An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs

John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy

An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs

John Tobin, Christina Thorpe, Damien Magoni, Liam Murphy
University College Dublin, Dublin, Ireland
john.tobin.1@ucdconnect.ie
christina.thorpe@ucd.ie
damien.magoni@ucd.ie
liam.murphy@ucd.ie

Abstract: Inter-vehicular communication is a growing trend among the motor vehicle industry, as part of the shift to the Intelligent Transportation System (ITS) paradigm and the emergence of autonomous vehicles. The benefits of using vehicular communication systems are many: traffic congestion can be abated leading to increased route efficiency and fuel economy; road traffic accidents and fatalities can be prevented; and new services are made available to both driver and passengers. Due to the important functions carried out by these networks, it is essential that communication is secure and free from interference by malicious parties. But the very nature of these networks (i.e. public and dynamically forming, over a shared medium) make them susceptible to certain attack vectors. Black hole attacks are a discernible threat to vehicular communication and the availability of Vehicular Ad Hoc Networks (VANETs). Previously, we proposed a solution to mitigate these attacks in the case of a single malicious node. This countermeasure comprised a detection, accusation, and blacklisting scheme. We now extend that work to also account for cases where multiple malicious nodes are present in the same network. For cases where there is only one malicious node on multiple routes, we add a recursive element to our algorithm to handle additional detections during the accusation phase. Routes containing a node with a pending accusation are also precluded from selection. Where multiple malicious nodes exist on the same route, we adapt our former strategy to allow for multiple concurrent accusations and to find alternate routes to non-malicious nodes that need to be queried when verifying an accusation. We provide validation for our proposal using a simulation model built in NS-3. Results from simulation show the efficacy of our solution in detecting and preventing multiple malicious node black hole attacks in VANETs.

Keywords: black hole attack, vehicular networks, denial of service, network security, VANET.

1. Introduction

Intelligent Transportation Systems are on the rise and offer a plethora of benefits to users. Improved road utilisation, efficiency and safety are among the top advantages. VANETs are wireless networks that facilitate inter-vehicular communication. VANETs play a substantial role in ITS by propagating traffic and important safety information to nodes. For example, if there is a road traffic accident ahead which is blocking off a road, nodes in the VANET will alerted to this prior to reaching the scene of the incident. Nodes can then divert and avoid a traffic build-up around the accident. A more recent safety application (with the potential to save lives) is the electronic brake light system (Biswas, et al., 2006). Such systems transmit braking information to nearby nodes within a VANET and alert drivers to when other vehicles apply their brakes, which is particularly useful as brake lights can often be obscured by other vehicles. However, more advanced and integrated versions of this technology provide an even greater advantage: they can have the vehicle automatically apply the brakes in response to receiving a message, and sensing, that another vehicle directly ahead has suddenly applied their brakes (e.g. due to an obstacle on the road). The ability to react in this case is quicker than that of the human driver and may prevent a road traffic incident from occurring. VANETs can additionally provide multimedia content, communication and messaging services, and automobile internet access. Due to the importance of some of these applications, and particularly with the emergence of autonomous vehicles, the security of VANETs is a paramount safety consideration.

VANETs are a close relative of the Mobile Ad-Hoc Network (MANET) but differences in node mobility and a rapidly-changing topology distinguish them. Furthermore, VANETs are formed spontaneously and often have a short lifespan. Mobile nodes (i.e. vehicles) are the primary consumer of a VANET but networks may be supported by fixed infrastructure known as Road Side Units (RSUs). Nodes that wish to communicate with another node in the network may do so by routing through nodes to reach their destination, if not directly in range. Many routing protocols exist, however, in this paper we will focus on Ad hoc On-Demand Distance Vector Routing (AODV) (Perkins, et al., 2003) which is one of the most commonly used.

Attacks on availability are of considerable concern to VANETs – particularly as reliance on applications requiring intervehicular communication increases. In this paper, we focus on the black hole attack. In this attack, a node falsely advertises itself as having the shortest route to a destination. After this route is selected, the node should relay packets from the source to the next hop on the route, but instead maliciously drops these packets thereby preventing communication between the source and destination nodes.

We have previously proposed a countermeasure to this attack for instances where there is a single malicious node present in a network. We consider the single malicious node scenario to be the base case of this problem and our work is intended to be incremental, gradually increasing the scope of detection and prevention afforded by our countermeasure. This paper proposes two new algorithms to extend our countermeasure to be able to detect and prevent against black hole attacks with multiple malicious nodes. We validate the efficacy of these new algorithms and our revised countermeasure with simulations of the attack and an implementation of our solution in Network Simulator-3 (NS-3) (Riley & Henderson, 2010). Accurate detection and effective prevention of black hole attacks with our countermeasure is demonstrated in the results of these simulations. The use of our solution led to a corresponding increase in network performance against non-use in scenarios where a black hole attack was present.

This paper is structured hereinafter as follows: Section 2 discusses related work from the literature. In Section 3, we outline the concept behind a black hole attack and show how this attack is performed in practice. Section 4 concerns our proposed countermeasure to mitigate the threat posed by black hole attacks on VANETs. We first detail our previous work in this area, a solution to single malicious node black hole attacks. We then propose two new algorithms to expand the scope of this solution to detect and prevent against multiple malicious node black hole attacks. In Section 5, simulations undertaken and their parameters are described, while the results from these simulations are discussed in Section 6. Finally, Section 7 concludes the paper.

