters as $(\alpha_{ij} + \alpha'_{ij}, \beta_{ij} + \beta'_{ij})$. The updated belief is then computed as the posterior expectation as

$$E(X_{i,j})' = \frac{\alpha_{ij} + \alpha'_{ij}}{\alpha_{ij} + \alpha'_{ij} + \beta_{ij} + \beta'_{ij}} \quad (5)$$

D. Flocking: Disseminate Reputation Information

Some previously proposed schemes [14] forbid dissemination because of the fact that Byzantine nodes may take advantage of dissemination to start false accusation attacks. However, when information dissemination is not used, the time needed to detect malicious nodes can be fairly long. Therefore, we will carefully use information dissemination to shorten the misbehavior detection time.

Each node periodically sends reputation information to its neighbors. From a neighboring node j , node i receives the reputation information $(\alpha_{jk}, \beta_{jk})$ for all $k \neq i, j$. This information is cryptographically signed by j and i first verifies the signature. If it is correct, node i updates its reputation record with a special flocking algorithm to be described below.

Let $v_t(i)$ be a value stored at i at time t , such as α_{ij} or β_{ij} . In a standard flocking algorithm [7], the evolution rule is

$$v_{t+1}(i) = \frac{1}{d_t(i) + 1} \left(v_t(i) + \sum_{j:(i,j) \in G_t} v_t(j) \right), \quad (6)$$

where $d_t(i)$ is the degree of node i in graph G_t .

It is obvious that under this evolution rule, the internal value computed by node i and the incoming value from each of i 's neighbors are treated non-discriminatingly. However, in our reputation system, as we have explained earlier, the internal value obtained by detection and observation should be prior to the incoming value obtained by information dissemination. Also, node i may have different reputation record for each of the neighbors. It is reasonable that it gives higher weights to the ones it trusts more. Therefore, we need to redesign the flocking algorithm to consider different weights. Let $w_t(i, j)$ denote the weight that node i assigns to node j at time t . The weighted flocking algorithm is proposed as

$$v_{t+1}(i) = w_t(i, i)v_t(i) + \sum_{j:(i,j) \in G_t} w_t(i, j)v_t(j) \quad (7)$$

Since the internal value obtained by detection and observation has the highest priority, $w_t(i, i)$ is set to a large value. The weights assigned to the neighbors are determined by their *trust levels* computed by node i . Assume j is a neighbor of i . Let $\ell(i, j)$ denote its trust level computed by node i . We compute $\ell(i, j)$ as

$$\ell(i, j) = 1 - E(X_{i,j}) \quad (8)$$

Then the weight that i assigns to j is calculated as

$$w(i, j) = [1 - w(i, i)] \times \frac{\ell(i, j)}{\sum_{k:(i,k) \in G_t} \ell(i, k)} \quad (9)$$

Combining Eqs. (7, 8 and 9), we get the complete weighted flocking algorithm for reputation dissemination. Each node periodically uses this flocking algorithm to exchange the number of negative and positive evidence with all neighbors.

IV. PERFORMANCE EVALUATIONS

In this section, we study how effectively the proposed FORBID mechanism could identify and isolate Byzantine nodes. We have developed an event-driven simulator using C++

programming language. Although FORBID could potentially be built on top of any source routing protocols, in particular, we implement it over DSR protocol [12].

The general settings are as follows. Consider a network consisting of non-colluding nodes. We choose the locations and transmission power levels such that these nodes are randomly connected by wireless links based on the transmission range. Nodes do not move once their locations are fixed. The false overhearing problem discussed in Section II exists in the network. Without loss of generality, each source generates data packets at the rate of 1 packet per second. The transmission latency of a single packet between two nodes is set to be 1 second. Unless explicitly mentioned, the default network and algorithm parameters are as follows: the total number of nodes is 90, 30% of nodes are randomly chosen to be Byzantine, $w_t(i, i) = 0.998$ for all i and t , and $T = 0.505$.

A Byzantine node pretends to work well during the routing stage, but potentially misbehaves during the forwarding stage. We generate two kinds of malicious behaviors: (1) during the forwarding stage, a Byzantine node drops each data packet with some probability generated from a normal distribution $N(0.7, 0.05)$ and truncated to be in $[0, 1]$; (2) during each step of reputation dissemination, a Byzantine node randomly selects another node and sends false accusation of it with probability 0.5.

