International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Evaluation of the Alignment between the Location of Rogue Mobile Information Technology (IT) Gadgets and the Nature of Information that they Dispatch

Maxwell Mago
Lecturer, University of Zimbabwe School of Technology

Abstract**—** *Rogue mobile IT gadgets (RMITG) are mobile network handsets that are used for rogue (unorthodox) intentions such as stealing, cheating and other forms of cybercrime. Many earlier studies in mobile network security focused in other network sections, ignoring the lower layers of the Open Systems Interconnection (OSI) reference model, especially the network gadgets. This gap has caused a grey area being formed in the establishment of the location of RMITGs. This study attempts to determine the alignment between the location of RMITGs and the nature of information that they contain, in an effort to try and address the problems caused by the RMITGs. To satisfy the explanatory and exploratory nature of the study, the researcher applied a triangulated approach, using a multi-case strategy on different classes of 50 respondents. It was established that amongst the other variables that determine the relationship between the location of RMITGs and the information that they dispatch, their tracking is most influential. The researcher recommends an establishment of a mobile IT gadgets software application that monitors and records their changing locations in real time for use as and whenever necessary. These results are likely to help in directing resource allocation amongst mobile IT network security operators for their own benefit and that of their customers*.

Keywords**—** *Gadgets, information, mobile, network, operators, rogue, security, technology, tracking.*

I. INTRODUCTION

The location of mobile IT gadgets is about the positions of these network terminals, in respect of the network infrastructure. Location awareness is a crucial part of the context-awareness mechanism for ubi-computing [18]. Unlike in the case of older static IT networks, the locations of gadgets in the current mobile IT networks can be shifted wily Nelly. [16] says that modern mobile IT networks are no longer confined to geographical country boundaries, with the advent of instant roaming capabilities between various networks across borders. It is the basis of the abrupt changes in the locations of mobile IT gadgets. Users of wireless devices can be difficult to trace because they roam in and out of their wireless zones, have no fixed geographical point and can go online and offline easily and without warning [12].

These are the same terminals which are the sources of information that is communicated by mobile IT networks, yet the information may be genuine or rogue. Rogue gadgets are the ones that generate information content that is undesirable (disastrous, impersonating and/or malicious) to other users and/or networks. [14] says that a research conducted by security company GreenBorder showed that most of the malicious code that were cleaned from computers resulted from user behavior. The problem with the portable machines is that people will want to connect to the office no matter where they are or what they might have picked up while surfing at the nearest Wi-Fi hotspot [10]. These are practical habits that make the information that is dispatched by mobile IT gadgets becoming security suspects in the successful operations of the networks.

According to [15] (Available at prashant@tele.pitt.edu, accessed 04/11/2016), position location technologies are gaining prominence in the wireless market for several reasons: for hospitals to locate patients and equipment in a timely fashion; in homes to locate children and pets; in the military and public sector for enabling solders, policemen, and fire fighters with knowledge of their location and that of other personnel, victims, exits, dangers, the enemy, etc. However, scholars have suggested that the location behavior of mobile gadgets have tended to follow some form of pattern. This is more likely, if the gadgets are under the influence of undesirable users such as hackers, whose intention is primarily to intentionally achieve unauthorized access onto the targeted gadget and/or network. The motive would ostensibly include avoidance of detection. The derived technologies have also found applicability in other wireless features. [1] notes that once an attacker has physical access to a device, it is usually relatively easy to obtain complete access to all data and software on the device, and disappear ‘on the go’ since the device does not require constant attachment to a particular physical position.

II. BACKGROUND

The difficult economic situation in Zimbabwe, evidenced by unprecedented unemployment levels and liquidity crunch manifested itself by promoting an environment of inhuman behavior such as thieving. Mobile money transfers (using ecocash, telecash and one wallet), e-banking, e-commerce and other business app transactions have turned mobile IT networks to be the major custodian of personal privacy details, their economic data and resources. This paradigm shift to cashless business transactions promulgated by the central bank and other business quarters caused the practice of thieving to move to mobile IT networks, using the widely accessible gadgets. [17] note that a number of factors have been attributed to the notable growth of mobile financial transactions: the increased penetration of mobile technology, the large part of the financially excluded population in the traditional banking system, the increased phone density

