AUTHORS Tristan Hore, Thi Doan, Alan Gaughler, Johnsons Sangah
AFFILIATIONS Univeristy of Canberra

Preventing Black Hole Attacks In Manets Using Dynamically Generated Audit Data

MOBILE ADHOC NETWORKS (MANETS)) IS A TYPE OF WIRELESS NETWORK WHERE SEVERAL DEVICES, SUCH AS RADIOS, SMARTPHONES, LAPTOPS, DRONES OR SENSORS, COMMUNICATE DIRECTLY WITHOUT NEEDING ANY PRE-EXISTING OR CENTRALISED INFRASTRUCTURE.

1.

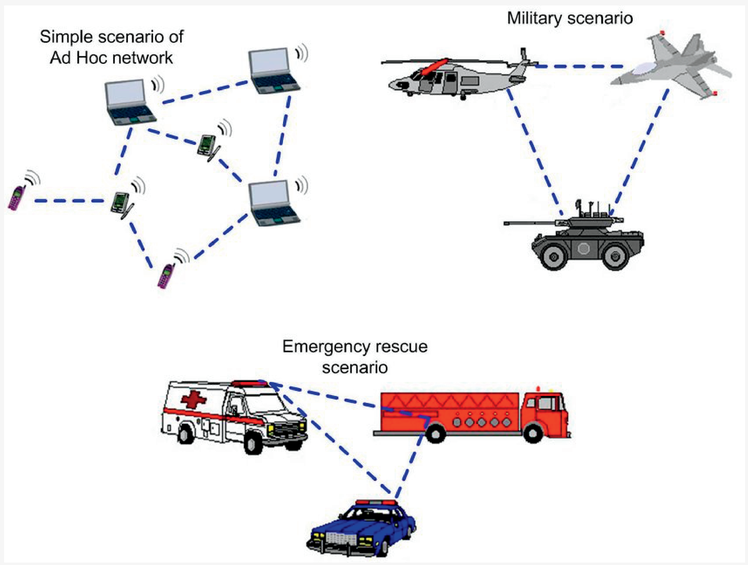


Figure 1. *Diagram of MANET with a Black Hole Node A (Source: Fakultas et al.)*

2.

INTRODUCTION

MANETS ARE USED WHERE EXISTING NETWORK INFRASTRUCTURE IS DAMAGED, UNAVAILABLE, OR NOT POSSIBLE SUCH AS IN DISASTER-STRICKEN AREAS, MILITARY OPERATIONS, OR REMOTE REGIONS.

THE ADHOC NATURE OF THE NETWORKS MAKE THEM VULNERABLE TO VARIOUS ATTACKS - SUCH AS A BLACKHOLE ATTACK. A BLACK HOLE ATTACK IS A TYPE OF CYBER-ATTACK WHERE A MALICIOUS OR COMPROMISED NODE IN THE NETWORK FALSELY CLAIMS TO HAVE THE SHORTEST ROUTE TO A DESTINATION, MAKING IT THE PRIORITISED PATH FOR LINK ESTABLISHMENT.

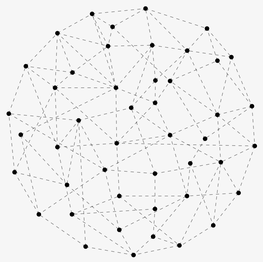
OBJECTIVE

This project aimed to prevent blackhole attacks in MANETs using dynamically generated audit data.

METHODOLOGY

The approach taken in this project to address the aim included:

- Performing a literature review to understand what the current state of the literature
- Using NS3 to create a MANET and generate audit data
- Developing and evaluating a machine learning algorithm to identify and detect malicious nodes from audit data



3.

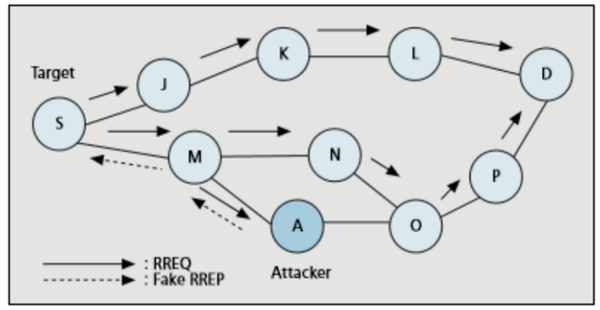


Figure 2. *Diagram of MANET with a Black Hole Node A (Source: Fakultas et al.)*

4.

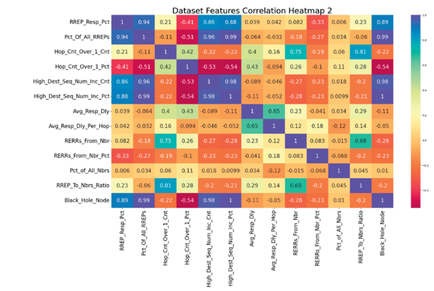


Figure 3. *Correlation heatmap between features and target variable*

5.

