Reputation Based Routing in MANET using Blockchain

Maqsood Ahamed Abdul Careem and Aveek Dutta
Department of Electrical and Computer Engineering
University at Albany SUNY, Albany, NY 12222 USA
{mabdulcareem, adutta}@albany.edu

***Abstract*—One of the core issues in routing packets within Mobile Ad hoc Networks (MANETs) is the lack of trust and reputation of the participating nodes, which often leads to unreliable packet delivery. We use a fraction of nodes to validate routing actions taken by other nodes and leverage the distributed consensus mechanism in Blockchain networks to accrue the reputation of each node. Specifically, we employ heterogeneous difficulty for Proof of Work to represent the credibility of validation and design a scoring system to isolate malicious nodes via distributed consensus. The reputation of a node is then based on the combination of the difficulty level and the score. This reputation is incorporated in a novel routing metric to calculate the shortest, most reputed path between a source and destination node. The goal is to discourage malicious nodes by excluding those from participating in routing packets. A joint simulation of the Blockchain and routing algorithm reveal $\approx 12\%$ improvement in overall packet delivery in the presence of routing attacks, compared to conventional routing algorithms in MANETs.**

I. Introduction

With the advent of the Internet of Things (IoT), there is a renewed interest in MANETs, especially in security and veracity of low-power networks. Examples of such networks include swarms of Unmanned Aerial Vehicles (UAVs), clusters of sensors in Smart Cities and Smart Homes and Agricultural IoT. Being constrained in resources (power, storage, connectivity, etc.) implementing conventional security apparatus is a challenge, which has led to crosslayer and multi-faceted security models that collectively guarantee higher assurance of these MANETs [1], [2]. We propose and evaluate such a system that assigns reputation to nodes to implement reliable and trustworthy routing of packets. Conventional routing protocols in MANETs are based on some notion of *shortest path* between a source-destination pair, often represented in the number of hops [3]. The goal is to reformulate this cost of routing with the information about the nodes' reputation along the path. Therefore, we introduce the concept of "shortest, most reputed path" routing over simply choosing the shortest path, which is common in existing protocols.

Central to the idea of reputation based routing, is the ability to maintain information about a node's behaviour and assess the reputation in a purely distributed manner among trustless entities. Distributed Ledger Technologies (DLT) like Blockchain provide immutability and distributed consensus for *transactions* between participating nodes, which enables aggregation and dissemination of common knowledge among untrustworthy entities. For example, Bitcoin, uses the Blockchain to record financial transactions while Etheruem [4] and Hyperledger [5] use Smart Contracts [6] to enforce contractual obligations between parties. Similarly, by monitoring the exchange

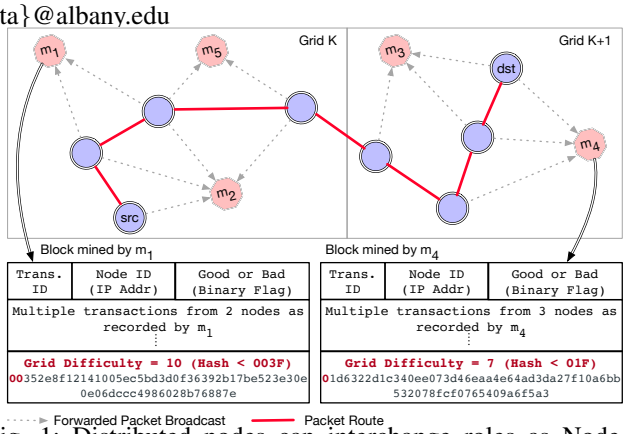


Fig. 1: Distributed nodes can interchange roles as Node or Miner. Miners assess the actions of the routing node and create transactions to record those and Blocks are mined with a Proof of Work difficulty proportional to number of miners in a grid. The historical actions recorded in the blockchain is used to assign reputation to each node in the MANET.

of wireless packets between nodes in a MANET we can create unique transactions that record the actions (*good* or *bad*) taken by the nodes in routing a particular packet. The Blockchain is then used to record these transactions from the genesis of the network and all the nodes arrive at a consensus on those actions by employing a Proof of Work or Proof of Stake algorithm as done in various DLTs. Key element in computing the historical reputation of any node, is the *Difficulty* parameter of the consensus algorithm. The intuition here is that a higher concentration of Miners (or Validators) in the vicinity can afford to mine blocks with higher difficulty while maintaining a consistent average time to mine a Block across the network. This is quite different from conventional mining activity where all Miners are assigned the same Difficulty of mining [7]. Hence, with variable difficulty, the information contained in a block that is mined with higher difficulty is deemed as more credible as more resources (energy or stake) are required to mine that block. Therefore, a non-linear function of the average of the historical actions (represented by a numerical score) recorded in the Blockchain, weighted by the difficulty of the consensus algorithm is used to adjust the cost function to implement shortest, most reputed path routing.