Maxwell Mago, “Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch,” *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

amongst the populace, amongst others. This in evidently also caused a proliferation of the so called rogue users. According to [11], a rogue user is an active participant in an online community who violates the community's rules or spirit.
The mobility of the gadgets at the disposal of these undesirable elements of societies has not helped the situation. It is widely believed that the perpetrators easily flee from law enforcement agents by relocating immediately after pouncing on their unsuspecting targets. Instances of fake currency note dealers, identity thefts and stolen handsets have been recorded, as innocent citizens fall victim. [5] suggests that it is how traditional PR and corporate communication theories, models and paradigms may not be successfully used in an area of advanced information technology and global audience. Such theories and propositions have exposed the requirement to look further into the alignment between the location of rogue mobile IT gadgets and the information that they dispatch, in an attempt to establish some patterns. When established, such patterns could be the starting point in monitoring the behavior of those gadgets in order to combat their effects.

A. *Problem Statement*

The difficulty in apprehending the rogue network users that arises from their constant mobility is cause for concern to both network vendors, law enforcement agents and other members of societies. If it continues unabated, the nation will continue to lose out from these money laundering agents and ineffective law enforcement investments.

This study will endeavor to find ways of lightening the efforts of solving this surmountable task, by exposing the alignment between the location of rogue mobile IT gadgets and the information content that they generate.

B. *Objectives and Hypothesis*

The major objective of this study is to establish the alignment that exist between the location of rogue mobile IT gadgets and the information content that they dispatch. Following are the derived specific objectives:

- To determine how rogue mobile IT gadgets behave;
- To express the nature of information rogue mobile IT gadgets contain;
- To develop a suitable mobile IT gadgets tracking method;
- To recommend on the tracking of the established relationship between the location of rogue mobile IT gadgets and the information that they originate.

The null hypothesis is that there is no alignment between the location of rogue mobile IT gadgets and the content of the information that they dispatch.

C. *Significance, and Paper Outline*

This study will significantly benefit various groups of people. Law enforcement agents will be assisted with the improved body of knowledge derived and increase in the returns of their primary roles; network vendors will improve the security of their networks and achieve greater customer satisfaction; and the nation will benefit through the suppression of money laundering activities leading to better national development.

The remaining part of this paper contains literature review on rogue mobile IT gadgets behaviors and the nature of information content that they derive, in order to unmask a deeper understanding of the origins of this study; the study methodology applied and data analysis methods used.

III. LITERATURE REVIEW

Scholars assume the possible existence of a relationship between the behavior of mobile IT gadgets and the content of information that they generate. Genuine and authentic users are likely to remain stable, while those that derive rogue information most probably have reason enough to become jittery and think of changing locations in order to avoid possible identification by their victims and law enforcement agents. [6] say that the absence of wired link makes it easier to cheat on identities: being untethered, the attacker can more easily impersonate a legitimate user.

A. *Determining How Rogue Mobile IT Network Gadgets Users Behave*

It is assumed that rogue users of mobile IT networks behavior in a unique manor, primarily because they are willing offenders of the law. According to [26], not only can people send false information to our gadgets, they can also obtain personal data from us without our knowledge (Available at https://books.google.co.zw/books, Accessed 07/11/2016). It is evident that these are practices that are undertaken on purpose and usually well planned beforehand. It gives the perpetrator all the reasons and room to organize and execute his/her escape plan. [4] says that the increased attack on smartphones is attributed to the huge sales that smartphones make over personal computers which implies there are a lot of potential victims out there which appeals to cybercriminals, who see more potential victims as more opportunities to exploit. This is an indication that such behavior is bound to increase in the future, a reason good enough for studies to be undertaken that focus on its determination.

B. *Expressing the Nature of Information Rogue Mobile IT Gadgets Contain*

When the content of information that is generated by mobile IT gadgets raises ethical issues, it becomes the reason behind their classification as rogue. [8] says that one might suggest that ethical problems occur when one or more of the following are deemed to have occurred: the tactics used to secure information are questionable since they appear to go beyond what might be deemed acceptable, ethical, or legal business practice; the nature of the information sought can itself be regarded as in some way private or confidential; and the purpose for which the information is to be used are against the public interest. A single data breach can cost an organization extensive loss in profits and reputation [13]. Examples of such practices that originate from network terminals are cases of industrial espionage; identity, data and finances theft; denial of service; and misrepresentation, which stifle data integrity and security, putting into doubt users'

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

reliance towards privacy and trust. [2] note that there have been instances of identity and data theft crimes involving millions of debit and credit card numbers, which indicate the seriousness of this issue and reinforce the concerns of security professionals.