2. Related Work

A black hole attack is an attack vector that poses a threat across a wide range of disciplines and is not unique to the vehicular networking domain. MANETs, the parent network from which the VANET emerged, are particularly sensitive to this type of attack and much of the work regarding detection of prevention of these attacks has been focused in the MANET domain. Different approaches to countering this attack vector have been proposed, with reputation-based schemes among the most common. The use of collaborate Bayesian watchdogs (Serrat-Olmos, et al., 2012), where each node monitors their neighbours' behaviour and assigns reputation values accordingly, yields accurate attack detection but at the expense of significant overhead from message passing and packet transmission monitoring of all neighbouring nodes. Fidelity tables, where each node essentially has a reliability level, have been used with some success (Tamilselvan & Sankaranarayanan, 2008). Here, when a node acts unreliably (e.g. no ACK is received) its fidelity level is decremented. When ACKs are received, it's fidelity level is incremented. When a node's fidelity level reaches 0 it is deemed to be a malicious node and is excluded from the network. This solution can counter multiple malicious node attacks but results show that its effectiveness is considerably reduced with increasing node speed, making it unsuitable for VANETs.

A number of efforts at mitigating black hole attacks have focused on the routing protocol itself as a means of preventing this attack. New protocols have been developed with this in mind, however, due to the prevalence of AODV, few have been adopted for use. Secure AODV (SAODV) is an extension of AODV proposed due to the lack of security offered at the routing layer (Zapata, 2002). It employs cryptographic means to offer security features (e.g. authentication) that AODV lacks. While not the author's intention, it indirectly offers limited protection against black hole attacks as a malicious node can only lie about itself and reduce the hop count in an RREP by one. However, this is the extent of its protection against this attack vector. Other protocols extending AODV have been designed specifically to offer protection against black hole attacks. One such protocol by Khamayseh, et al., (2011) modifies the AODV protocol to have each node maintain a trust table holding the addresses of reliable nodes. For a node to be added to another node's trust table, it must pass a behavioural analysis filter which considers link parameters of the other node's active connections and other historic information that nodes must store. This modification yielded a 13 – 15% increase in Packet Delivery Ratio (PDR) for single and multiple malicious node attacks. However, the modified protocol lacks a means to

remove a malicious node from a network and raises questions regarding the overhead incurred by nodes from having to store historic network data on its neighbours.

Intrusion detection systems have been adopted to tackle the problem of black hole attacks in MANETs. Alem & Xuan (2010) used anomaly detection to develop an effective solution capable of detecting malicious nodes and preventing the attack thereafter. This particular scheme can be used with any number of malicious nodes and has a low network overhead between nodes. The disadvantage of this countermeasure is that each node protects only itself. Furthermore, a centralised node monitoring traffic flows is required, thus making such a solution impractical for use in a VANET.

Mishra, et al., (2013) propose using Data Routing Information (DRI) tables (which store information on packet forwarding by neighbouring nodes) in conjunction with probe packets to determine if a node is malicious. Another cooperative node, for acknowledging the probe packets, is required. Simulation results for this strategy show meaningful network performance improvements and that multiple malicious node attacks can be aptly detected. The authors do not reference the overhead incurred by such a solution, however, but do acknowledge that detection of malicious nodes remains a challenge.

3. Black Hole Attack

A black hole attack is an attack on availability and a type of Denial-of-Service (DoS) attack. In this attack, a malicious node fraudulently advertises itself as having the shortest route to a source node requesting a route to its destination. Then, after the source selects this route for use, the malicious node drops all data packets it receives, instead of relaying these to the next hop in the route. No message alteration or inspection takes place in this attack, rather, its goal is to prevent communication between nodes in a network.

We distinguish between a black hole attack and a grey hole attack. In the former, malicious nodes drop all data packets indiscriminately. In the latter, malicious nodes may selectively drop packets or discard them in line with a probability distribution. We are concerned only with black hole attacks in this paper. For scoping purposes, we assume that all honest nodes (i.e. non-malicious nodes) always act in good faith. Furthermore, we presume that there are multiple paths from a source node to its destination and vice versa. Finally, we assume that malicious nodes are always malicious and cannot change or spoof their identity to evade detection. There are practical ways in which this may be enforced, such as through Electronic Vehicle Identification (EVI) or integration of security hardware modules (e.g. Tamper Proof Hardware (TPH) and Electronic License Plates (ELP) (Al-kahtani, 2012)) into vehicles by manufacturers.