Network Model: In a MANET, the area of interest is divided into K finite grids denoted by $k \in \{1, \ldots, K\}$, as shown in figure 1. Even though figure 1 shows equal sized grids, our approach supports any cell shape and size. Let $\mathcal{N} = \{n_1, \ldots, n_N\}$ be the set of N wireless nodes and $\mathcal{M} = \{m_1, \ldots, m_M\}$ be the set of M miners in a given area. The nodes and the miners

are mobile entities with omnidirectional antennas having fixed transmission range. Distributed nodes can interchange roles as routing Node or Miner. Typically, nodes with more processing power are likely to assume the role of a Miner. Thus, there are typically more nodes than miners ($M \ll N$) in any given grid. The nodes may route data packets to any other node within the same or different grid, as shown by red line in figure 1.

Blockchain Model: Each grid represents the region of reachability of miners from each node within that grid such that the packets forwarded by the nodes are received by at least one miner in the vicinity (shown as dotted arrows in figure 1). Each miner monitors the actions taken by the nodes in routing the packets and flags them as good or bad actions and records them as transactions. These transactions are aggregated by the miner and used to create a block. In this work, the role of Blockchain is two fold: 1) Provide an immutable record of the behavior of the nodes and 2) By requiring the *Difficulty* for mining to be proportional to the number of miners in the grid, it acts as a measure of credibility of the validation. The mined blocks are multicast within the miners to converge on the block that is mined with the highest difficulty as it is deemed as the most credible validated block [8]. We define this as the *Most-Difficult-Chain* consensus. Once each Miner gets an updated Blockchain state, it broadcasts that to the nodes within the grid to update their local states as well. The information stored in the blockchain is used to calculate the reputation of each node to be used in computing future routes. This work is not restricted to any specific type of financial incentives and any method to reward the miners or the nodes is applicable [9], and are excluded from the scope of this work.

Threat Model: *1) Malicious Nodes (Routing threat):* A *black hole* attack is caused by a malicious node absorbing all incoming traffic, by disseminating false routing information. In *Grey hole* attacks packets are dropped selectively (e.g., all routing packets are forwarded but data packets are dropped) [10]. In a *Misrouting* attack an illegitimate node sends data packets to the wrong destination by modifying the destination address or by forwarding packets to wrong next hop node. We show, that by assigning reputations to nodes based on their historical forwarding actions, the above threats are mitigated. *2) Malicious Miners (Blockchain threat):* Malicious miners may inject false transactions in the block they mine. Additionally, traditional threats in blockchain, like the 51% attack [11] are possible but become less likely as the chain grows with more packets being routed and when more miners are present in the network. Thus, a successful attack results in the forging of the current or most recent blocks. Since, the miners may assume the role of a node in the future and the routing of packets from it will depend on the reputation of other intermediate nodes, the miners are intrinsically discouraged from falsifying.

Therefore, we make the following contributions:

1) A novel Blockchain design to record the routing actions of nodes, where the Difficulty of mining is proportional to the number of miners in a grid. This provides a measure of credibility of validation (§II).
2) A non-linear function to aggregate historical routing actions and the difficulty of the block to compute a reputation score for each node (§III-B).
3) Novel routing protocol that leverages reputation of nodes to achieve "shortest, most reputed path" routing (§III-C).
4) Practical evaluation on integrated Blockchain based reputation management and MANET routing simulator (§IV).

