AODV-Miner : Routage par Consensus Basé sur la Réputation

Edward Staddon, Valeria Loscrì, Nathalie Mitton

AODV-Miner : Routage par Consensus Basé sur la Réputation

Edward Staddon[1], Valeria Loscri[1] et Nathalie Mitton[1]

[1] *Inria, 40 Avenue Halley, 59650 Villeneuve-d'Ascq, France*

Avec le déploiement de l'Internet des Objets (IoT), la sécurisation de leurs communications est une tâche importante. Dans les réseaux sans-fil multi-sauts, les différents nœuds doivent faire confiance de manière inconditionnelle à leurs voisins pendant le processus de routage. Cependant, ceci est souvent à leurs dépens puisque des nœuds malicieux peuvent infiltrer le réseau et, en conséquence, semer le chaos lors du routage. Pour y faire face, nous permettons aux différents nœuds la possibilité d'évaluer le comportement de leurs voisins via une méthode de consensus inspiré du Blockchain. Ainsi ils peuvent convenir de la crédibilité de tous les nœuds du réseau de manière distribuée. Cette métrique est exprimée par la réputation des nœuds, permettant ainsi aux autres d'identifier rapidement leur fiabilité et, dans le cas d'un nœud malicieux, l'isoler des opérations du réseau. En intégrant cette méthode dans un protocole de routage multi-saut tel que AODV, nous pouvons influencer le choix de la route, non plus fondé sur sa longueur à partir du plus petit nombre de sauts, mais sur la meilleure réputation possible. Des simulations de cette approche ont montré une baisse d'environ 48% du nombre de paquets jetés dans un contexte statique quand le réseau est soumis à de multiples attaques de type "black hole", comparé au protocole de routage AODV original.

Mots-clefs : IoT, AODV, Blockchain, Consensus, Réputation, Cybersécurité

1 Introduction

Wireless Internet of Things (IoT) based networks are becoming more and more prominent in various areas. With this development, the protection of communications is paramount, especially when used in important systems, such as wearable healthcare devices. When using the multi-hop paradigm, routing activities are a prime target for attack, throwing the network into chaos if performed efficiently. To combat this risk, we propose a new routing protocol based upon the Ad hoc On-Demand Distance Vector (AODV) routing protocol called *AODV-Miner*. By integrating reputation metrics with a consensus-based validation system using blockchain dissemination, we can determine the most trustworthy route, avoiding malicious entities, increasing network efficiency by $\approx 48\%$.

The use of reputation metrics is not new and have been analysed in conjunction with AODV in the past [GvdSS+10]. Furthermore, blockchain use in routing has also been analysed and solutions using its qualities have been proposed also [MDB17]. In our situation, we base our study on the solution proposed in [CD20], extending their work to include new updated metrics, such as an updated *link cost* metric as well as the notion of *reputation decay*. Furthermore, an improved consensus-based validation system associated with a lightweight blockchain implementation alleviates the intensive computations associated with Proof-of-Work. Finally, a dynamic role selection allows nodes to determine their own role at will, making them either a "router" or "miner", carrying out the consensus-based validation.

2 System Model

Network Model: We consider a connected wireless network scenario with N nodes with a fixed transmission range. All nodes are aware of all traffic on the wireless medium in proximity to them at all times. They also possess the ability to determine their own role for a specific route, making them either a router or validation miner. Determined during route discovery, their role is valid for the duration of the route, with

priority given to routing over mining. As such, a received RREP specifies the node as a router, whereas overhearing an RREP identifies potential miners. Subsequently, nodes can participate simultaneously in multiple routes, thus taking on multiple roles.

