**Poster Discussion 29/04/23**

**Size requirements:**

Is it A0? (841x1189mm).

Is the minimum font size 18 points?

**Grammar:** spell black hole as two words

**General:** focus on MANET or AODV protocol?

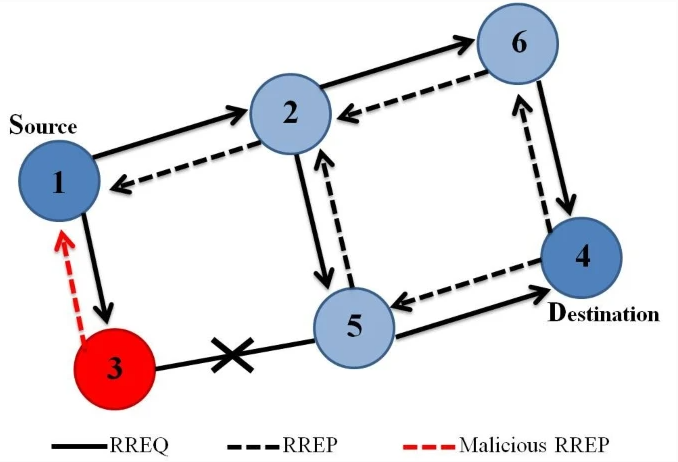
Background colour?

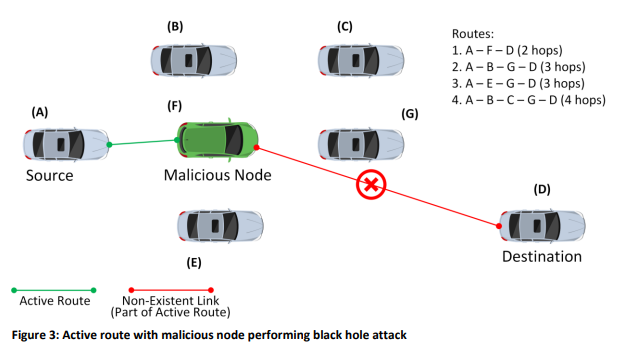
**Introduction:**

Mention they can be deployed rapidly.

**Objective:** Preventing attacks was a little bit beyond our scope. Should we limit it to just detecting black hole attacks? This also relates to the title. At least mention detect. Should AODV be mentioned in the objective?  
**TH** I agree that the objective should be to detect BH using ML from network traffic.

Two figures from the same source??







**Methodology:**

Add: Creating a dataset from NS3 AODV network simulations

Maybe in \* 2 write “and convert it into a useable dataset.”

Identify and detect? Maybe just identify

3. Over D node super impose **Destination**

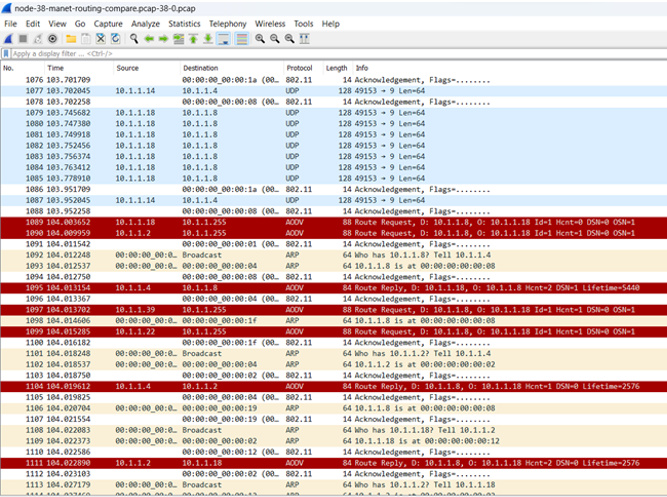


Figure 5. Example Output of network messaging from the NS3 that was transformed into a dataset.

Findings:

This project found that developing and evaluating a machine learning algorithm to detect black hole attacks in MANETs is possible. However, this project was unable to adequately simulate a black hole attack within the time frame due to technical challenges faced. Editing some data with expected black hole node behaviour allowed us to continue.

Finding 1: open source nature? Tristan can summarise this better

Finding 2:

Black hole nodes can be detected by their unique behaviour:

They always respond to a route request (RREQ) with a route reply (RREP).

They always claim to have the shortest path to the destination.

They always claim to have the most recent path to the destination. (high sequence number)

They never forward a RREQ to their neighbours.

Finding 3: Maybe better to state. “SVMs and RF classifiers perform well to detect black holes attacks.

Remove Finding 4

Random Forest not forrest

6. Should we replace this with something else?

**Conclusion:**

Delete last two words.

Should we stay clear of the technical issues?

Preventing blackhole attacks in MANETS using dynamically generated audit data is feasible. This project succeeded in developing and evaluating a machine learning algorithm that can be used in future work to detect and prevent blackhole attacks. Future work should focus on evaluating the performance of the machine learning algorithm dynamically in the MANET.

Further, the use of NS3 requires specialist knowledge and future work should ensure this specialist knowledge exists or time given to the knowledge being acquired. Preventing blackhole attacks in MANETs will be great benefit to society as it will give assurances to disaster and emergency management applications that the use of MANETs will be safe.