II. Blockchain to record Actions

A. Anomaly Detection

We present the "shortest, most reputed path" routing by integrating the reputation metric in the Ad hoc On-Demand Distance Vector (AODV) routing protocol for MANETs. But we rely on basic mechanisms of route discovery & selection typical to any routing protocol. Hence we claim that this solution can be easily adapted to other MANET routing protocols other than AODV. AODV is a reactive routing protocol which determines the path, $\mathcal{P}$ to route data by flooding route request packets (RREQ) from the source and receiving a corresponding route reply (RREP) from the destination node. During the routing of data packets, if an intermediate node correctly forwards the packet to an intended neighbor (as given by the path, $\mathcal{P}$) it is considered a *good action* and any malicious behaviour (e.g., dropping packets or altering the intended path of packets) is flagged as a *bad action*. Algorithm 1 presents the `BC-AODV` protocol for assessing the reputation of nodes and including the reputation metric in the discovery of the shortest, most reputed path. Lines 2-14 describe the functions of the Miners and lines 15-24 describe the functions of the Nodes in the network. Because the wireless channel is open, each miner can perform localized anomaly detection by overhearing ongoing transmissions within its grid (as in line 3) and evaluating the behavior of its neighbors. We assume that each miner is capable of detecting whether an action performed by a node is good or bad[1] by employing a *watchdog module* within the miner as in [12] and shown in line 5. Each miner keeps a record of information of packets broadcasted by its neighbors and waits for their re-transmissions: a fault event (*bad* action) is detected for a node in the event that data packets are changed or a timeout expires. The watchdog module at each miner outputs the node id (the IP address of the node that performed the action), and a $flag$ associated with the action observed by the miner, defined as $flag$=1 for a *good* action, and $flag$=0 for a *bad* action. For each packet received, the miners' create a transaction by including a transaction id, the node id, and the $flag$ for that action as shown in line 6 and figure 1. The transactions are aggregated and are put in a block as in line 7. The process of creating a block is called *mining* and is outlined in lines 8 and 9.

B. Difficulty of Miners

Algorithm 1 ensures that every node in the MANET contain the most recent copy of the blockchain. Miners in each grid, generates a block $\mathcal{B}$ by aggregating the transactions, iterating over a nonce value and calculating the hash of a block with

[1]Miners may detect a variety of malicious routing behaviour with varying accuracy using a variety of methods [1], [12]. Our work subsumes any such paradigm without loss of generality.

Algorithm 1: BC−AODV: Reputation-based Routing

1 **Function** *BC−AODV(Role, Blockchain, M, k, $|\mathcal{M}_k|$)*
2 **if** *Role = Miner* **then**
3 $pkts$ = Receive packets from nodes in grid k;
4 **for** *each* $pkt \in pkts$ **do**
5 $[nodeID, flag]$ = WatchDogModule(pkt);
6 $transaction = < transID, nodeID, flag >$;
7 $transactions$ = Aggragate all transactions;
8 D_k = Evaluate Difficulty of grid k from (1);
9 $\mathcal{B}$ = CreateBlock($transactions, D_k$);
10 $CandidateChain$ = Add $\mathcal{B}$ to $Blockchain$;
11 Multicast $CandidateChain$ to all miners;
12 Receive $CandidateChain$ from other miners;
13 $Blockchain$=MostDifficultRule($CandidateChain$)
14 Broadcast $Blockchain$ to nodes within grid k;
15 **if** *Role = Node* **then**
16 Receive $Blockchain$ from miners within grid;
17 **for** *each* $n_i \in neighbours$ **do**
18 **for** *each* $\mathcal{B}_l \in Blockchain$ **do**
19 $[|good\ actions|_i^l, |bad\ actions|_i^l]$=Count transactions of n_i in $\mathcal{B}_l$ with flag 1 or 0;
20 Calculate S_i^l from (2);
21 D^l = Extract Difficulty of $\mathcal{B}_l$;
22 Calculate $\mathcal{R}_i$ from (3);
23 Update Reputation Table entry of n_i with $\mathcal{R}_i$;
24 Upon reception of RREQ, increment *route cost* field in RREQ and Routing Table with *link cost* from (4)

the nonce value included [8]. For the block $\mathcal{B}$ to be considered *valid*, a value of a cryptographic hash function has to be less than a target T, i.e., $\mathrm{hash}(\mathcal{B})<T$. The process of creating a valid block, typically requires a large amount of computation, which serves as a Proof-of-Work for the miners. The difficulty is a measure of how hard it is to find a hash below a given target T. Unlike in many blockchain implementations we use a heterogeneous difficulty assignment, where miners in different grids are assigned a different difficulty target, while miners within the same grid are assigned the same difficulty. The difficulty of miners within each grid k is defined as,

$$D_k = \left\lceil D_{max} \times \frac{|\mathcal{M}_k|}{M} \right\rceil \quad \forall k \in \{1, \ldots, K\} \tag{1}$$

where $|\mathcal{M}_k|$ is the number of miners within grid k, determined by counting the status messages exchanged between miners [13] within same grid. M is the total number of miners in the area and D_{max} is the maximum difficulty (designer's choice). The difficulty assumes an integer value in the interval $[1, D_{max}]$ and represents the number of leading zeros in the target T. An example of valid blocks and hashes for different difficulty targets are shown in figure 1.