C. Establishing the Relationship Between the Location of Rogue Mobile IT Gadgets and the Information that They Generate

Since the information that mobile IT gadgets generate is likely for some particular purpose, it ought to have some correlation with the location behavior of the gadget user. While these network gadgets provide new opportunities for interaction and socialization among users, the overwhelming amount of information generated, exchanged, and redistributed by users demands the adoption of new tools and techniques to search, analyze and secure online data [9]. [24] concurs, saying that media convergence is more than simply a technological shift, but alters the relationship between existing technologies, industries, markets, genres, and audiences.

Literature shows that a number of studies have been undertaken in the nature of information that originate from the so called rogue mobile IT gadgets, as well as the way they behave. However, no attempt has been made to try and find establish and make use of the relationship between the two parameters. This study has endeavored to address the missing link, determining the correlation between the two constructs, in order to produce a model that can be used in enhancing security in mobile IT devices. The study is guided by the conceptual framework in Figure 1 below and the research methodology discussed in the next part.

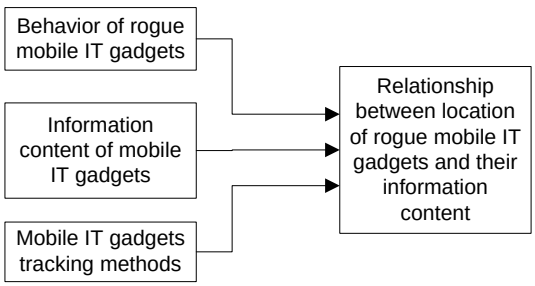

Fig. 1: Conceptual framework.

IV. METHODOLOGY

The purpose of this study was to establish the existence and strength of the cause and effect relationship between the two groups of variables. It was seeking to derive a confirmatory relationship that exist in rogue mobile gadgets location behavior and information content, through situational searches and in-depth interviews. The null hypothesis that it set out to prove was that there is no alignment between the location of rogue mobile IT gadgets and their information content.

Research design, philosophy and strategy

According to [27], a research design is the logical sequence that connects the empirical data to the study's initial research questions and ultimately to its conclusions. Such an explanatory study required a quantitative approach because it needed to establish figures and numbers that explicitly determine the relationships being sort after, for the conclusiveness of the study. [23] say that studies that establish causal relationships between variables may be termed explanatory research, whose emphasis is on studying a situation or a problem in order to explain the relationship between variables. The findings were expected to be confirmatory for management decision making purposes. A quantitative research is best achievable by using a positivist approach, because of the requirement for quantifiable observations that bring out figures and numbers in their raw state to explain the determined levels. Such a paradigm made the findings become objective by minimizing and/or eliminating subjective influences of any particular respondent(s).

Additionally, the study required to establish a deeper understanding in the opinions and experiences of respondents in the relationship between the location and information content of rogue mobile IT gadgets. It was for this reason, to help further understand the nature of the relationship that led it into adopting an exploratory design. An exploratory study is a valuable means of finding out 'what is happening; to seek new insights; to ask questions and to assess phenomena in a new light' [22], particularly useful if you wish to clarify your understanding of the problem, such as if you are unsure of the precise nature of the problem. This was achieved by the involvement of the opinions of the most relevant mobile IT network participants such as vendors, operators and other users. These were found to be well placed by their day to day experiences and challenges as they engaged the network services. It required a qualitative approach to the investigation. According to [20], qualitative designs or approaches have been seen by their advocates as being especially good for impact analysis and have been advocated primarily in conjunction with other evaluative functions such as implementation analysis, process and community self-analysis, and understanding of experiences. A qualitative research therefore provides insights into the problem and is also used to uncover trends in thoughts and opinions, and dive deeper into the problem. Combining both the qualitative and quantitative approaches therefore, a triangulation method was applied.

