Feature Engineering for Detection of Wormhole Attacking in Mobile Ad Hoc Networks with Machine Learning Methods

Jonny Karlsson[1], Magnus Westerlund[2], Laurence Dooley[3], Göran Pulkkis[4]

Abstract

Due to the self-configuring nature of a Mobile Ad Hoc Network (MANET), each node must participate in the routing process, in addition to its other activities. Therefore, routing in a MANET is especially vulnerable to malicious node activity leading to potentially severe disruption in network communications. The wormhole attack is a particularly severe MANET routing threat since it is easy to launch, can be launched in several modes, difficult to detect, and can cause significant communication disruption. In this paper we establish a practice for feature engineering of network data for wormhole attack prevention and detection with intrusion detection methods based on machine learning.

Keywords: Mobile Ad Hoc Networks, MANET, wormhole attack, feature engineering

1 INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a self-configuring arrangement of mobile devices interconnected by wireless links, with no fixed infrastructure like base stations and dedicated routers. MANETs can be used e.g. for establishing wireless sensor networks, vehicular networks, military communications, extreme rescue operations and providing Internet connectivity where some nodes are located out of radio range of an Internet connection point.

[1] Arcada University of Applied Sciences, Finland, Department of Business Management and Analytics, [jonny.karlsson@arcada.fi]
[2] Arcada University of Applied Sciences, Finland, Department of Business Management and Analytics, [westerma@arcada.fi]
[3] The Open University, UK, Computing and Communications Department, [l.s.dooley@open.ac.uk]
[4] Arcada University of Applied Sciences, Finland, Department of Business Management and Analytics, [goran.pulkkis@arcada.fi]

Due to the self-configuring nature, each MANET node participates in the routing process, in addition to its other activities. Several routing protocols have been proposed for MANETs, such as Ad Hoc On Demand Distance Vector (AODV) (Perkins & Royer 1999) and Dynamic Source Routing (DSR) (Johnson & Maltz 1996), but security has typically not been a priority in routing protocol development (Taneja & Kush 2010). Consider for example a large scale MANET that is integrated in the future world of Internet of Things (IoT), where devices both dynamically and autonomously enter and leave the network, and it is therefore difficult to establish trust relationships among the nodes. Consequently, routing in a MANET is especially vulnerable to malicious node activity leading to potentially severe disruption in network communications (Karlsson, Dooley & Pulkkis 2012, Agrawal, Jain & Sharma 2011). Such disruption can range from deliberately ignoring the routing protocol to tampering routing packets. For example, to save energy a selfish node may simply not take part in the routing process leading to packet loss, while a malicious node can launch serious network attacks, such as rerouting packets from their original path to an erroneous destination node and even stealing the identity of a node.

The wormhole attack (Hu, Perrig & Johnson 2003) is a particularly severe MANET routing threat since it is easy to launch, can be launched in several modes, difficult to detect and can cause significant communication disruption. Two collaborating malicious nodes create a fictive shortcut link in the network by forwarding routing packets to each other with the intention to attract more data packets to traverse the wormhole link. Once the wormhole has been successfully established, the malicious nodes can disrupt network operation by either dropping packets or launching more serious attacks, such as eavesdropping and packet sniffing.

A wormhole attack can be launched in either hidden mode (HM) or participation mode (PM) (Khabbazian, Mercier & Bhargava 2006). In a HM wormhole, malicious nodes capture and forward routing packets to each other without modifying the actual packets, so the wormhole nodes never appear in routing tables. A PM wormhole operates in the same way as a HM wormhole with the exception that the malicious nodes process routing packets as any pair of legitimate nodes and thus appear in a wormhole infected route as two contiguous nodes. The malicious nodes can forward routing packets to each other using either an in-band (I-B) or out-of-band (O-B) wormhole link. I-B tunnels packets between the malicious nodes via genuine network nodes. O-B wormhole links are more complex from the attacker's point of view because they require an external communication channel, i.e., network cable or directional antenna, to establish a direct link between the wormhole nodes.