Validation Model: The role of validation miners is 1) to "mine a route", validating routing behaviour; and 2) to "mine a block", confirming and distributing results through the blockchain. Captured RREP packets allow the construction of forwards and reverse *Route Validation Tables* (*RVTs*), allowing the identification of anomalies during routing. Each action is subsequently categorised as either *good* or *bad* and associated with the transmitting node for that route. When the route expires, the miners share a temporary block containing all *good* and *bad* actions with neighbouring nodes. With our consensus-based validation, we assure only confirmed blocks are disseminated throughout the network using our lightweight blockchain system. By comparing received blocks with their own, miners can determine if they are valid or not, in which case they transmit their own block instead. If no response is received, a miner considers its work to be valid, inserting it into the blockchain.

Threat Model: We concern ourselves with routing based attacks, where a malicious node can drop, destroy or re-route any or all passing packets, impacting network efficiency [SLM21]. In particular, we consider *black holes* as the target of our analysis, where all passing packets are immediately dropped.

3 AODV-Miner

3.1 Node Reputation

A nodes reputation depends on their previous activities in the network. If a node acts as expected (i.e. correct hop), it has performed a *good* action, where any deviation is considered malicious and *bad*.

$$R_n = \frac{1}{1 + e^{-\delta_n}} \quad (1) \qquad \delta_n = \beta \times \frac{S_{good_n} - \alpha \times S_{bad_n}}{S_{good_n} + \alpha \times S_{bad_n}} \quad (2)$$

By keeping a record of all *good* and *bad* actions, we can calculate the overall reputation $R_n \in [0,\ 1]$ of node n as shown in (1) which uses a sigmoid function $\delta_n \in [-1.1]$. This sigmoid function can be calculated as shown in (2), where S_{good_n} and S_{bad_n} correspond to the sum of the previous W_n actions, with $\beta = 8$ the sensitivity factor as in [CD20] and α the weight of malicious activities. By varying W_n and α, we can influence the amount of history taken into account as well as defining the impact of *bad* actions, increasing or decreasing the corresponding punishment.

We also propose an update to the *link cost* metric from [CD20] which replaces AODV's hop count field, corresponding to the "cost" of using a certain node.

$$C_n = \lfloor (1 - R_{n_t}) \times (C_{max} - (C_{min} - 1)) + C_{min} \rfloor \quad (3) \qquad C_{max} = \frac{255}{L_{max}} - 1 + C_{min} \quad (4)$$

This cost is directly related to the node's reputation as shown in (3), assigning a higher cost C_n the lower the reputation R_{n_t} at time t. Since R_{n_t} is normalised between 0 and 1, we scale the result based upon the maximum possible value C_{max} as determined in (4) with a minimum value of $C_{min} = 1$. By associating the scaling function to the number of nodes in the network L_{max}, the precision of the *link cost* metric can be increased the fewer nodes are present (i.e. $C_{max} = 8$ with $L_{max} = 32 \mid 4$ with $L_{max} = 64$ (default)). Furthermore, this scaling can be integrated into AODV by associating L_{max} to the `NET_DIAMETER` configuration variable.

We then propose a new metric which allows a nodes reputation to decay overtime towards a neutral value of 0.5 if it hasn't been used for a certain duration. This allows nodes to be given a second chance, thus allowing the reintegration of sanitised nodes.

$$Rd_{n_t} = (t - t_{R_n}) \times (\frac{\lambda}{t_{\frac{1}{2}R}}) \quad (5) \qquad R_{n_t} = R_n - Rd_{n_t} \quad (6)$$

Rd_{n_t} (5) corresponds to the decay value of n at time t based upon the decay factor λ and the half life of the reputation $t_{\frac{1}{2}R}$. The final reputation is represented as R_{n_t} (6) and is the value used for all reputation based calculations, such as (3). Our system uses a liner decay function with $\lambda = 0.25$, resulting in a return to neutral after $2 \times t_{\frac{1}{2}R}$ where $t_{\frac{1}{2}R} = 15\ min$.

