SMS Mobile Botnet Detection Framework

Abdullah J. Alzahrani and Ali A. Ghorbani

Faculty of Computer Science, University of new Brunswick

ISCX Information Security Centre of Excellence

UNB

Introduction

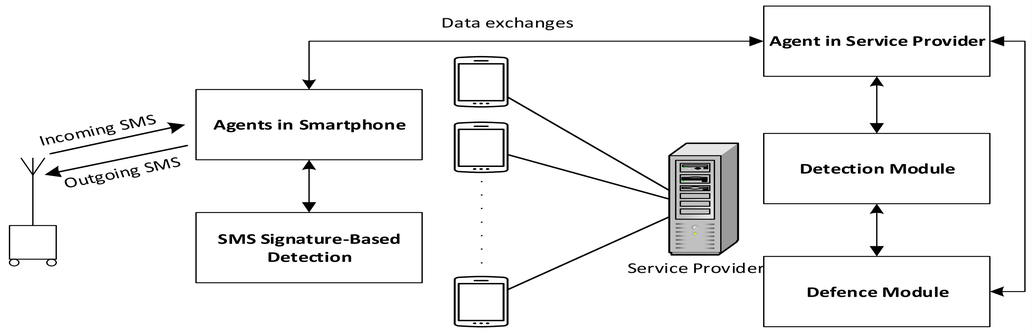
Mobile botnet *is a set of* ***compromised*** *smartphones that share the same command and control (C&C) channel, which are controlled by a bot master to perform a variety of* ***malicious*** *attacks.*

Objective:

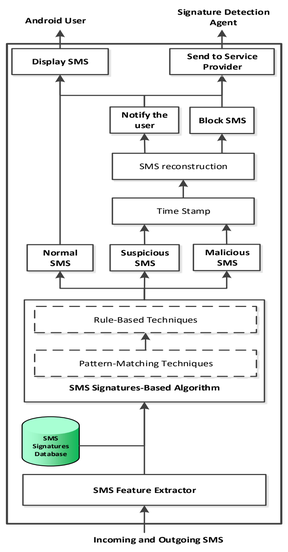
Developing a hybrid model of SMS botnet detector with following features:

- *A combination of signature-based and anomaly-based approach.*
- *Employ multi-agent technology to detect SMS botnet.*
- *Use Android botnet defence strategies.*

The Proposed Framework



SMS Signature Detection Module



✓Focusing on incoming and outgoing SMS messages.

✓Real-time content-based signature detection.

✓Using two approaches:
- Pattern-matching approaches.
- Rule-based techniques.

✓This approach was evaluated through the use of 50,000 text messages.

Signature Detection Experimental Results

Types	Features	# of SMS	Total	Percentage
Malicious	SMS body	0	165	0.5%
	Phones#	0		
	URLs	26		
	Commands	139		
	FromPhone#	0		
	ToPhone#	0		
Suspicious	Phones#	869	3115	5.5%
	URLs	144		
	Commands	2182		
Normal			51721	94%

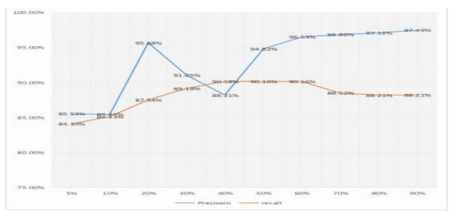
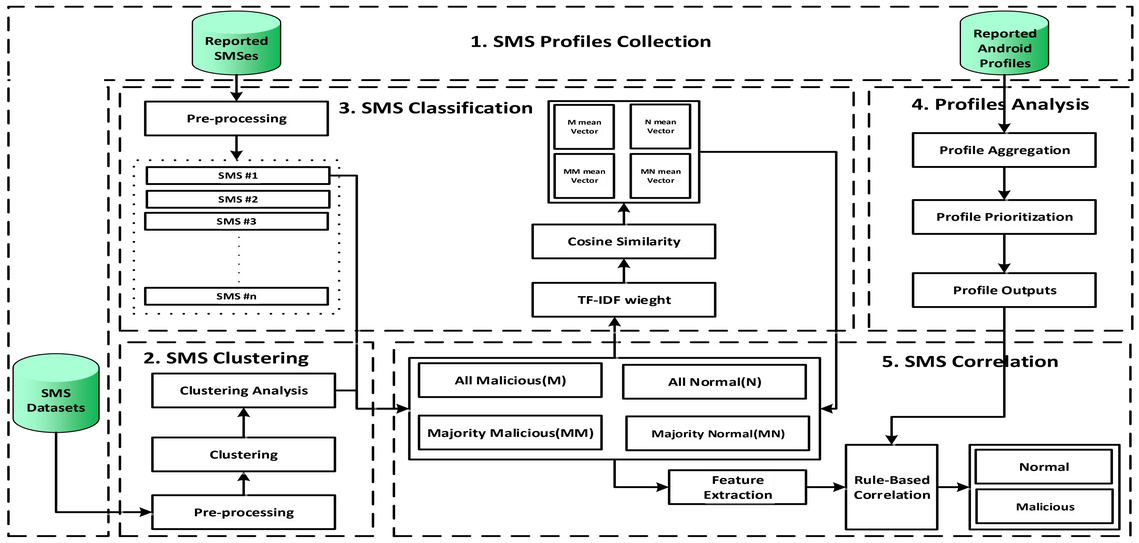