The mining power or the average hash rate increases proportional to the number of miners. The average time for a pool of miners to create a valid block is inversely proportional to their combined hash rate and directly proportional to the difficulty of the target [7]. Miners in different grids are assigned different difficulty values, such that the average time to create a valid block from each grid remains constant (e.g., 1.5s as detailed in §IV). Hence, a grid with a higher concentration of miners can afford to create a block with a higher difficulty, while a grid with fewer miners would resort to a lower difficulty to mine a block within the same time. With variable difficulty, *the information contained in a block that is mined with higher difficulty is deemed as more credible as more resources (energy or stake) are required to mine that block*. Miners are rewarded according to their effort (the difficulty) [9] while they contend with other miners in the entire network to mine a valid block.

Lines 8-14 describe the miners' actions from creating a valid block to arriving at consensus on blockchain state. Each miner first determines the difficulty level associated with the grid using (1) and creates a valid block with the assigned difficulty level by incorporating the pool of transactions. Once a valid block is created it is added to the current blockchain and multicasted to the other miners in the network. The miners select the candidate chain with the highest aggregate difficulty, which is termed as the *Most-Difficult-Chain rule* (line 13). Since, the Difficulty of mining is a measure of the credibility of validation, the Most-Difficult-Chain represents the most credible validated chain of information. In the event that multiple miners succeed in creating a block, the blockchain may fork. Even if a blockchain fork occurs, the blockchain would converge, because each miner selects the chain with the highest aggregate difficulty and generates a new block following the most difficult chain. Even though blocks are mined and arrive at the miners at different times, the chain is synchronized by the status messages exchanged between miners [13]. In line 15, the miners broadcast the blockchain to all the nodes within their grid.

Choice of Maximum Difficulty (D_{max}): A higher maxmimum difficulty, sets a lower target value for the calculated hash [8]. For a lower D_{max} miners can generate a valid block faster with less computation (suited for resource constrained devices), so the delay in disseminating the information is reduced. However, the blockchain may fork more frequently and its security is compromised, since the amount of computation required by miners to regenerate a valid block is less. Thus, there is a trade-off between computational power (or delay in convergence) and security, which can be exploited to enable BC−AODV depending on the resources available on devices.

III. Reputation based Routing

Lines 15-24 in Algorithm 1 describe the steps taken by each node to calculate the reputation of its neighbours and incorporate it in the routing metric. A copy of the Most-Difficult-Chain is available at all the nodes in the network through broadcasts from the miners within their grid (line 16). We use the transactions recorded in the blockchain to assign reputations to nodes over time and use the reputation of nodes to guide packets through the shortest, most reputed path.

A. Forwarding Score of a Node

Let $\mathcal{B}_l$ represent the l^{th} block in a blockchain of length L. The forwarding score of a node n_i for block $\mathcal{B}_l$, denoted by $S_i^l \in [-1,1]$, is the *net* forwarding behaviour of node n_i based on its good and bad actions recorded in block $\mathcal{B}_l$ defined as,

$$S_i^l = \frac{|good\ actions|_i^l - |bad\ actions|_i^l}{|good\ actions|_i^l + |bad\ actions|_i^l} \tag{2}$$

where $|\cdot|_i^l$ represents the *number* of the particular action performed by node n_i as recorded in $\mathcal{B}_l$. The value of

$|good\ actions|_i^l$ (or $|bad\ actions|_i^l$) is determined by counting the number of transactions in block $\mathcal{B}_l$ associated with node n_i (i.e., the node id field in the transaction matches the IP address of n_i) that has a flag of 1 (or 0) as shown in line 19.