3.2 RREP-2Hop

To create their *RVTs*, miners need information from passing RREPs. However, this information is limited, only pertaining to the two nodes in the exchange. As a result, a miner cannot validate the activity of the RREPs transmitter since its next expected hop is unknown. We propose an update to the RREP packet format called *RREP-2Hop* (Fig. 1), where we append the address of the transmitters next hop to the standard RREP. As such, miners can now extrapolate the RREP transmitter's next hop, thus allowing its activities to be validated. To allow seeming-less integration, we have also included a miner flag, allowing parsers to determine which version of RREP is used. Furthermore, we allow the incorporation of both MAC and IP addresses, the former of which is needed by the miners and the latter to construct 2-hop routing table entries if required.

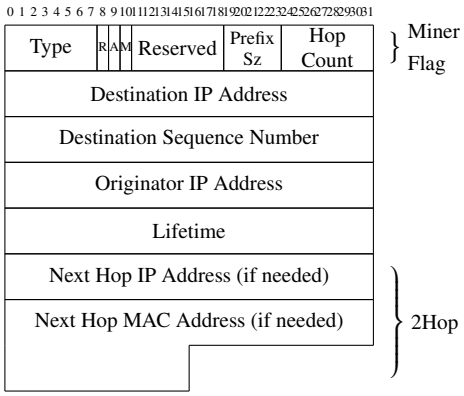


FIGURE 1: RREP-2Hop packet structure

3.3 Behavioural Validation

By using their *RVTs*, miners are capable of validating routing activities. For each routed packet, the miners capture and analyse the transmitted message, determining if its hop is correct and storing its hash. This continues until the route expires, at which time the packet hash buffer is analysed to determine if packets have been dropped, before beginning the blockchain dissemination phase. The nodes prepare their blocks by aggregating their computed actions and transmit them with $TTL = 2$ to all neighbouring nodes, thus only reaching miners for the same portion of route. When receiving a block, the miners first confirm the contents with their own block before determining the efficiency factor, making sure only the most efficient blocks are inserted. This factor corresponds the the percentage of nodes in common in the received block as well as the miners own. If this value is higher for the miners block, then the received block is considered more efficient as it contains more nodes overall, in which case nothing is done. However, if the received block is less efficient, or contains incorrect activities, then the miner transmits its own block, overruling the previous one. If no blocks are received after a certain duration, the last block is considered valid, and its owner inserts it into the blockchain.

4 Results

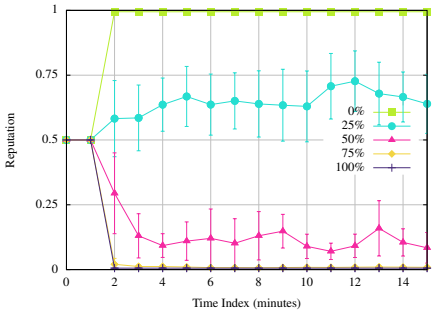
AODV-Miner was implemented and tested using Contiki-NG †'s Cooja simulator with 30 nodes in a $150m \times 150m$ area with a transmissions range of $50m$. Our preliminary analysis pitches *AODV-Miner* against its older brother AODV, in a network where malicious *black holes* are distributed at random.

Fig. 2a shows the calculated reputation based on malicious activities with $\alpha = 2$ (default). We can see that the higher the malicious activity, the lower the overall reputation. Also, the reputation is determined after the first exchange, around the one minute mark, generally remaining stable thereafter.

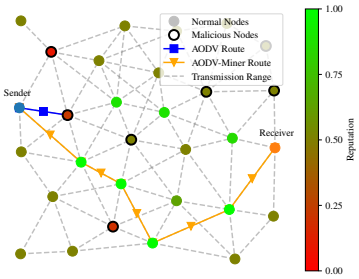
Fig. 2b presents the status of a network of 30 nodes after 15 min. with 25% of nodes being black holes (thick circled), with node reputation and most used routes superimposed. Contrary to AODV which uses the shortest most direct route via a malicious node, *AODV-Miner* can determine a free trustworthy route. We can see that in this scenario, our system has identified three malicious nodes, giving them a bad reputation, whereas all others used have received good reputations, identifying multiple routes to the receiver.