Due to the open nature and lack of dedicated central nodes such as routers, routing security in MANETs cannot rely on cryptography. Instead, security must be based on anomaly detection and trust in the network established based on node behavior. Several proposals for Intrusion Detection Systems (IDSs) for MANETs have been proposed in the literature but they typically do not take all types of attacks into account, especially not all wormhole attack types. Many research papers also propose mechanisms for detecting specific threats, but in a realistic MANET the most convenient solution would be a comprehensive IDS capable of identifying at least all severe routing attacks.

In feature engineering the most important factor has been considered to be the features used. For many independent features correlating well with a class, learning has been easy. However, if a class is a very complex function of the features, then it might be impossible to learn such a class. When the raw data is not in a form that is amenable to learning, features can still of be constructed features from it. It has been considered that most of the effort in a machine learning project goes to feature engineering. (Domingos 2012)

In this paper we look at the feature engineering task of identifying wormhole attacks by pre-formatting MANET data for an IDS based on Machine Learning data. The contribution of this paper is to identify specific features of each wormhole attack type for distinguishing the difference between healthy and wormhole infected routes. These features can then be utilized for creating training data.

The rest of the paper is organized as follows. In Chapter 2 an overview of previous feature engineering related research on IDS for MANETs is given. Chapter 3 provides a detailed overview of the different wormhole attack types and points out the specific features differentiating wormhole infected routes from healthy routes. Finally, some concluding comments and plans for future research on machine learning based IDSs for MANETs are presented in Chapter 4.

2 RELATED RESEARCH

The fundamental goal for machine learning based IDSs is to generalize beyond the examples in the training set. Hence, capturing the underlying complexity of the raw data set when performing feature engineering is of outmost importance. Simply reducing data dimensions or compressing data is often difficult, even for a well-known problem. Intrusion attack metrics are needed in feature engineering for machine learning based IDS implementations. Four wormhole attack metrics are defined in (Mahajan et al. 2008):

1. *Strength:* the number of end-to-end routing paths passing through a wormhole tunnel.
2. *Path Length:* the length difference between an advertised routing and an actual routing path.
3. *Attraction:* the decrease in routing path length offered by a wormhole.
4. *Robustness:* the persistency of a wormhole without a significant strength decrease for minor network topology changes.
   Maulik & Chaki (2010) add a fifth wormhole attack metrics to this list:
5. *Packet Delivery Ratio:* number of delivered packets divided by the total number of dispatched packets.

Use of information entropy in feature engineering for selection of most relevant features in an IDS based on machine learning is shown in (Kayacik, Zincir-Heywood, & Heywould 2005, Tang, Jiang, and Zhao 2010). A methodology to calculate the Information Gain (IG) (Information 2014) for each feature and for each intrusion attack class in a training dataset for machine learning is presented and applied to the "10% of KDD CUP 1999" dataset (KDD 1999). The most relevant feature in each class (22 intrusion attack classes and the normal class) is defined by the highest IG in comparison with other features. Features in a subset of size 10 from a set of 41 features in the training dataset had

the highest IG in at least one of the 23 classes and these ten features were chosen for the testing phase. A SVM-based machine learning algorithm TASVM (Triangle Area Based SVM) was proposed and used in the testing phase in (Tang, Jiang, and Zhao 2010). In comparison with two other intrusion detection models, intrusion detection rate was higher in binary intrusion detection (99.88%) and in four of five attack classes (at least 92,35 %) while false positive rate was about the same (2,99%).

Mahajan et al. (2008) proposed an IDS for detecting I-B wormholes created by three malicious nodes, a pair of wormhole endpoint nodes and a node for forwarding wormhole traffic. The link between the wormhole endpoint nodes is called a self-contained I-B wormhole, which can be extended to wormhole links between legitimate node pairs. The proposed IDS is based on anomaly detection in features representing measured delays:

- The difference between end-to-end delay and the sum of hop delays is anomalously large for wormhole infected routes.
- Hop delays in uninfected routes are anomalously prolonged in nodes used by a wormhole tunnel because of the tunneled network packets.

