Literature Review for Capstone Project

Preventing Black Hole Attacks In MANETS Using Machine Learning

Audience
Project sponsors, project mentors, unit coordinators and all others in the university and ITC community interested in this project.

Purpose
The purpose of this document is to concisely summarise the major findings of the literature review for this project that provided us with the knowledge to proceed with the dataset creation and the meachine learning stages. The bibliography gives credit to the most valuable sources of information for the acquired knowledge that was required for this project.

Authour
Alan Gaugler

An extensive literature review of MANET’s (Mobile ad hoc networks), AODV (Ad Hoc On-Demand Distance Vector) protocol and typical black hole cyber-attacks was carried out by the team. This in-depth review was essential in correctly understanding how nodes in MANETs, in particular those that employ the AODV protocol behave and establish communication. It was also essential to understand how a black hole node would infiltrate the network and interact with other nodes, acting as a transfer point between nodes but dropping the data packages, causing disruption in essential communications.

Many videos were also observed by the team which proved to be essential in learning the protocols and the configuration of the NS-3 network.

From the literature review, a solid understanding of the AODV network protocol was learned as well as the behavioural characteristics of black hole nodes infiltrating the network. Several of these characteristics could be used for a node to identify a first-tier neighbour as a black hole node rather than a normal node.

These include:

Neighbour is never the Origin of RREQ and never sends RREQs: As a black hole node is not a node common to the network or group, it is unlikely that it would ever initiate a data transfer to a legitimate node. A strong indicator that the neighbour is a BHN is it has a count of 0 of RREQs with itself as the origin. Additionally, if a BHN always responds to an RREQ with an RREP, it would never re-broadcast the RREQ. It is also highly likely that several other legitimate nodes are also inactive during the simulation period, however, this is still a suitable flag that can be used.

Neighbour is never the Destination of RREQ: Similar to above, as a black hole node is not a node common to the network or group, it is unlikely that it would ever be the desired endpoint of a data transfer from a legitimate node. A strong indicator that the neighbour is a BHN is it has a count of 0 of RREQs with itself as the destination. It is also highly likely that several other legitimate nodes are never the desired destination during the simulation period, however, this is still a suitable flag that can be used.

High response rate to RREQ messages: As a black hole node aims to disrupt as much communication as possible, it is likely to respond to most or all of the RREQ messages it receives from a neighbour with an RREP message so as to disrupt as much communication as possible. This would lead to a very high response rate of RREQ messages which is a strong indication that the neighbour is a BHN.

Low Hop Count: The hop count counts the number of tiers or hops between the current node and the destination node. When a node is involved in setting up a link between the source and destination, one of its priorities is to set up the shortest link or the lowest hop count to the destination. A black hole node would not only respond to an RREQ with an RREP and high sequence number, but it would also respond with a short hop count to the destination node to make it a more attractive routing option. It is very likely that a BHN would always respond with the minimum hop count of 1 to an RREQ so that it is the favoured routing path.

High Sequence number increment: A sequence number is utilized in an AODV network for communication between nodes to identify which received message from a node is the most recent. The higher sequence number is always treated as the most up-to-date message by any node reading it and will update its routing tables accordingly. A black hole node will typically respond to an RREQ message with a higher than usual sequence number in its RREP (response message). The behaviour of a normal node is to increment the sequence number by 1 or send back the current sequence number in its routing table if it is greater. So a key indicator of a black hole node is receiving RREP responses with a higher than normal sequence number.

Rapid Response time: A black hole node will typically respond immediately to a RREQ with a RREP, instead of waiting longer for the RREP message to actually arrive from the destination node.

Low number of RERR messages: When a data packet for an inactive route or unknown destination is received, a Route Error (RERR) message is generated. This RERR is broadcast to all neighbours.

Low number of Data Packets being sent: After an RREP is returned to the origin node, a connection between the origin and destination has been established and then data transfer will begin. The data transfer may be a unicast from the origin node but very often it is two-way communication such as a conversation. As such it is expected that a considerable number of data packets will be forwarded from the neighbour node onto the subject node which will then forward it onto the next hop towards the destination. As the BHN has never established the connection between the source and the destination, no data packets will ever come from the BHN to be forwarded on towards the destination.

The identification of these main unique behavioural characteristics of black hole nodes lead to the development of a dataset that could be used for the machine learning process for malicious node detection.

Please refer to the bibliography at the end of this document to find the most useful research papers reviewed for this project.

Bibliography

Dr. B Awerbuch and Dr. A Mishra, “Ad hoc On Demand Distance. Vector (AODV) Routing Protocol”, Department of Computer Science Johns Hopkins University. https://eclass.uoa.gr/modules/document/file.php/DI367/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/aodv.pdf

Farahani, G., 2021. Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. Security and Communication Networks, 2021, pp.1-15.

Jaiswal, P. and Kumar, R., 2012. Prevention of black hole attack in MANET. *International Journal of Computer Networks and Wireless Communications*, *2*(5), pp.599-606.

Jhaveri, R.H., Desai, A., Patel, A. and Zhong, Y., 2018. A sequence number prediction based bait detection scheme to mitigate sequence number attacks in MANETs. *Security and Communication Networks*, *2018*, pp.1-13.

Kumar, J., Kulkarni, M. and Gupta, D., 2013. Effect of Black hole Attack on MANET routing protocols. *International Journal of Computer Network and Information Security*, *5*(5), p.64.

Majumder, S. and Bhattacharyya, D., 2019. Adopting Machine Learning Technique to Mitigate Various Attacks in MANET-A Survey Report. *International Journal of Scientific Research and Review*, *8*(6), pp.288-295.

Mukkawar, M.R. and Gawali, S.Y., A Survey on How Black Hole and Worm Hole Attack Evolves on AODV Routing Protocol.

Perkins, C., Belding-Royer, E. and Das, S., 2003. *Ad hoc on-demand distance vector (AODV) routing* (No. rfc3561).

Rani, P., Verma, S. and Nguyen, G.N., 2020. Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. *IEEE Access*, *8*, pp.121755-121764.

Shafi, S., Mounika, S. and Velliangiri, S., 2023. Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET. *Procedia Computer Science*, *218*, pp.2309-2318.

Srivastava, S., Yadav, C.S. and Kumar, P., 2021. Security Analysis Of Malicious Attacks In MANET Through Machine Learning Algorithm. Webology (ISSN: 1735-188X), 18(6).

Tejaswini, M.K. and Adilakshmi, M.Y., 2020. Black Hole Attack Detection Using Machine Learning Algorithms in MANET–Performance Comparision. International Research Journal of Engineering and Technology (IRJET) Volume, 7.

Tseng, F.H., Chou, L.D. and Chao, H.C., 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), pp.1-16.

Yassein, M. B.., Khamayseh, Y., AbuJazoh, M., Feature Selection for Black Hole Attacks. *Journal of Universal Computer Science, vol. 22, no. 4, Apr. 2016*