Fig. 3 compares the efficiency of *AODV-Miner* to AODV. We use the number of packets dropped ($|Sent| - |Received|$) to determine the overall network throughput. Fig. 3a and 3b present these two analyses respectively. We can see a significant decrease of $\approx 48\%$ in packets dropped with 10% malicious nodes, which is confirmed with a higher overall throughput, whatever the proportion of malicious nodes in the network. It is to be noted that not all drops are prevented since malicious actions must occur for the reputation to be calculated. It is also possible that using a bad node has an overall lower cost than multiple

†. https://github.com/contiki-ng/contiki-ng

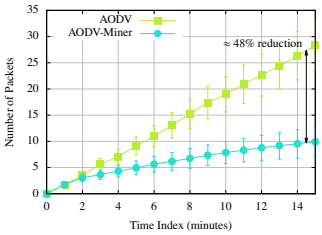


(A) Reputation overtime with varying malicious activity

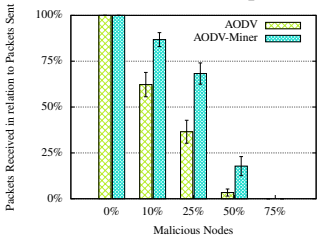


(B) Route reputation after 15 min with 25% malicious nodes.

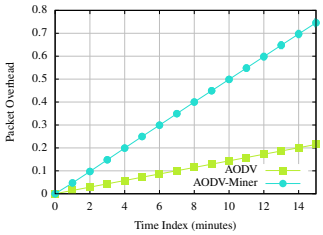
FIGURE 2: Network Reputation



(A) Packets dropped with 10% malicious nodes



(B) Throughput with varying presence of malicious nodes



(C) Normalised overhead with 10% malicious nodes

FIGURE 3: Routing efficiency between *AODV-Miner* and AODV in the presence of malicious nodes

good nodes (i.e. 1 node with *link cost* of 4 is cheaper than 5 nodes with *link cost* of 1). This higher efficiency comes at a high cost, that of increased network transmissions as confirmed in Fig. 3c, where *AODV-Miner*'s overhead is significantly higher than AODV's in this preliminary analysis.

5 Conclusion

Our analysis shows *AODV-Miner* is capable of reducing the number of packets dropped from black hole attacks by determining the most trustworthy route available. By using reputation metrics, nodes are rewarded or punished based upon their previous actions in the network, allowing *good* nodes to be used again and *bad* nodes to be avoided. Thanks to blockchain technology, the resulting reputation can be disseminated throughout the network to be used to calculate node *link costs*. Furthermore, with the addition of a new RREP packet format, we allow miners to recover more information from the network, thus confirming the activities of all neighbouring nodes. To complete our analysis, our next step is to increase the network size and complexity, as well as use different threats such as grey holes in our analysis to evaluate the efficiency of our system in multiple new scenarios. Finally, the overhead also needs to be analysed and a more efficient blockchain distribution system proposed to combat the increase.

This work was supported by CPER DATA and H2020 Project CyberSANE.

References

[CD20] M. A. A. Careem and A. Dutta. Reputation based routing in MANET using Blockchain. In *Int. Conference on COMmunication Systems NETworkS (COMSNETS)*, 2020.

[GvdSS+10] L. Guillaume, J. van de Sype, L. Schumacher, G. Di Stasi, and R. Canonico. Adding reputation extensions to aodv-uu. In *IEEE Symp. on Comm. and Vehicular Technology in the Benelux (SCVT)*, 2010.

[MDB17] A. Moinet, B. Darties, and J.-L. Baril. Blockchain based trust & authentication for decentralized sensor networks. *ArXiv*, abs/1706.01730, 2017.

[SLM21] E. Staddon, V. Loscri, and N. Mitton. Attack categorisation for iot applications in critical infrastructures, a survey. *Applied Sciences*, 11(16), 2021.