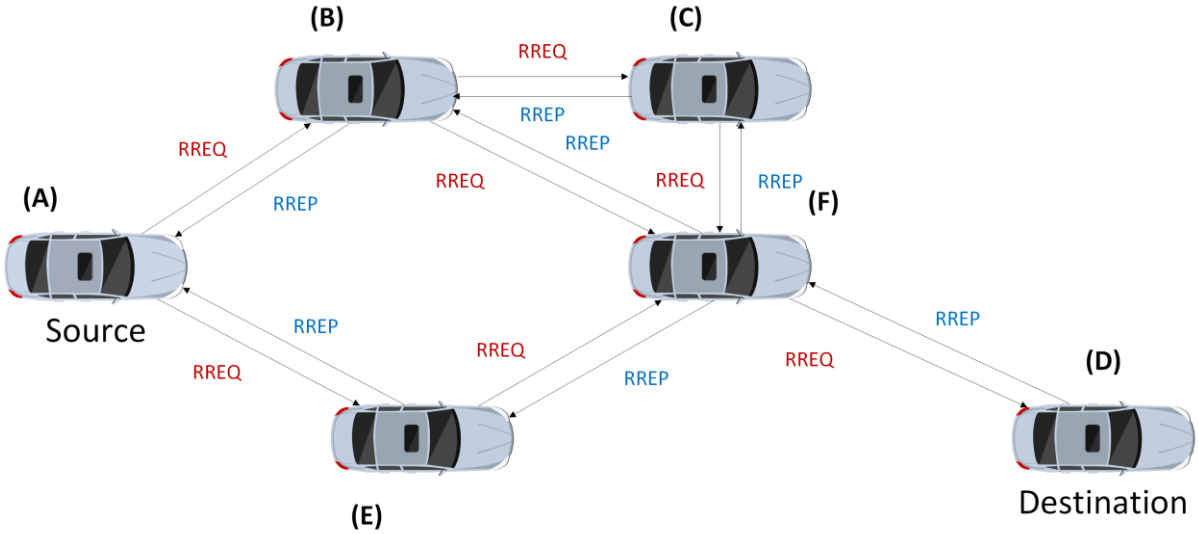

Figure 1: RREPs back propagated to the source node after an RREQ reaching the destination.

Under AODV routing, when a source node requires a route, it broadcasts a RREQ to neighbouring nodes. RREQs are propagated through the network to neighbours, as shown in Figure 1, until the destination (or a node with a valid route to the destination) is reached. A RREP is then unicast back to the source.

In a black hole attack, a malicious node endeavours to be selected as part of an active route. As such, it is advantageous for malicious nodes to advertise themselves as having the shortest route possible – that they have a direct path to the destination – in response to any RREQ received. This is irrespective of whether such a path exists between the malicious node and the destination. As the malicious node has no intention of relaying the source's packets towards the destination, it is not concerned with having a route to the destination and so the malicious node forges an RREP stating that the destination is its next hop. This RREP is then sent back to the source node, as per Figure 2.

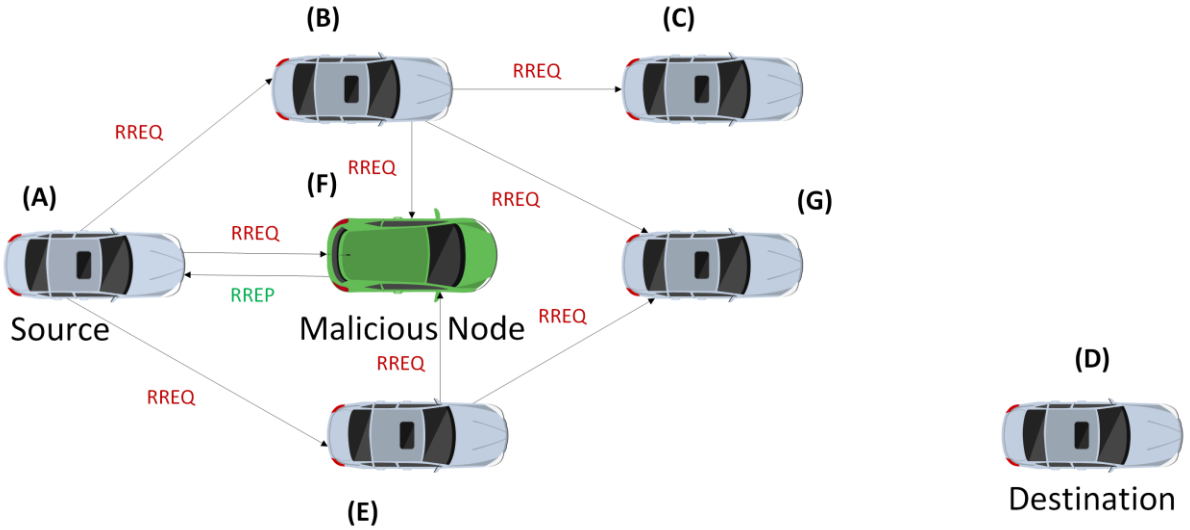

Figure 2: RREQs propagating through the VANET, however, in this case a malicious node forges an RREP stating dishonestly that it has a direct path to the destination.

It is the malicious node's hope that the source selects the false route it has replied with, as depicted in Figure 3. If so, the node starts to receive traffic to relay, which it discards – hence the name of the attack, the malicious node becomes a black hole for the source's traffic.