The study adopted a multiple-case study strategy, using a questionnaire. Case-study design is appropriate for investigation of highly-contextualized phenomena that occur within the social world [3]. The multiple-case technique was necessary for providing different respondents the opportunity to participate on an equal footing, with various sources of information, in order to draw a single set of "cross-case" conclusions by incorporating their differing views for validity and relevance purposes. Any other strategy would not have been able to satisfy these requirements. Other strategies such as experiments, observations and interviews that are of a purely subjective nature would not have been as suitable. Although their results could also have been conclusive, their major short coming was the absence of unhindered participants' responses which were important in establishing the causal effects between the variables in such a research.

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

A. Population and Sampling Procedure

[17] Says that with the current widespread of the internet, issues of security have now become pertinent in various companies. The widespread use of the mobile networks in the previously financially excluded sections of societies also expanded the interested parties to the research. It brought about a 'mushrooming' of mobile IT gadgets users, making a phenomenal increase to the population size of such a study. These happened to be ordinary cellular phone users, electronic airtime and electricity tokens vendors, money transfer traders, e-banking agents, e-commerce operators, etc.

In order to produce proper representativeness of the large target population, it was deemed necessary to apply judgmental sampling method in selecting a suitable sample for the required minimum of 50 informants. [7] says that purposive or judgmental sampling is an improvement on convenience sampling in that the researcher applies his/her experience to select cases which are, in the researcher's judgment, representative or typical of the relevant population. From the available mobile IT users in the country, the researcher applied his knowledge (on the basis of individual educational level of potential respondents) in selecting those that were deemed most suitable for participating in the study, in order to ensure reliability of the information provided.

B. Data collection and Research Instruments

For data collection method, the study favored the questionnaire in gathering primary data, mainly because of its ability to provide a record of raw information as evidence. The researcher dispatched the prepared and modified research instrument to the 50 respondents individually, and later collected the completed questionnaires by appointment after a period of three days. The method was complemented by triangulated observations from the researcher, wherever possible.

The questionnaire used was composed of both structured, and close and open-ended questions. These were able to address the respondents' knowledge, experiences and proposals in all the identified variables of the study.

C. Validity, Reliability and Data Analysis

For the purpose of ensuring obtaining findings that would be of high value, the researcher dissociated the influence of his own opinion from the derived responses. It was achieved by absenting himself from the respondents during their completion of the questionnaires, in order to secure their independence of influence from 'convenient responses'.

The suitability of the instrument used was enhanced by the involvement of a few experts in mobile security matters during its development and modification. It was piloted before use, to obtain its consistency, by the calculation of Cronbach's Alpha coefficient, whose threshold of 0.7 was deemed to ascertain internal consistency amongst the variables. Separate respondents from those targeted for the research were approached for instrument pilot testing, to avoid influencing the eventual responses for the study.

For data analysis, SPSS statistical package was used. Descriptive statistics to establish the frequency distribution of the respondents; and correlation for direction, statistical significance and magnitude of relationship of the pairs of variables were performed. Regression analysis was applied to determine the predictive power of the constructs onto the dependent variable.

V. Presentation and Discussion of Results

SPSS 16.0 statistical package was applied in analyzing the gathered quantitative data and established the frequency distributions of the different parameters of the respondents, correlation between the various study constructs, model summary and the individual contributions of the various independent variables to the model. The statistical significance of the independent variables' contributions plus the entire established model were also determined. This was meant to confirm the authenticity of the respondents that participated and the strength/reliability/dependability of the established model.

"Qualitative analysis transforms data into findings. No standard formula exists for that transformation" [21, p.432]. The researcher employed spatially-compressed, organized display modes, called data display tables and detailed write-ups, as recommended by [19]. The approach is called constant comparative analysis, a strategy that involves taking one piece of data (one interview, one statement, one theme) and comparing it with all others that may be similar or different, in order to develop conceptualizations of the possible relations between various pieces of data [25].

The approach summarized the gathered qualitative responses in a comparative process that led into the establishment of similarities, differences and scaling of the accounts of the respondents, classified according to the type/class/position of the informants, in order to map up the results derived from the gathered information. The technique helped the researcher in comparing and contrasting the accounts and opinions of the different respondents, by posing analytical questions and generating knowledge about common patterns and themes within and across the different cases.

A. Demographics

Table I below shows that from the 50 respondents that were involved, 34 were male and 16 female.