B. Reputation Metric

The reputation of a node n_i is calculated from the information stored in the blockchain as shown in lines 15-24. For a blockchain of length L, the reputation, $R_i \in [0,1]$ is defined by the non-linear sigmoid function, whose exponent, η_i is the historical weighted average of the difficulty of the block, D^l and the forwarding scores of the node n_i for each block, S_i^l,

$$\mathcal{R}_i = \frac{1}{1+e^{-\eta_i}}, \text{ where, } \eta_i = \frac{\beta}{L.D_{max}} \left(\sum_{l=1}^{L} D^l S_i^l \right) \quad (3)$$

where β=8 is the sensitivity factor that asymptotically drives the sigmoid reputation function, $\mathcal{R}_i$ to a value of 1 (or 0), when the exponent, η_i is largely positive (or negative) respectively. The nonlinear reputation function ensures that a node which consistently takes either good or bad actions will converge to a reputation of 1 or 0 respectively over time. Alternatively, the reputation of nodes that frequently alter their behaviour will experience high variations in their reputation metric. The reputation value computed in (3) provides a global view of each node's truthful behavior as monitored by miners over time, which is the basis of the reputed routing solution.

C. Modified Routing Cost Function

In AODV the path length is determined during the reply process, by counting the number of hops traversed. Every time a node receives the RREP message it increments the *hop-count* value by one to account for the new hop through the intermediate node. In contrast, we define a new link cost between two nodes that is not just the hop count but takes into account the reputation of the node attached to the link. BC−AODV protocol (Algorithm 1) determines the cost of routing using the RREQ packets. The hop-count field in the RREQ message in AODV is replaced by a *route cost* field, which is incremented with the *link cost* at each traversing node. The nexthop field the RREQ message is replaced by a *route-list* field that includes the nodes through which the RREQ has traversed. Route discovery involves flooding RREQ packets from the source targeting the destination. An intermediate node receiving an RREQ packet, increments the *route cost* field with the *link cost* and re-broadcasts the RREQ packet. When destination receives an RREQ, it generates an RREP.

When an RREQ packet is forwarded from a node n_i to its neighbour n_{i+1}, the link cost (for the link between n_i and n_{i+1}) is calculated by n_{i+1} and is given by,

$$c(n_i, n_{i+1}) = \alpha + (1-\alpha)(1-\mathcal{R}_i) \quad (4)$$

The node n_{i+1} increments the route cost field in the RREQ packet with $c(n_i, n_{i+1})$. The first term in (4) represents the *hop-count cost* in AODV, i,e., the cost associated with the length of the link (for a single link, the hop-count is 1). The latter term represents the *reputation cost*, i.e., cost incurred due to the reputation of the node that forwarded the RREQ packet. The term $(1-\mathcal{R}_i)$ ensures that when a node is more (or less) reputed, the *reputation cost* is close to 0 (or 1) respectively.

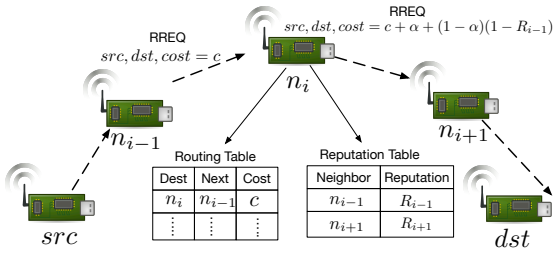


Fig. 2: Operation of BC−AODV protocol: Reputation of nodes are used to modify the cost of a path in RREQ phase. Destination node chooses the path with least cost.

For example, if n_i is a truthful node, then $\mathcal{R}_i \approx 1$ and the latter term is 0, and if n_i is purely malicious then the latter term is $(1-\alpha)$. $\alpha \in [0,1]$ is a tuning parameter (designers' choice) that trades-off the length of the route with the reputation of nodes. In a network with less trustworthy nodes, α maybe chosen close to 0, to include more reputed nodes in the route, towards achieving more reliable routing. Figure 2 illustrates an example route of an RREQ packet from source to destination node. The link cost is added to the cost field of the RREQ packet at the upstream node.

Implementation of BC−AODV: The hop-count field in the *Routing Table* of each node is replaced by the route cost field. Each node also maintains a *Reputation Table* populated with the reputation metric of its neighbours using (3). These changes are shown in figure 2. When an intermediate node receives an RREQ packet, it retrieves the reputation metric for the node that forwarded the RREQ packet from its Reputation Table, and computes the cost of the link using (4) as shown in figure 2. In BC−AODV the destination node and intermediate nodes may receive multiple RREQ packets which are not immediately discarded. This allows the destination node to select the shortest, most reputed route among all the paths taken by the RREQ packets. The ability to receive multiple duplicate RREQ packets at the nodes opens up the possibility of routing loops, which are mitigated similar to [14].