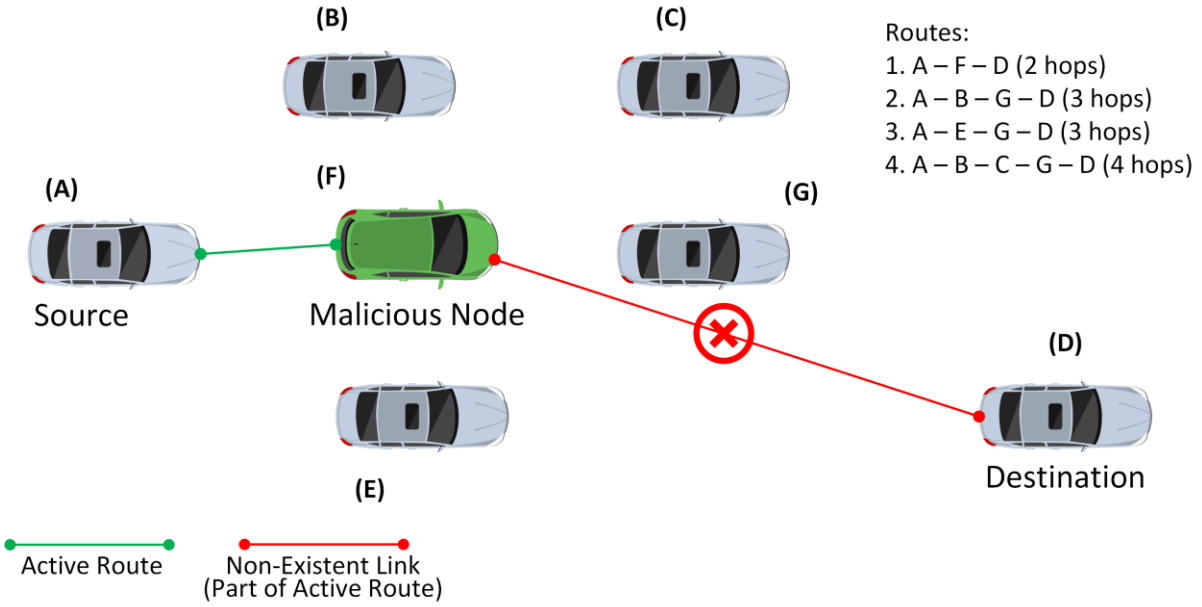

Figure 3: Active route with malicious node performing black hole attack

Variations of this attack present when more than one malicious node is introduced to the network. When multiple malicious nodes partake in a black hole attack, they do so independently. If these nodes were to act in concert, it would constitute a grey hole attack instead. We have identified two scenarios in which multiple malicious nodes may organise themselves (and which require different strategies to counter).

3.1 One Malicious Node per Route on Multiple Routes

In the first of the identified scenarios, the malicious nodes are organised such that there is only a single malicious node on any given route. As there are multiple malicious nodes present in the network in this instance, multiple routes will likely have a malicious node as a hop. This is akin to the single malicious node case of a black hole attack, albeit with multiple occurrences thereof within a single network. Figure 4 depicts this scenario.

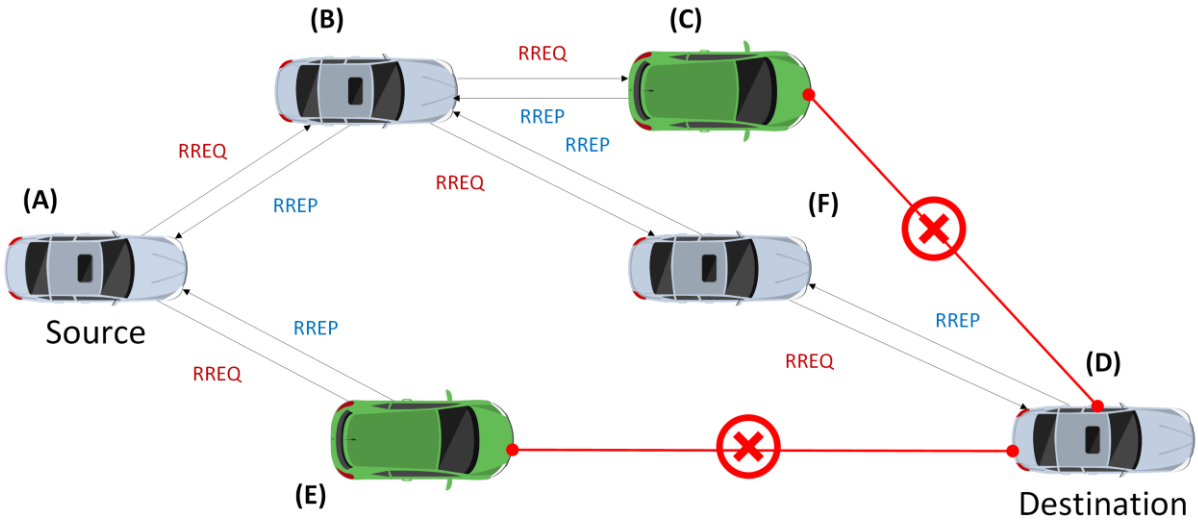

Figure 4: Two Malicious Nodes, (C) and (E), Performing a Black Hole Attack on Separate Routes (One Malicious Node per Route)

3.2 Multiple Malicious Nodes on Single Route

A more complex scenario occurs when multiple malicious nodes exist on a single route. Should two nodes independently of each other seek out a route to their counterpart, and two or more malicious nodes separate them, then it is probable that each will fall victim to a black hole attack perpetrated by a different malicious node to the other. Accordingly, both will be presented a different, non-existent, route by the respective malicious node. This makes detection of the black hole attack markedly more difficult for our countermeasure. This is due to each endpoint of the route initiating detection procedures on a different malicious node, and consensus requirements in blacklisting. A visual representation of this scenario is given in Figure 5.