TABLE I. Frequency distribution for Gender.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	34	68.0	68.0	68.0
	2	16	32.0	32.0	100.0
	Total	50	100.0	100.0	

The following table II shows the distribution of the ages of the respondents. The results indicate that the largest (40%) of the respondents were in the 26-35 year age group, followed by the 36-45 years at 28%, 20-25 years at 24%, and 46-55 years at 8%. This demonstrates that the study involved the most active age groups in mobile technology issues, which goes on to validate its findings.

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

TABLE II. Frequency distribution for ages.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	12	24.0	24.0	24.0
	2	20	40.0	40.0	64.0
	3	14	28.0	28.0	92.0
	4	4	8.0	8.0	100.0
	Total	50	100.0	100.0	

Table III below gives the distribution of the current positions of the respondents in their declared status in respect to mobile IT networks. It shows that the study mostly attracted mobile network customers (users) with the largest (30 out of 50) count, followed by the different vendors at 5 out of 50 each. This may be attributed to the amount of concern that individual users attach to the losses that they personally incur whenever they get duped by these rogue mobile IT network gadgets. They are highly driven into serious searches for remedies, hence the interest demonstrated.

TABLE III. Frequency distribution for positions.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	30	60.0	60.0	60.0
	2	5	10.0	10.0	70.0
	3	5	10.0	10.0	80.0
	4	5	10.0	10.0	90.0
	5	3	6.0	6.0	96.0
	6	2	4.0	4.0	100.0
	Total	50	100.0	100.0	

Following is table IV that shows the distribution of the academic qualification of the respondents, indicating that the researcher made a deliberate effort to involve respondents with high academic qualifications. This was meant to secure enriched responses that come from knowledgeable people and avoid poor responses from uneducated individuals. It also helped in validating the obtained findings. The same information is also displayed in the following Figure 2.

TABLE IV. Frequency distribution for qualifications.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	12.0	12.0	12.0
	2	11	22.0	22.0	34.0
	3	11	22.0	22.0	56.0
	4	11	22.0	22.0	78.0
	5	11	22.0	22.0	100.0
	Total	50	100.0	100.0	

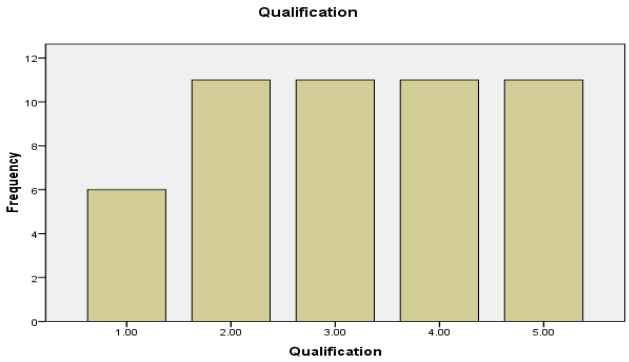

Fig. 2. Frequency distribution for Qualifications.

TABLE V. Correlation matrix.

			MITG_behavior	RMITG_infor_content	MITG_tracking	Rel_btwn_MITG_loc_n_info_cont
Spearman's rho	MITG_behavior	Correlation Coefficient	1.000	.284*	-.059	.019
		Sig. (2-tailed)	.	.046	.684	.893
		N	50	50	50	50
	RMITG_infor_content	Correlation Coefficient	.284*	1.000	.382**	.252
		Sig. (2-tailed)	.046	.	.006	.077
		N	50	50	50	50
	MITG_tracking	Correlation Coefficient	-.059	.382**	1.000	.561**
		Sig. (2-tailed)	.684	.006	.	.000
		N	50	50	50	50
	Rel_btwn_MITG_loc_n_info_cont	Correlation Coefficient	.019	.252	.561**	1.000
		Sig. (2-tailed)	.893	.077	.000	.
		N	50	50	50	50

*. Correlation is significant at the 0.05 level (2-tailed).
**. Correlation is significant at the 0.01 level (2-tailed).