Figure 1.2: Precision and Recall Comparison for The First Experiment

Design of SMS Botnet Detection Module



➢ *SMS Profiles Collection:*

✓Responsible for collecting, combining, storing and retrieving data to perform anomaly detection.

➢ *SMS Clustering:*

✓Provides a rational summary of the collected data in terms of text-clusters.
✓Takes a set of data and then groups it based on the similarities.
✓X-means clustering: (Based on K-means -Find the number of clusters dynamically.)
✓Analyze the result of clusters and group them into four class labels.

➢ *SMS Classification:*

✓The clustering technique can increase the classification accuracy of detection
✓Apply machine-learning algorithm to classify the SMS messages SMS to one of the four class labels list:
- The TF-IDF is a statistical-based approach.
- Similarity Measurement.

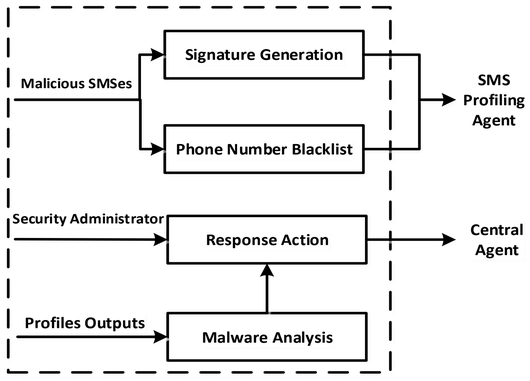
➢ *Profiles Analysis:*

✓Used to look for evidence of compromise rather than any specific attack.
✓Profile Aggregation: takes into account the similarity between particular profile features.
✓Profile Prioritization : prioritize each prole based on the following two features:
- Dangerous permissions
- User connectivity time.

➢ *SMS Correlation:*

✓Identify the relationship between the outputs of the profiles and each detected SMS message.
✓Apply rule-based correlation approach:
- The set of rules helps to produce fewer false positive alarms.
- It also has the ability to label unknown attack

SMS Botnet Defence Module



❑ Uses the output received from a detection module make logical decisions

➢ Signature Generation

✓ Signatures that are representative of attack patterns.
✓ Utilize Content-based approach:
- Very fast and robust algorithm.
- Create automatic signatures of SMS.

➢ Phone number Blacklist (PNBL).

✓ A list of phone numbers that the SMS botnet detection app should block.

➢ Malicious Application Analysis

✓ Analyzing reported apps and extracting their features is therefor a strong method defence against SMS botnets.
✓ Security administrator can perform static and dynamic analysis using common tools.

➢ Response Action

✓ To take down SMS bots and cutting the C&C channel, it requires the Android user to carry out action by removing the malicious application.

Detection Performance Experimental Results of two dataset

Detection Metric	A.1 experiment	A.2 experiment
Accuracy	0.968	0.965
Precision	0.986	0.982
Recall(TPR)	0.978	0.978
FNR	0.022	0.022
TNR	0.909	0.888
FPR	0.091	0.112
F-measure	0.982	0.980