The performance metric is the packet loss rate, which is defined as the *ratio* between the number of lost packets and the total number of packets sent by all source nodes. We vary different parameters to generate different scenarios. For each scenario, the results are obtained by averaging over five independent experiments.

In the first scenario, we study the impact of the percentage of Byzantine nodes on the performance of FORBID. The result is as shown in Fig. 2. For comparison, we include the performances of two other schemes. For “defenseless”, it refers to the case that the network is equipped with no mechanism against Byzantine behaviors. For “watchdog-1”, it refers to an enhanced Watchdog scheme, in which Watchdog is combined with an information exchange mechanism based on the linear opinion pool [3]. To show the effect due to the false overhearing problem, we also include the result (“watchdog-2”) for the enhanced Watchdog mechanism in a network without this issue.

In the case without any mechanism against misbehavior, a small percentage, say 20%, of Byzantine nodes already causes a significant packet loss rate of over 55%. Watchdog is able to effectively mitigate packet loss rate by passive overhearing. With 20% of Byzantine nodes, it achieves a packet loss rate slightly below 10%. However, this improvement could be compromised when the overhearing is not always accurate. The packet loss rate is increased to 16% when false overhearing exists. FORBID, as we expected, offers even better performance in avoiding packet loss. The packet loss rate is reduced to 3%. With the further increase of the percentage of Byzantine nodes up to 90% in our experiments, FORBID always exhibits obvious advantage over watchdog. Such observations confirm FORBID's effectiveness in detecting and isolating Byzantine nodes.

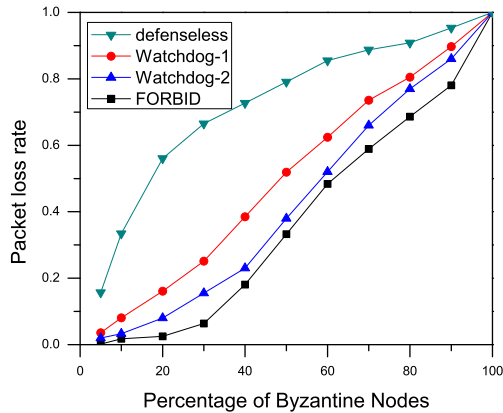


Fig. 2. Packet loss rates under different mechanisms.

It would be interesting to see how effectively that FORBID identifies Byzantine nodes, by comparing the evolution of reputation values for rational and Byzantine nodes. In particular, we target at two nodes of different categories - node 27 being rational and node 38 being Byzantine. We keep track of the reputation values for the two nodes at three disperate network locations, on nodes 6, 16 and 56, respectively.

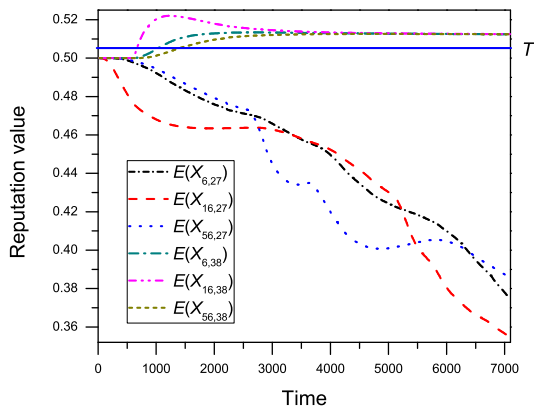


Fig. 3. Evolution of reputations, rational vs. Byzantine.

The six traces are shown in Fig. 3. For example, $E(X_{6,38})$ describes the belief of node 6 on how likely node 38 is Byzantine. Initially, both nodes 38 and 27 are treated equally. Overtime, the rational node 27 gains better and better reputation (small value) among other nodes. The reason is that by forwarding packets for other nodes, it gains better reputation and in turn gains more chance of being chosen by the routing protocol due to its good reputation. On the other hand, the reputation values for the Byzantine node 38 quickly increases over time. Then the value enters the steady state, which indicates node 38 has been successfully isolated. The quick convergence speed shows that FORBID is able to detect Byzantine nodes within a short time period.