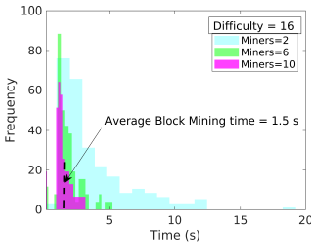
A path $\mathcal{P}$ is defined as the set of nodes that the RREQ packet has traversed through. Using the new link metric in (4) the *route cost* $c(\mathcal{P})$ of a packet traversing through path $\mathcal{P}$ is,

$$c(\mathcal{P}) = \alpha|\mathcal{P}| + (1-\alpha)\left(|\mathcal{P}| - \sum_{n_i \in \mathcal{P}} R_i\right) \quad (5)$$

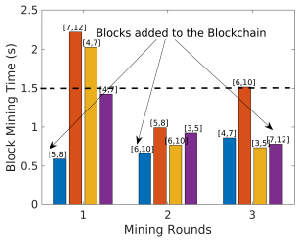
$|\mathcal{P}|$ represents the cardinality of the path and is equal to the number of hops. The destination node receives multiple RREQ packets, and picks the path $\mathcal{P}_{rep}$ with the least *route cost*. This ensures that the path $\mathcal{P}_{rep}$ is the shortest, most reputed path among all possible paths from source to destination given by,

$$\mathcal{P}_{rep} = argmin_{\mathcal{P}}\ c(\mathcal{P}) \quad (6)$$

The destination node sends the RREP packet through the nodes in $\mathcal{P}_{rep}$ in reverse order. Upon reception of RREP packet, the source node routes its data packets through $\mathcal{P}_{rep}$, which is the shortest, most reputed path, since it has the least route cost. The intuition behind including the reputation of nodes in the *route cost* of a path, is to include more reputed nodes in the path while avoiding the less reputed ones. Accounting for the reputation of nodes in the route cost metric of the RREQ packet, ensures an intrinsic security of



(a) Block Mining time with varying number of miners.



(b) Mining time per grid and winning block in each round.

Fig. 3: Impact of the number of miners in each grid on the block mining time and the winning block. In (b) each color bar represents the earliest blocks arriving from each grid. The numbers on the top of the color bar indicate the number of miners and the difficulty in each grid. i.e., $[|\mathcal{M}_k|, D_k]$.

TABLE I: Simulation Parameters

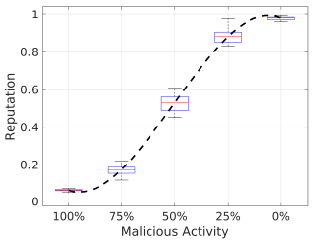
Parameters	Value/Model
Routing Protocol	AODV
Traffic Type	Constant bit rate (CBR)
Transmission Range	30 m
Node Distribution	Uniform Distribution
Mobility Model	Random Waypoint
Area	100m $\times$ 100m
Grid Size	50 m
Number of Nodes (N)	30
Number of Miners (M)	[10, 20]
Cryptographic Hash Function	SHA-256
Maximum Difficulty (D_{max})	16
Tuning parameter (α)	0.5

the protocol: A malicious node cannot modify the impact of its own reputation on the route cost, since the reputation of that node is incorporated in the link cost by upstream nodes.

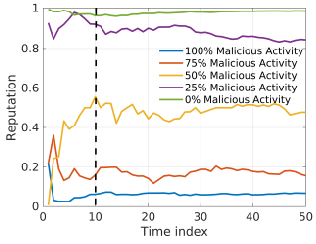
IV. Results

BC−AODV is evaluated using a novel integrated Blockchain-AODV simulator implemented in Matlab with parameters given in table I. We consider a random network topology with several nodes and miners. The nodes and miners are mobile with varying speeds according to a Random Waypoint mobility model and are equipped with a single 802.11 interface and an omnidirectional antenna. Malicious nodes are implemented as nodes that drop bursts of packets with varying probabilities to emulate both black hole and grey hole attacks. Packet dropping is applied exclusively to data packets to include malicious activity in the operation of the routing protocol. This allows malicious nodes to be potentially included in routes. We compare the performance of BC−AODV with AODV protocol.