A hop delay is defined by the time spent in the sending node. Wormhole detection rate was in most cases 70 – 100 % in MANET simulation experiments with 4 randomly chosen topologies for 15 nodes in an area size of 1500*1500 meter.

In (Barani & Gerami 2013) machine learning based on One-class Support Vector Machine (OCSVM) (Schölkopf et al. 2001) is used for anomaly detection of flooding, blackhole, neighbour, rushing, and wormhole attacks in a dynamic MANET. Each network node monitors own network traffic and measures own network state in a time slot as a p-dimensional feature vector. Each measured feature value is scaled to a [0,1] interval value for input to the used machine learning algorithms. Machine learning consists of an initial training phase and an updating phase integrated in the detection phase. Each node updates in each time slot the OCSVM feature vector set with detected normal feature vector and removes feature vectors with weights less than a given threshold. The dynamic MANET characteristics are taken in consideration by weights decreasing over time for feature vectors in the OCSVM feature vector set. In simulation experiments with 30 mobile MANET nodes a feature vector with 22 values was measured by each node at each time slot. Three features were related to the used constant bit rate traffic, ten features were related to the route discovery process, five features were related to route disruption, and four features were related to the used modified AODV routing protocol. In the detection phase one node was selected to be a malicious node, which launched flooding, blackhole, neighbour, rushing, and wormhole attacks. Inclusion of the updating phase improved average detection rate from about 50% to about 95% and decreased the average false positive rate from about 10% to about 2%.

In (Pastrana et al. 2012) the efficiency of intrusion detection in MANETs is evaluated for six classification algorithms i.e., Multilayer Perceptron, the Linear classifier, the Gaussian Mixture Model (GMM), the Naïve Bayes classifier, the Support Vector Machine (SVM) model, and Genetic Programming (GP) algorithms. Detection out four different attack types i.e. Black Hole, Forging, Packet Dropping, and Flooding was studied in simulation experiments with 50 randomly placed MANET nodes. Eleven input data features were used for anomalous network activity detection i.e., number of Route Request packets sent/received, number of Route Reply packets sent/received, number of

route error packets sent/received, number of bytes sent/received, number of one-hop neighbours of each node, percentage of changed routed entries in the routing table of each node, and percentage of the changes in the sum of hops in all routing entries for each node. For simulation experiments with a multiclass dataset intrusion detection rate was about 75%, false positive rate between 5% and 25% and class error about 20% for all six classifiers. Excluding GP, classification results were best for the machine learning based SVM model.

3 WORMHOLE ATTACK TYPES AND THEIR SPECIFIC FEATURES

In this chapter, different wormhole attack types are described in detail and their individual features are highlighted. The knowledge of these features can be utilized for generating training data for Extreme Learning Machine (ELM), SVM, and other machine learning based IDS algorithms.

3.1 Hidden Mode Wormhole

Consider the MANET scenario shown in Figure 1 where S is the source and D is the destination. The shortest path in terms of hops from S to D is in this case S - I_1 - I_2 - I_3 - I_4 - I_5 - I_6 - D. However, if malicious nodes M_1 and M_2 launch a HM wormhole, the shortest path is S - I_1 - I_6 – D as I_1 and I_6 falsely appear to each other as neighbors since M_1 does not add its own IP address to the source field of the IP packet carrying the route request (RREQ) packet received from I_1 to be forwarded to its neighbors. Instead M_1 encapsulates the original RREQ packet into a new IP packet that is tunneled to M_2. When receiving the tunneled RREQ, M_2 extracts the original RREQ packet and forwards it to its neighbors without modifying any of the routing packet parameters. Hence, to I_6 it appears the RREQ was sent from I_1 and as a result the IP address of I_1 is added to the routing table as next hop on the route towards node S.