Next we study the impact of $w_t(i, i)$ as part of the flocking algorithm. We compare the two different scenarios: with and

without false accusations from Byzantine nodes. The results are shown in Fig. 4. With false accusations, small values of $w_t(i, i)$ lead to high packet loss rate. This is because false reputation information from Byzantine nodes weighs too much in the flocking algorithm, and thus makes the reputation mechanism less useful. When we increase the value of $w_t(i, i)$, reputation information from other parties becomes less weighted. As a result, false accusation attacks become less effective. However, if we further increase $w_t(i, i)$ to values close to 1 and thus (almost) disable the flocking algorithm, packet loss rate is actually increased. This is due to the fact that without information dissemination, the latency to detect misbehavior becomes so long that malicious nodes could potentially do more harm to data packet forwarding. Without false accusations from Byzantine nodes, the packet loss rate is not sensitive to small values of $w_t(i, i)$. However, we observe similar trend when $w_t(i, i)$ is close to 1. This experiment confirms that information dissemination, if used properly, is useful to shorten the detection time. However, it is very important to choose suitable weights such that good trade-off is achieved in case of false accusation attacks. In addition, by comparing with the data points in Fig. 2 with 30% Byzantine nodes, we can see that the performance of FORBID is better or comparable to that of Watchdog with a large range of weight values.

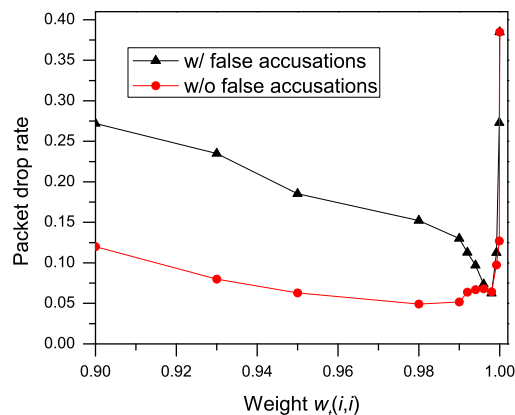


Fig. 4. Packet loss rates with and without false accusations.

Due to limited space, we will report results on the impact of other parameters like network size and the threshold T in future work. These results further demonstrate the effectiveness of FORBID over a wide range of systems.

V. RELATED WORK

The first reputation system to identify and then avoid Byzantine nodes was proposed by Marti *et al.* in [14]. It is comprised of the watchdog and pathrater components. Watchdog relies on passive overhearing for detection of denied packet forwarding and pathrater rates every path used. An obvious drawback of this solution is that Byzantine nodes are not punished and their packets can still be forwarded by others. CONFIDANT [2] updates reputation record by means of experience, observation and report from friends. A path manager is used for

nodes to adapt their decision according to reputation record. An improved way of representing, updating and integrating reputations based on a Bayesian approach is proposed in [3]. The limitation of these works is that the reputation record update is not always reliable and how to select friends has not been suggested. Michiardi and Molva proposed CORE in [15]. A watchdog component complemented by a sophisticated reputation mechanism is adopted. This mechanism differentiates between subjective reputation (watchdog observation), indirect reputation (reports by others) and functional reputation (task-specific behavior). The problem of CORE is that watchdog may not be applicable for asymmetric links and many other situations. This method also tends to overestimate the selfish behavior of nodes, due to the effects of radio errors or packet collisions that can be mistaken for intentional packet drops. How to deal with unreliable observation and false accusation needs to be considered. Two enhancements to the watchdog method have been proposed in [17] to reduce the impacts of inaccurate observations due to packet collisions and link failures. Firstly, nodes exhibiting misbehavior are not punished immediately. Instead, they are put into a warning mode so that falsely accused nodes are given a chance to demonstrate they are in fact cooperating. Secondly, if it is found that a node does not cooperate only due to link failure, its reputation will not be degraded. Although the performance of the watchdog method is improved, the fundamental problem of overhearing is not addressed. In [23], a Dirichlet reputation system is proposed to differentiate good, selfish and malicious nodes. A moving window mechanism is also proposed to adjust responsiveness of the system to changes of node behaviors. The establishment of the reputation record in each node is only based on its own observations and reputations reported by its immediate neighbors based on their first-hand observations. Besides malicious nodes, path selection in this scheme also tends to avoid rational nodes. This is contrary to our belief that better performance can be obtained if rational nodes are provided incentives to cooperate.