Blockchain performance: The performance of mining with varying number of miners and difficulty is shown in figure 3. When there are more miners in a grid, the mining power (average hash rate) of the pool of miners increases, and they are capable of generating more hashes per second. Thus, a grid with more miners can create a valid block with a higher difficulty target within a shorter time compared to a grid with fewer miners. Figure 3a shows the improvement in the block mining time with increasing number of miners in the grid, when the difficulty is constant. When there are 10 miners in 1 grid, on average, a valid block is created every 1.5 seconds with a difficulty of 16. Figure 3b shows the time required by miners in each grid to generate a valid block. When the number of miners in a grid increases, their mining power increases proportionally, but the heterogeneous difficulty metric defined in (1) also increases proportionally. Thus, regardless of the number of miners, a valid block is created from each grid (on average) at the same time. But, the block added to the most-difficult-chain is the block with the highest difficulty (i.e., the most credible block among the miners) that is mined within a block-wait-time of 1.5 s. As shown in the figure, in the first and third mining rounds the miners in grid 1 and grid 4 respectively, successfully create the most difficult blocks within 1.5 s and are added to the most-difficult-chain.



(a) Reputation vs maliciousness



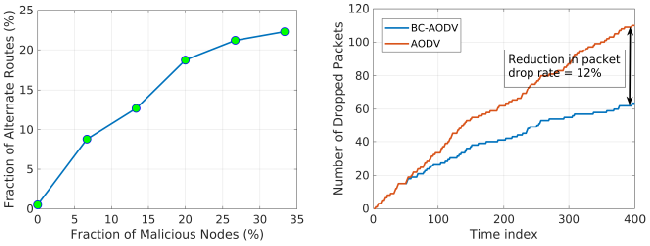
(b) Reputation over time

Fig. 4: Reputation in (3) with varying degree of maliciousness.

Reputation Metric: Figure 4 shows the reputation assigned to nodes, with varying degrees of malicious activity. Nodes drop packets with a probability equal to their degree of maliciousness. The nonlinearity of the reputation function as shown in Figure 4a, further accentuates the reputation accrued by predominantly truthful nodes while diminishing that accrued by malicious nodes, which consequently helps include more reputed nodes in the route. Nodes that predominantly exhibit good behaviour ($malicious\ activity < 10\%$) by truthfully forwarding packets accrue a reputation of 1. Malicious nodes that continuously drop packets ($malicious\ activity > 90\%$: e.g., a continuous black hole attack) will accrue a reputation close to 0, due to the vast number of flagged bad transactions. The reputation of nodes that arbitrarily alter their (good or bad) behaviour by dropping or forwarding packets with a certain probability, are more susceptible to change based on their relatively dominant behaviour. For example, the nodes which exhibit $malicious\ activity$ between 25% to 75% accrue reputation that accurately reflects its degree of malicious activity.

The variation in the reputation of nodes over time is shown in figure 4b. Over time, the reputation values of nodes that exhibit consistently, either good or bad behaviour settle much quicker, compared to nodes that exhibit alternating behaviour. It is clear that after about 10 blocks the reputation of nodes settle to within 10% of their steady state reputation. It is important to note that even in the presence of a malicious miner the impact on the reputation is minimal. This is because, the reputation of any node is assimilated from the entire blockchain. Even if a malicious miner manages to create valid blocks with forged information, the impact of these few forged blocks on the reputation decreases significantly with the number of miners and the length of the blockchain.

Routing Performance: While AODV protocol identifies the shortest path (in terms of the Hop Count) from source to destination node, BC−AODV determines the shortest, most reputed



(a) Fraction of route alterations in BC−AODV from AODV.

(b) Cumulative sum of packets dropped over time.

Fig. 5: Comparison of the performance of the BC−AODV with AODV in the presence of malicious nodes.

path. The difference in the paths selected by both algorithms is more pronounced in the presence of larger number of malicious nodes. This is because BC−AODV strives to avoid including malicious nodes in the route. Figure 5a shows the number of times BC−AODV chooses a different path from that chosen by AODV, with the fraction of malicious nodes. When the fraction of malicious nodes increases, BC−AODV will select more paths that are different from AODV.