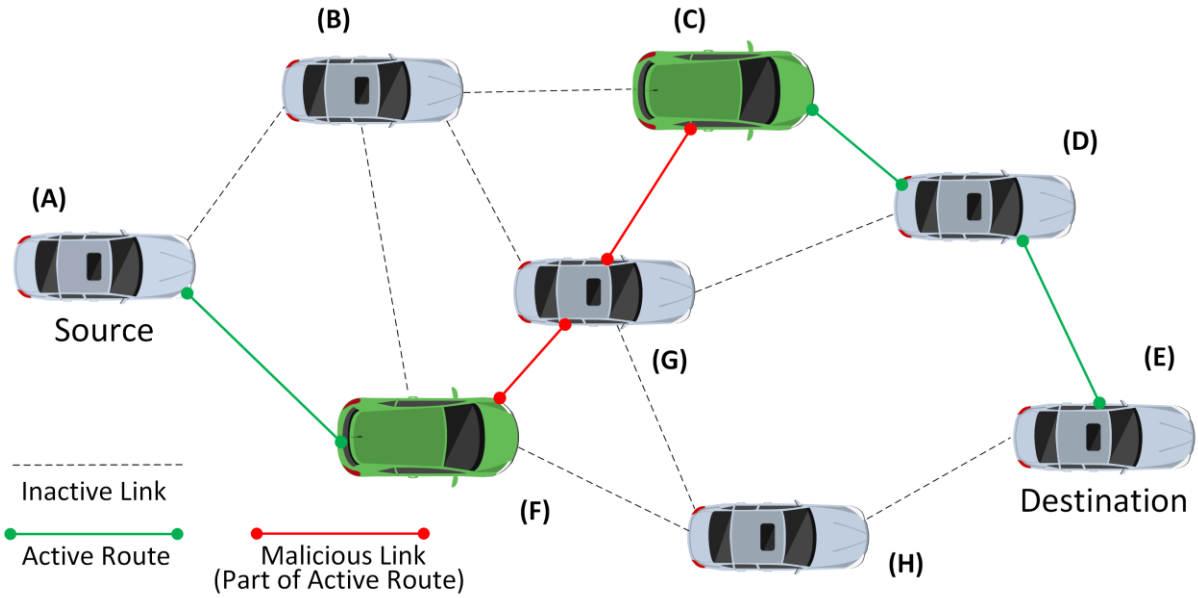

Figure 5: Two Malicious Nodes, (C) and (F), Performing Black Hole Attack on a Single Route (A-F-G-C-D-E)

4. Proposed Countermeasure

Previously, we proposed a solution to prevent single malicious node black hole attacks (Tobin, et al., 2017). We consider this to be the base case for such an attack. Now, we propose two new algorithms that build upon our previous solution to expand its scope. This incremental work is intended to detect and prevent against black hole attacks in cases of both a single malicious node and multiple malicious nodes present in the network. This Section begins by discussing our previous work on this countermeasure and then goes on to propose two new algorithms for black hole attacks with multiple malicious nodes.

4.1 Previous Work – Single Malicious Node Attacks

Our prior work serves as the foundation for our countermeasure. It solely mitigates the threat of black hole attacks with a single malicious node. Our solution takes a 3-step approach to detecting malicious nodes and preventing the attack by removal of such nodes from participation in the network. These steps consist of: attack detection, node accusation, and malicious node blacklisting. Once an attack is detected, and the offending node isolated, measures are taken to prevent the node from causing further disruption or joining other networks. Part of this countermeasure requires that nodes can digitally sign (and can verify a digital signature). All nodes should support asymmetric cryptography and possess a public-private key pair to fulfil this requirement. The OpenPGP standard (Callas, et al., 2007) is proposed for this purpose.

4.1.1 Attack Detection

Attack detection is complicated by the inherently lossy nature of the shared wireless medium of VANETs. Indiscriminate public user access and rapidly changing network topologies further compound this. Typically, when network connectivity is lost or a link goes down, an intermediate node along a route will detect this (as all nodes periodically monitor neighbouring link status). Upon detection, the node will transmit a Route Error (RERR) message back along the route, informing nodes that the route is no longer valid. This is how nodes become aware of a problem with packet transmission, particularly with stateless protocols such as UDP. Unfortunately, this is not the case when a network is subjected to a black hole attack. As nodes do not lose the link to the malicious node, the routing protocol offers no assistance in detecting packet non-delivery.

Under AODV, nodes do not know the full composition of a route. Instead, any node with a route to a particular destination has knowledge only of the next hop and the number of hops. This hinders attack detection. Thus, to facilitate attack detection we modify the RREP message format to have intermediary nodes append their hop number and IP address to any RREP received and being relayed. This adds minimal overhead to routing protocol messaging. A standard RREP is 160 bits. Our modified RREP, for any given hop in a route, has a size of 160 + 40n bits, where n is a given node's hop number. Considering the throughput of modern IEEE 802.11 standards and typical number of hops in a VANET route, we conclude that this overhead is negligible.