A deviant feature of a route infected by a HM wormhole is that the distance between false neighbor nodes is significantly longer than between legitimate neighbor nodes. It is impractical to assume each node is able to get location information through a navigation system, such as GPS, but the distance can also be estimated for example by measuring the packet traversal time (PTT) of a packet between two nodes, as proposed in (Khabbazian, Mercier & Bhargava, 2006). Each node can thus keep track of the PTT between itself and its neighbors. This track keeping can then be used for analyzing the validity of a neighbor.

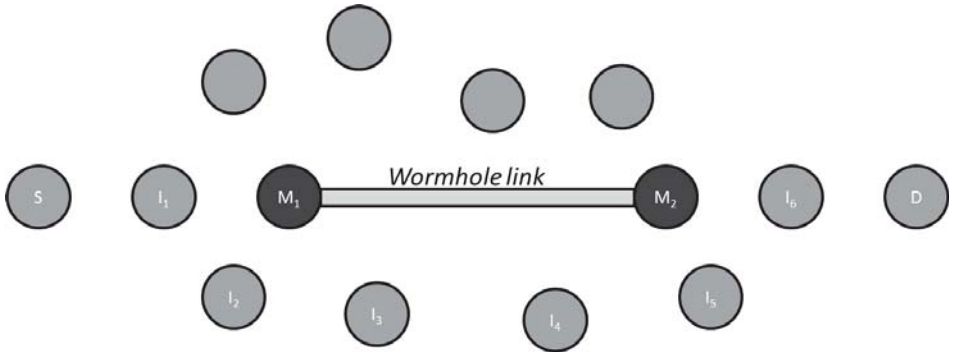

Figure 1. A MANET example scenario.

3.2 Participation Mode Wormhole

If M1 and M2 (see Figure1) launch a PM wormhole, then the shortest path would be S – I_1 – M_1 – M_2 – I_6 – D. In this case, the PTT between M_1 and M_2 would be significantly higher than the PTT for any other pair of nodes. Since M_1 can falsely confirm M_2 as its neighbor and vice versa, neighbor validation is not reliable for identifying PM wormholes. However, PTT is still a reliable metric, if it is analyzed for a whole route, as is proposed in (Karlsson, Dooley & Pulkkis, 2011). So, a reliable and deviant feature of route infected by a PM wormhole is that PTT per hop count (HC) is significantly higher than for a legitimate route.

Assuming that the malicious wormhole nodes always use the same identities (such as IP and/or MAC address) and that a network node is able to collect and track information about each intermediate node on every found route, as in the dynamic source routing (DSR) routing protocol, a deviant feature is that the malicious nodes appear as legitimate neighbors on significantly more tracked routes than any other legitimate pair of nodes. The average HC of routes traversing the wormhole nodes may also be significantly lower than the HC of other routes not traversing the wormhole link.

3.3 In-band Wormhole Link

An I-B tunnel is shown in Figure 2. In this case when M_1 receives a RREQ packet from I_1 it encapsulates it into a new packet that is sent to M_2 through legitimate nodes (I_3 – I_4 – I_5). If a wormhole uses an In-band wormhole link it will produce a very high PTT since it includes packet processing delays at the nodes through which packets are tunneled. Thus PTT is a highly reliable metric for identifying such a wormhole.

3.4 Out-of-band link

An example of an O-B wormhole link is shown in Figure 3. On the other hand, an O-B link is much more effective than I-B as it has a significantly lower delay (meaning it will attract more traffic) and at the same time more difficult to detect based on PTT

analysis as it sets a high requirement upon the accuracy of the PTT measurement, especially if the wormhole is launched in PM.