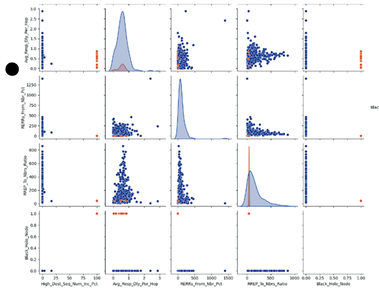


Figure 4. *A pair plot showing the relationship between variables. The blackhole nodes are the brown colour.*

RESEARCH / FINDINGS

This project found that developing and evaluating a machine learning algorithm to detect and prevent blackhole attacks in MANETs is possible. However, this project was unable to adequately simulate a blackhole attack due to technical challenges faced.

Support Vector Machines and Random Forrest Classifier were the chosen models. Once trained using the created sample data, the models demonstrated a strong performance.

FINDING 1.

Simulating a blackhole attack in NS3 is technically challenging, due to it's open source nature.

FINDING 2.

To detect a blackhole node, the features to use include: route request (RREQ), route reply (RREP) and average response delay

FINDING 3.

Support Vector Machines and Random Forrest Classifiers are high performing models.

FINDING 4.

The AODV protocol is most commonly used in practical settings such as disaster and emergency management

6.

	Msg_Index	frame_time	frame_time_relative	This_Node	Nbr_Node	Next_Hop	TTL	AODV_Msg	Source_Node	Destination_Node	Hop_Count	Source_Seq_Num	Dest_Seq_Num	BroadCast_ID
903	1153	106.035556	106.023254	10.1.1.45	10.1.1.25	10.1.1.22	2	RREP	10.1.1.18	10.1.1.8	1		0	
904	1155	106.037315	106.025011	10.1.1.45	10.1.1.8	10.1.1.2	2	RREP	10.1.1.18	10.1.1.8	0		0	
905	1157	106.039569	106.027265	10.1.1.45	10.1.1.31	10.1.1.22	1	RERR		10.1.1.37	2		0	
906	1158	106.040347	106.028043	10.1.1.45	10.1.1.8	10.1.1.2	2	RREP	10.1.1.20	10.1.1.10	5		0	
907	1160	106.042064	106.02976	10.1.1.45	10.1.1.31	10.1.1.2	2	RREP	10.1.1.18	10.1.1.8	1		0	
908	1161	106.042615	106.030311	10.1.1.45	10.1.1.8	10.1.1.2	1	RERR		10.1.1.10	1		0	
909	1163	106.047176	106.034872	10.1.1.45	10.1.1.1	10.1.1.2	2	RREP	10.1.1.18	10.1.1.8	1		0	
910	1167	106.055479	106.043175	10.1.1.45	10.1.1.1	10.1.1.2	2	RREP	10.1.1.18	10.1.1.8	1		0	
911	1168	106.060203	106.055899	10.1.1.45	10.1.1.1	10.1.1.2	2	RREP	10.1.1.18	10.1.1.8	1		0	
912	1178	106.298831	106.286507	10.1.1.45	10.1.1.32	10.1.1.255	7	RREQ	10.1.1.20	10.1.1.10	2	8	0	8
913	1179	106.299117	106.286813	10.1.1.45	10.1.1.8	10.1.1.255	6	RREQ	10.1.1.20	10.1.1.10	3	8	0	8
914	1180	106.301117	106.288813	10.1.1.45	10.1.1.37	10.1.1.255	6	RREQ	10.1.1.20	10.1.1.10	3	8	0	8
915	1181	106.302861	106.290557	10.1.1.45	10.1.1.46	10.1.1.255	6	RREQ	10.1.1.20	10.1.1.10	3	8	0	8
916	1182	106.304118	106.291814	10.1.1.45	10.1.1.37	10.1.1.255	6	RREQ	10.1.1.20	10.1.1.10	3	8	0	8
917	1184	106.307811	106.295507	10.1.1.45	10.1.1.1	10.1.1.255	7	RREQ	10.1.1.20	10.1.1.10	2	8	0	8
918	1188	106.310424	106.29812	10.1.1.45	10.1.1.3	10.1.1.255	5	RREQ	10.1.1.20	10.1.1.10	4	8	0	8

Figure 5. Example Output of a Data Frame after a MANET simulation using the AODV protocol.

CONCLUSION

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. Technical challenges limited the ability for the algorithms performance to be evaluated dynamically and this can be the focus of future work. 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 to use.

REFERENCES

Reference 1
Reference 2
Reference 3
Reference 4