We propose a malicious node detection scheme based on route backtracking and querying of intermediate nodes for statistics to determine the malicious node. This is achieved by analysing statistics (e.g. packets sent/received) for each node and finding the node causing the discrepancy, thus revealing the malicious node. There are many suitable network statistics for this purpose, however, our experiments have shown the packets sent and received counter to be a reliable indicator for malicious node detection, consistently yielding good results. In our implementation, the triggering node will query the next hop (and so on) for the number of packets it received from its previous hop and the number of packets it relayed to its next hop. Should the node fail to reply to such a request, the node is flagged as potentially malicious. This attack detection step is triggered by a source or destination node noticing a lack of expected replies (or missing ACKs) with no reported link lossage (e.g. no RERR received). Application layer services may be involved in triggering this step.

If a node is flagged, and a discrepancy is not large enough to support an accusation, the triggering node proceeds to alert its counterpart (e.g. the destination node if the source is the triggering node) to begin attack detection using an alert message that is sent on an alternate route without the flagged node or its previous hop. The alert message contains details of the active route, the alternate route, and the IP addresses of the flagged node and the previous hop in the active route. Where there is no alternate route excluding both of these nodes, the triggering node attempts to send the alert on alternate routes excluding one of these nodes, using a timeout before proceeding to the next possible route. The alert must be acknowledged by the other

party and as a result, if one alternate route fails to receive an alert ACK, this can infer that the flagged node on this route is the malicious node and support an accusation thereof.

Upon receiving an alert message, the counterpart node begins attack detection in the same manner as the triggering node. After reaching and querying the flagged node, if there is still no reply from this node then the counterpart moves to accuse this node. Should this node reply, this suggests that it is in fact the next hop that is the malicious node (the 'previous hop' in the alert message). This can be confirmed by querying the next hop and failing to receive a reply, which triggers node accusation. If both nodes reply, the counterpart node looks for a discrepancy in the statistics received to derive which is the malicious node. Failing that, the counterpart continues backtracking along the route. If the triggering node is reached, attack detection is dropped by both parties as this indicates no black hole attack along the route.

4.1.2 Node Accusation

Node accusation is ordinarily started by the node receiving an alert message, though either source or destination may accuse a node along its route following attack detection. Accusation involves sending an accusation message to the other party on an alternate route excluding the accused node. An accusation message contains details of the active route, the IP address of the accused node and its previous hop, and packet statistics as reported by both these nodes for verification. This message also requires acknowledgement.

On receipt of an accusation message, the receiving node moves immediately to querying the accused node and the other node included in the accusation message. With the packet statistics from the other end of the route in addition to the statistics it received from its own query, the receiving node now determines if the accused node is acting maliciously or not. If the receiving node concurs and upholds the accusation, the receiving node moves to blacklist the accused. Without concurrence by both parties, the accusation is dropped thus terminating the countermeasure process.

4.1.3 Malicious Node Blacklisting

A blockchain (Nakamoto, 2008) is used as the distributed public ledger maintaining all blacklist entries. As all nodes hold a copy of the blockchain, a blacklist is not limited to any short lived VANET but rather is global, applying to all VANETs. The effect of a blacklist entry is that all nodes subscribed to the blockchain will refuse to communicate with (or through) the blacklisted node, excluding it from participation in any VANET.

Blacklist entries are time-limited, set by policy, thereby allowing the possibility of node redemption. A blacklist entry consists of the offending node's unique identifier, a timestamp of when the entry was created and of when it is due to expire. In addition, the unique identifiers of source and destination nodes, their public keys, and a digital signature on the blacklist entry by each node are also included.

4.2 New Algorithms Proposed – Multiple Malicious Node Attacks

Having examined the literature to identify black hole attack adaptations with multiple malicious nodes, it appears only two true variations of multiple malicious node black hole attacks exist. Other proposed instances of this attack that are of a co-operative or selective nature instead fall under the remit of grey hole attacks, despite erroneous labelling as black hole attacks at times. The two scenarios that are within the scope of black hole attacks for multiple malicious nodes are outlined in Sections 3.1 and 3.2.

4.2.1 Algorithm 1 – The Recursive Element

The first algorithm deals with what essentially multiple single malicious node attacks within a VANET, as described in Section 3.1. This scenario has a number of malicious nodes (at least two), however, in any given route there exists no more than one malicious node. Our previously proposed countermeasure is ill-equipped to deal with this scenario. This is because our countermeasure will hang during the sending of an alert message on an alternate route if this route is also subject to a separate black hole attack by a different malicious node. The first revision of our solution furthermore fails to trigger attack detection on the alternate route, even if it appears there is an active black hole attack.

To protect against this attack variant, we modify our previously proposed attack detection step. We amend this step such that when an alert message does not receive a reply, attack detection is triggered on the alternate route that the alert message was sent on, if necessary (e.g. no RERR received). This happens recursively if the same is true of further alternate routes. A timeout is added as it is necessary should nodes go out of range while the countermeasure executes on other routes.

4.2.2 Algorithm 2 – Multiple Detection Cooperation

In a scenario where more than one malicious node is present along a single active route, such as in Figure 5, it is likely that source and destination nodes would each detect a different malicious node. On the triggering of the detection step of our countermeasure, the source and destination nodes will detect the malicious node closest (in terms of hops) to them. This raises issues in our previous iteration of this countermeasure when it comes to the counterpart node verifying the accusation as during the backtracking algorithm, the malicious node closest to the counterpart will instead be detected as the malicious node rather than the accused node.