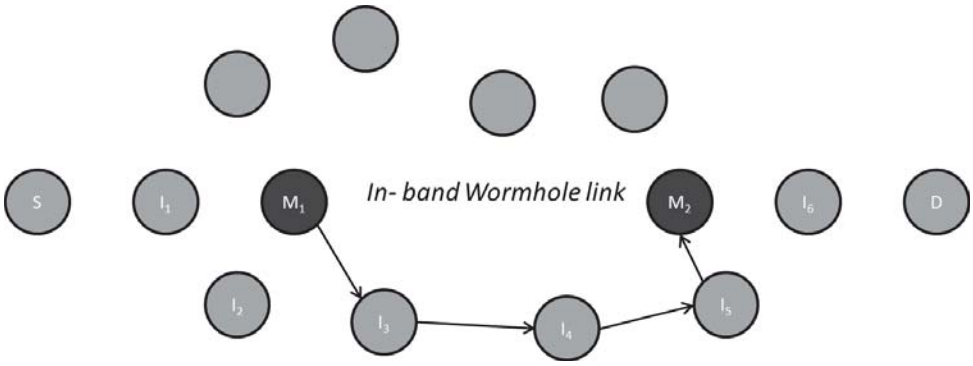

Figure 2. An example of an in-band wormhole link.

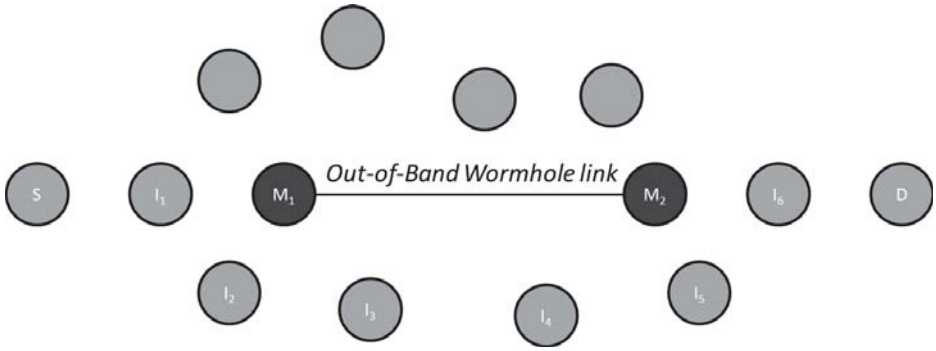

Figure 3. An example of an out-of-band wormhole link.

3.5 Summary of Features

The features that can be utilized and analyzed for identifying the specific wormhole types are summarized in Table 1. The only feature that can identify all four types of wormholes is PTT/HC. However, if the wormhole link has a low delay, i.e. launched in PM O-B, there is a high requirement upon the PTT measurement accuracy, since the difference between a healthy and an infected route is typically less than a microsecond. Therefore the wormhole attack detection precision can be strengthened by analyzing multiple features.

4 CONCLUSIONS AND FUTURE WORK

Machine learning based algorithms are effective for IDSs due to their generalizability. However, current algorithms proposed for MANETs are not capable of detecting all variants of the wormhole attack which is a severe threat on MANET routing. In this paper, specific features for each wormhole attack type have been identified. In terms of future research, the aim is to create training data based on the identified features needed

for making machine learning based algorithms capable of detecting all types of wormhole attacks. A long-term goal is to develop for MANETs a single adaptive IDS, which is based on machine learning and capable of effectively detecting/preventing all severe routing attacks, in order to eliminate the need for using multiple standalone security mechanisms.

Table 1. Features characterizing different types of wormholes and their estimated reliabilities: 1 = low reliability, 2 = medium reliability, 3 = high reliability.

WORMHOLE TYPE	O-B	I-B
PM	- High PTT/HC (2) - Frequent appearance of specific node pair in routes (2) - Routes including specific route pair has lower average hop count (1)	- High PTT/HC (3) - Frequent appearance of specific node pair in routes (2) - Routes including specific route pair has lower average hop count (1)
HM	- High one hop PTT (3) - High PTT/HC (3)	- High one hop PTT (3) - High PTT/HC (3)

REFERENCES

Agrawal, S., Jain, S., & Sharma, S. 2011, A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. in: *Journal of Computing*, Vol. 3, pp. 41-48.