The metric for packet loss is defined as $|\text{Dropped Packets}| = |\text{Packets Sent}| - |\text{Received Packets}|$, where $|\cdot|$ represents the *number* of the particular type of packets. Figure 5b compares the number of packet drops in AODV and BC−AODV when 10% of the nodes exhibit black hole attack (by dropping all their data packets). At the beginning, BC−AODV performs similar to AODV since it takes some time to assess the behaviour and reputation of nodes as shown in figure 4b. However, once the reputation of nodes have been assessed, over time the number of packet drops in BC−AODV is significantly less compared to AODV. This is because BC−AODV is able to identify malicious nodes by their reputation and route packets along a more reputed path by avoiding these malicious nodes. However, the number of packets dropped by BC−AODV is not zero, because the path chosen by (6) trades-off the number of hops to the destination and the cumulative reputation of the nodes along the path. The packet loss can be further reduced by selecting a smaller α, and giving dominance to the *reputation cost* over the number of hops in (5). The average reduction in the packet drop rate in BC−AODV over AODV is $\approx 12\%$.

V. Related Work

Reputation and trust-based methods have been employed to enhance the security and reliability of routing protocols [15]. A routing metric aimed at mitigating the effects of certain routing attacks, based on estimation of trustworthiness of neighbours was introduced in [16] and implemented in [10]. However, such reputation based systems require a method for global detection and dissemination of malicious behaviour and consensus of trust-less nodes. A fraction of nodes serving as miners and the distributed consensus via blockchain serve as an attractive solution for such challenges. Blockchains have been of interest in reputation dissemination and routing. The distributed management of trust and reward in [17] relies on cooperative mining of trusted miners. Trust in BGP routing is addressed by proposing a blockchain-based [18] and smart contract based [19] secure routing scheme. These approaches introduce radically different routing techniques that requires changes in the protocol and standard design, before widespread use. In contrast, we propose the use of blockchain technology to disseminate assess and account for misbehaviour during the routing among mobile, trustless entities.

VI. Conclusion

We proposed a shortest, most reputed path routing scheme called BC−AODV, based on the reputation information disseminated via a blockchain. The novel heterogeneous difficulty assignment of miners in each grid and the use of the blockchain to capture the behaviour of nodes, provides a credible, fast and tamper-proof means to arrive at distributed consensus on the reputation of nodes, among trustless entities in MANETs. We showed how the reputation of nodes is used to modifiy the cost metric of AODV to improve the reliability of the route selection, by showing the robustness against threats such as black hole and grey hole attacks. Rigorous simulations show the effectiveness of the proposed solution with regard to the routing performance among trustless entities.

References

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, Feb 2004.

[2] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth International Conference on Computational Intelligence and Security*, Dec 2013, pp. 663–667.

[3] S. Puri and V. Arora, "Routing protocols in manet: A survey," *International Journal of Computer Applications*, vol. 96, pp. 7–12, 06 2014.

[4] D. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2014.

[5] T. L. Foundation, "Hyperledger," cited July 09. [Online]. Available: https://www.hyperledger.org/

[6] V. Buterin, "A next generation smart contract & decentralized application platform," 2015.

[7] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *25th ISSC 2014/CIICT 2014*, June 2014, pp. 280–285.

[8] D. Meshkov, A. Chepurnoy, and M. Jansen, "Revisiting difficulty control for blockchain systems," *IACR Cryptology ePrint Archive*, vol. 2017, p. 731, 2017.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf."

[10] L. Guillaume, J. van de Sype, L. Schumacher, G. Di Stasi, and R. Canonico, "Adding reputation extensions to aodv-uu," in *2010 17th IEEE SCVT2010*, Nov 2010, pp. 1–6.

[11] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," ser. MobiCom '00. New York, NY, USA: ACM, 2000, pp. 255–265.

[13] Ethereum, "Ethereum wire protocol (eth)," cited July 09. [Online]. Available: https://github.com/ethereum/devp2p/blob/master/caps/eth.md

[14] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, Nov 2001, pp. 14–23.

[15] M. M. Azza and S. B. Hacene, "An enhanced reputation-based for detecting misbehaving nodes in manet," 2017.

[16] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, Nov 2008, pp. 1–5.

[17] S. Goka and H. Shigeno, "Distributed management system for trust and reward in mobile ad hoc networks," in *2018 15th IEEE CCNC*, Jan 2018, pp. 1–6.

[18] M. Saad and M. Yuksel, "Routechain : Towards blockchain-based secure and efficient bgp routing," 2019.

[19] Q. Xing, B. Wang, and X. Wang, "Bgpcoin: Blockchain-based internet number resource authority and bgp security solution," *Symmetry*, vol. 10, no. 9, 2018.