To resolve the issues this attack scenario presents, we must modify our attack detection and accusation verification steps. The countermeasure is modified such that when both source and destination nodes have made a detection and send the respective counterpart node an alert message or accusation message, the first received of these messages is dealt with first. If both endpoint nodes have independently made detections at this point, the counterpart node halts its execution of the countermeasure while it handles the alert or accusation message it has received. The counterpart node resumes its execution of the countermeasure on its detected potentially malicious node when finished. Furthermore, the counterpart node uses its detection (if one has separately been made by it at this stage) to its advantage in excluding this flagged node, where possible, when selecting an alternate route.

The backtracking algorithm is modified to cater for detections by the counterpart, following receipt of an alert message, of a node (or nodes) other than the flagged node. The counterpart node adds the detected potentially malicious node to a list and an alert message is sent flagging this node (for each node on the list). These other detections are handled upon completion of the current execution of the countermeasure. The alert messages being sent during the current run of the countermeasure serve to build a list of potentially malicious nodes to be handled using this countermeasure on a First In, First Out (FIFO) basis, and to allow the triggering node to best select an alternate route to its counterpart. The backtracking algorithm continues as before however detected nodes other than the flagged node are isolated and an alternate route to hops beyond any detected nodes is found. If the flagged node is found to be non-responsive when reached, the counterpart node moves to accuse the flagged node.

The accusation step is amended to use knowledge of other detections when selecting an alternate route. Where possible, an alternate route excluding nodes on the detection list will be chosen. Furthermore, in order to verify an accusation, the node receiving an accusation message is required to query the next hop after the accused node on its active route. As it can no longer be assumed that only a single malicious node is present on an active route, instances where an accusation message is sent without a prior alert message must trigger attack detection backtracking instead of directly moving to query the accused node. This is to prevent false positives caused instead by another undetected malicious node on the active route. The node verifying an accusation must also use an alternate route that excludes the node prior to the accused node on the active route in querying the accused node or its next hop. This, again, is to prevent false positive detections. Taking Figure 5 as an example, if the destination node has sent an accusation message accusing node G of being malicious, the source node querying node G through node F would result in node G being falsely verified as acting maliciously, when in fact it is nodes C and F that are malicious. By having the source node exclude node F when querying nodes G and C, this prevents the false detection of node G as a malicious node.

5. Simulation Details

VANET simulation was accomplished using Network Simulator-3 (NS-3). The different black hole attack variants previously described were implemented through various simulation scenarios. The resulting effect on network dynamicity, the attack vector, and the efficacy of our countermeasure was observed. To ensure a particular attack variant remained constant throughout a simulation and did not change due to movement of nodes, node positions were fixed and a constant mobility model installed. Some scenarios were repeated with a more

realistic mobility model installed. We intend to run further simulation scenarios modelling practical situations going forward. Control simulations with no attack (both with and without our countermeasure implemented) were also undertaken to establish a baseline. All simulations were run a minimum of ten times and results averaged over these runs. Simulation parameters are outlined in Table 1.

Table 1: Simulation Parameters

Number of Nodes	5, 10 – 50 (step: 10)
Number of Malicious Nodes	Variable
Wireless Interface & Bandwidth	802.11p at 5.9 GHz
Antenna	Omnidirectional
Transmission Range	Dynamic
Traffic Type	Constant Bit Rate (CBR)
Mobility Model	Constant Position, Constant Velocity, Random Waypoint
Node Speed	5, 10, 15, and 20 m/s
Simulation Time	300 s
Map Grids	2 (1 blank grid; 1 urban map grid)
Grid Area	1000 m x 1000 m
Runs per Simulation	10

The scenarios simulated can broadly be classified into four main groups, which we label for clarity. These scenario groups are as follows: a control scenario with no attack and no solution implemented (NA_NS); a control scenario with no attack but with our solution implemented (NA_WS); a scenario with a black hole attack performed on the network and no solution in place (WA_NS); and, a scenario with a black hole attack performed on the network and with our solution in place (WA_WS). The latter two black hole attack groups can be further subdivided into the following subgroups: a single malicious node black hole attack (BH_SN); a multiple malicious node black hole attack with one malicious node at most per route (BH_MN_1PR); and, a multiple malicious node black hole attack with multiple malicious nodes per route (BH_MN_MPR). Several metrics were recorded during simulation runs to evaluate the effectiveness of our countermeasure. These included: detection time, detection accuracy (i.e. false positives/false negatives), average throughput, and PDR.