Barani, Fatemeh & Gerami, Sajjad. 2013, ManetSVM: Dynamic Anomaly Detection using One-class Support Vector Machine in MANETs, in: *Proceedings of the10th International ISC Conference on Information Security and Cryptology (ISCISC)*, IEEE Publishing.

Domingos, Pedro. 2012, A Few Useful Things to Know about Machine Learning, in: *Communications of the ACM*, Vol. 55, No. 10, pp. 78-87.

Hu, Y., Perrig, A., & Johnson, D.B. 2003, Packet leashes: a defense against wormhole attacks in wireless networks. In: *Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM'03)*, San Fransico, CA, USA, IEEE Publishing.

Information Gain. 2014. Lecture Notes, University of Washington, USA, Accessed 12.10.2014.
https://courses.cs.washington.edu/courses/cse455/10au/notes/InfoGain.pdf

Johnson, D.B. & Maltz, D.A. 1996, Dynamic Source Routing in Ad Hoc Wireless Networks. in: *Mobile Computing*, Vol. 353, pp. 153-181.

Karlsson, J., Dooley, L.S., & Pulkkis, G. 2011, A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis. in: *Sensors*, Vol. 11, No. 12, pp. 11122-11140.

Karlsson, J., Dooley, L. S., & Pulkkis, G. 2012, Routing Security in Mobile Ad-hoc Networks. in: *Issues in Informing Science & Information*, Vol. 9, pp. 369-383.

Kayacik h. Günes, Zincir-Heywood, A. Nur, & Heywood, Malcolm I. 2005, Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets, in: *Proceedings of Third Annual Conference on Privacy, Security and Trust.*

KDD Cup 1999 Data. 1999, Accessed 12.10.2014. Published October 10, 1999. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Khabbazian, M., Mercier, H. & Bhargava, V.K. 2006, NIS02-1: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure. in: *Proceedings of Global Telecommunications Conference (GLOBECOM '06)*, San Francisco, CA, USA.

Mahajan, Viren, Natu, Maitreya, & Sethi, Adarshpal. 2008, Analysis of Wormhole Intrusion Attacks in MANETs, in: *Proceedings of IEEE Military Communications Conference (MILCOM)*, IEEE Publishing, pp. 966-972.

Maulik, Reshmi & Chaki, Nabendu. 2010, "A Comprehensive Review on Wormhole Attacks in MANET. in: *Proceedings of the 9th International Conference on Computer Information Systems and Industrial Management Applications*, IEEE Publishing, pp. 233-238.

Pastrana, Sergio, Mitrokotsa, Aikaterini, Orfila, Augustin, & Peris-Lopez, Pedro. 2012, Evaluation of Classification Algorithms for Intrusion Detection in MANETs. in *Knowledge-Based Systems*, Vol. 36, Elsevier, pp. 217-225.

Perkins, C.E. & Royer, E.M. 1999, Ad-hoc on-demand distance vector routing. in: *Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, New Orleans, LA, USA, IEEE Publishing.

Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. 2001, Estimating the Sup.port of a High-Dimensional Distribution, in: *Neural Computation*. Vol. 13, No. 7, pp. 1443-1471.

Taneja Sunil & Kush, Ashwani. 2010. A Survey of Routing Protocols in Mobile Ad Hoc Network. in: *International Journal of Innovation, Management and Technology*, Vol. 1, No. 3, pp. 279-285.

Tang, Pingjie, Jiang, Rong-an, & Zhao, Mingwei. 2010, Feature Selection and Design of Intrusion Detection System based on k-means and Triangle Area Support Vector Machine. in: Proceedings of the Second International Conference on Future Networks. IEEE Publishing, pp. 144-148.