VI. CONCLUSION

We have presented the FORBID mechanism to cope with Byzantine behaviors in wireless multi-path routing and forwarding. Different from previous work that relies on passive overhearing, the proposed mechanism actively triggers detection process to collect evidence of Byzantine behaviors. Upon the availability of new evidence, each node uses Bayesian inference to update their beliefs that whether each of the other nodes is trustworthy. To accelerate the detection and isolation of malicious nodes, FORBID includes a carefully designed flocking algorithm to disseminate reputation information among nodes. Experimental results show that FORBID could effectively isolate Byzantine nodes and thus reduce the packet loss rate.

As the next step, we are currently working on combining our previous result on GSP auction with the FORBID reputation mechanism. Our goal is to design a jointly optimized mechanism that is provably effective in handling both rational and Byzantine behaviors.

REFERENCES

- [1] L. Anderegg and S. Eidenbenz. Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In *Proceedings of the ACM MobiCom*, pages 245–259, 2003.
- [2] S. Buchegger and J. Le Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of the ACM MobiHoc*, pages 226–236, 2002.
- [3] S. Buchegger and J. Le Boudec. The effect of rumor spreading in reputation systems for mobile ad-hoc networks. In *Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, volume 4, 2003.
- [4] L. Buttyán and J. Hubaux. Enforcing service availability in mobile ad-hoc WANS. In *Proceedings of the ACM MobiHoc*, pages 87–96, 2000.
- [5] L. Buttyán and J. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*, 8(5), 2003.
- [6] L. Buttyán and J. Hubaux. *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*. Cambridge University Press, 2007.
- [7] M. Cao, D. A. Spielman, and A. S. Morse. A lower bound on convergence of a distributed network consensus algorithm. In *Conference on Decision and Control*, 2005.
- [8] B. Carlin and T. Louis. *Bayesian Methods for Data Analysis (Texts in Statistical Science)*. Chapman and Hall/CRC, New York, 2008.
- [9] S. Eidenbenz, L. Anderegg, and R. Wattenhofer. Incentive-compatible, energy-optimal, and efficient ad hoc networking in a selfish milieu. In *40th Annual Hawaii International Conference on System Sciences*, 2007.
- [10] A. Gelman. *Bayesian data analysis*. Chapman and Hall/CRC, New York, 2004.
- [11] IEEE Standards Department. IEEE 802.11 standard for wireless LAN, medium access control (MAC) and physical layer (PHY) specifications. 1999.
- [12] D. Johnson. Routing in ad hoc networks of mobile hosts. In *Proceedings of the Workshop on Mobile Computing Systems and Applications*, pages 158–163, 1994.
- [13] L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.
- [14] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the ACM MobiCom*, pages 255–265, 2000.
- [15] P. Michiardi and R. Molva. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Advanced communications and multimedia security: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, 2002.
- [16] M. Osborne and A. Rubinstein. *A course in game theory*. The MIT press, 1994.
- [17] A. Rodriguez-Mayol and J. Gozalvez. Improving selfishness detection in reputation protocols for cooperative mobile ad-hoc networks. In *Proceedings of the IEEE PIMRC*, pages 26–29, 2010.
- [18] P. Roshan and J. Leary. *802.11 wireless LAN fundamentals*. Cisco Systems, 2004.
- [19] D. Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, New York, 2006.
- [20] X. Su, S. Chan, and G. Peng. Auction in multi-path multi-hop routing. *IEEE Communications Letters*, 13(2):154–156, 2009.
- [21] X. Su, S. Chan, and G. Peng. Generalized second price auction in multi-path routing with selfish nodes. In *Proceedings of the IEEE GLOBECOM*, pages 3413–3418, 2009.
- [22] S. Tomasin. Consensus-based detection of malicious nodes in cooperative wireless networks. *IEEE Communications Letters*, 15(4):404–406, april 2011.
- [23] L. Yang, A. Cemerlic, and X. Cui. A dirichlet reputation system in reliable routing of wireless ad hoc network. *Security and Communication Networks*, 3(2-3):250–260, 2010.
- [24] S. Zhong, J. Chen, and Y. Yang. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Proceedings of the IEEE INFOCOM*, volume 3, pages 1987–1997, 2003.
- [25] S. Zhong, L. Li, Y. Liu, and Y. Yang. On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretic and cryptographic techniques. *Wireless Networks*, 13(6), 2007.