6. Results Discussion

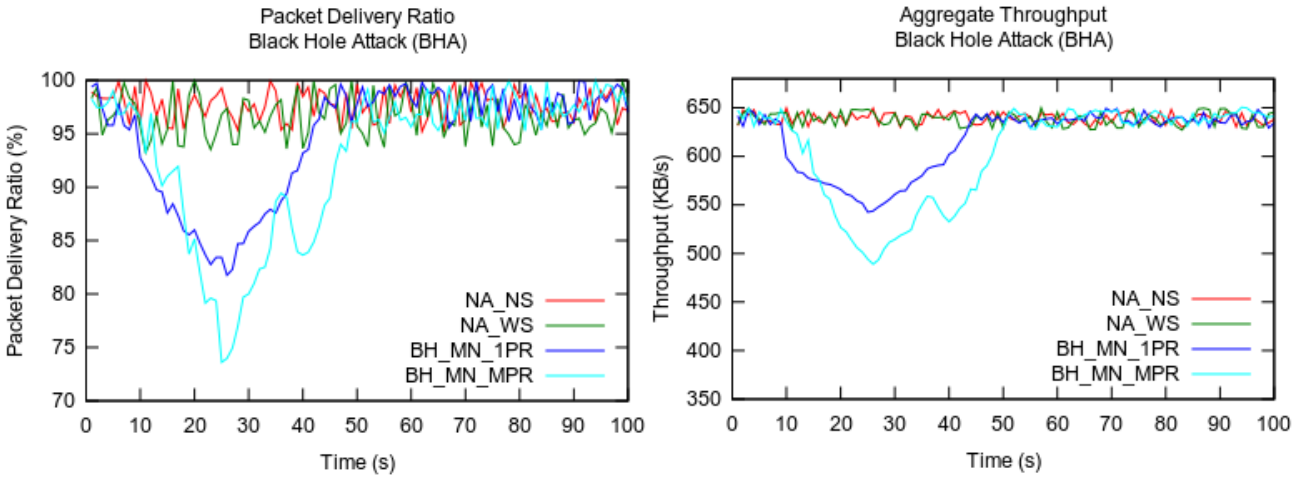

Figure 6: Packet Delivery Ratio and Aggregate Throughput for Multiple Simulation Scenarios

Figure 6 shows us the packet delivery ratio, calculated each second, for two control and two multiple malicious node black hole attack scenarios over a 100 second window. We can see that in the attack scenarios, our countermeasure begins to restore the PDR as it detects and blacklists malicious nodes from the network. Detection in the BH_MN_1PR scenario is delayed due to a range of alternate routes being subject to a black hole attack. In the BH_MN_MPR scenario, an additional dip in PDR is seen after 38 seconds as additional

malicious nodes are present on a selected alternate route. Fluctuations in PDR are attributable to nodes going out of range and retransmissions. Figure 6 also shows us the network throughput. Both attack scenarios degrade the aggregate network throughput however this is restored quickly with our countermeasure in place. There was a 0.89% false positive detection rate overall.

7. Conclusion

This paper sought to build on our previous countermeasure to single malicious node black hole attacks in vehicular wireless networks. We described two new variants of this attack where multiple malicious nodes undertake a black hole attack on a network. Furthermore, we introduced two new algorithms to expand the scope of our solution to detect and prevent against both identified scenarios. Simulation results show that this is a viable attack vector capable of effectively preventing communication between selected targets and causing a significant reduction in overall network packet delivery and throughput. As expected, the introduction of multiple malicious nodes produced a more drastic and substantial denial of service throughout the network. Implementation of our proposed algorithms to our existing countermeasure resulted in accurate attack detection and, similarly, prevention through blacklisting of malicious nodes. Network performance began to restore as blacklisting took effect. Further simulations are planned going forward with a focus on optimisation of our solution. Future work will target detection of a variety of grey hole attacks and expansion of our countermeasure to mitigate the threat of these attack vectors.

Acknowledgements

This work was supported with the financial support of the Science Foundation Ireland grant 13/RC/2094 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Irish Software Research Centre (www.lero.ie)

References

Alem, Y. F. & Xuan, Z. C., 2010. Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection. *2010 IEEE 2nd International Cdonference on Future Computer and Communication*, 21-24 May, pp. 672-676.

Al-kahtani, M. S., 2012. Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs). *2012 IEEE 6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 12-14 December, pp. 1-9.

Biswas, S., Tatchikou, R. & Dion, F., 2006. Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety. *IEEE Communications Magazine,* 44(1), pp. 74-82.

Callas, J. et al., 2007. *RFC 4880: OpenPGP Message Format,* s.l.: IETF.

Jain, A. K. & Tokekar, V., 2015. Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks. *2015 IEEE International Conference on Pervasive Computing (ICPC)*, pp. 1-6.

Khamayseh, Y., Bader, A., Mardini, W. & Yasein, M. B., 2011. A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks. *International Journal of Communication Networks and Information Security,* 3(1), pp. 36-47.

Mishra, A., Jaiswal, R. & Sharma, S., 2013. A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network. *2013 IEEE 3rd International Advance Computing Conference (IACC)*, 22-23 February, pp. 499-504.

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System,* s.l.: s.n.

Perkins, C., Belding-Royer, E. & Das, S., 2003. *RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing,* s.l.: IETF.

Riley, G. F. & Henderson, T. R., 2010. The NS-3 Network Simulator. In: *Modeling and Tools for Network Simulation.* New York: Springer, pp. 15-34.

Serrat-Olmos, M. D. et al., 2012. Accurate Detection of Black Holes in MANETs using Collaborative Bayesian Watchdogs. *Wireless Days (WD), 2012 IFIP*.

Tamilselvan, L. & Sankaranarayanan, D. V., 2008. Prevention of Co-operative Black Hole Attack in MANET. *Journal of Networks*, 5 May, pp. 13-30.

Tobin, J., Thorpe, C. & Murphy, L., 2017. An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks. *IEEE 85th Vehicular Technology Conference: VTC2017-Spring*.

Zapata, M. G., 2002. Secure Ad-hoc On-Demand Distance Vector (SAODV) Routing. *ACM SIGMOBILE Mobile Computing and Communications Review,* 6(3), pp. 106-107.