B. Variables

Table V that follows is a correlation matrix that shows the direction and strengths of the relationships amongst the independent and dependent variables. The results indicate the absence of multi-co linearity (correlation between the predictors is less than 0.7); and all of them are somehow correlated (positively or negatively) with the dependent variable. It is an indication that most of the independent variables studied are important in the determination of the relationship being sort after. Such results are in agreement

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

with earlier researchers such as [14, 15, 1, 13, 2]. User behaviors, position location technologies, changing physical locations and the rich networks information content have exposed the unorthodox exploitation of mobile IT gadgets, attracting the need to closely establish the pattern of functional relationship between the variants. However, only mobile IT network gadgets (MITG) tracking is evidently statistically significantly correlated to the dependent variable at the 0.01 level. This means that its variation do affect the relationship between MITG location and their information content. The behavior of MITG was found to be statistically insignificantly (sig. = 0.893 > 0.05) correlated. This is probably due to the fact that the behavior varies from user to user, and therefore remains un-deterministic.

TABLE VI. Model Summary[b].

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.541[a]	.292	.191	1.469	.292	2.892	3	21	.059

a. Predictors: (Constant), MITG_tracking, MITG_behavior, RMITG_infor_content
b. Dependent Variable: Rel_btwn_RMITG_loc_n_info_cont

Table VI below shows the obtained model summary, the simple linear regression goodness of fit. This means that the model produced from the studied variables is a good predictor (R = 0.541 = 54%) of the relationship between the location and information content of MITG, with a very small amount of inaccuracy (Std. Error of Estimate = 1.469). The behavior of MITG, information content of rogue MITG and the tracking of MITG explain 29% (R square = 0.292) variance in the dependent variable. The other 73% therefore is explained by other factors that are outside the scope if this study.

For statistical significance of the established model, table VII below displays an Anova table results. The p-value is less than 0.05 (sig. = 0.02), indicating that the model has statistical significance and does a good job in predicting the outcome rather than by chance.

TABLE VII. ANOVA[b].

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	705.692	3	235.231	5.614	.002[a]
	Residual	1927.588	46	41.904		
	Total	2633.280	49			

a. Predictors: (Constant), MITG_tracking, MITG_behavior, RMITG_infor_content
b. Dependent Variable: Rel_btwn_MITG_loc_n_info_cont

TABLE VIII. Coefficients table.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.877	2.074		1.388	.172
	MITG_behavior	.017	.265	.009	.064	.949
	RMITG_infor_content	.017	.587	.004	.028	.978
	MITG_tracking	1.005	.275	.516	3.652	.001

a. Dependent Variable: Rel_btwn_MITG_loc_n_info_cont

To show the individual contributions of the different independent variables is table VIII that shows the coefficient table. It shows that MITG tracking provide the largest (B = 1.005) and statistically significant (sig. = 0.01 < 0.05) unique contribution, while the other variables make statistically insignificant (sig. > 0.05) unique contributions.

Identified suggestions and proposals for eliminating the scourge

This section presents the suggestions identified by the respondents, from their experiences, as remedial actions towards eliminating the problem through tracking the established relationship and protect genuine network users from rogue mobile IT gadgets.

Question 1.3: What makes you think the behavior of rogue mobile IT gadgets is (isn't) usually the same?

Table IX below shows a summary of the responses received.

TABLE IX. Why the behavior of rogue mobile IT gadgets is (isn't) usually the same.

Case 1	**Response**
Customers (Users)	- It is, because of common egoist intention of harming the public and targeted individuals x 4. - It is not, because it depends of the particular user's intentions x 2. - It is, because the gadgets used are capable of running the same applications x 7. - It is not, because of the different applications in the different gadgets x 9.
Case 2	**Response**
Vendors (Airtime and e-wallet)	- It is not, because they are used for different purposes x 5. - It is, because they are never stable in their locations x 1. - It is not, because some are always improving on their tactics x 1.
Case 3	**Response**
Operators	- It is not, because it depends on the intentions such as hacking for private information or destroying the system all together x 1. - It is not, because it varies with the gadget model and application being used x 3.
Case 4	**Response**
Shareholders (Owners)	- It is not, because of the different brands of gadgets being used x 2.

Equal numbers of respondents in Case 1 gave opposing views, while the majority in other cases said the behavior is not the same. The major reason advanced for the varying behavior is the differences in the types/brands/models of gadgets and software applications being used which determine the different purposes and/or intentions.

Question 2.5: What kind of rogue information have you experienced from such gadgets?

A resume of the responses obtained is presented in the following table X.

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

TABLE X. The kind of rogue information experienced from such gadgets.

Case 1	**Response**
Customers (Users)	- Unsolicited messages (commercial and/or explicit pop up) x 3. - Application capable of stealing user information x 1. - Over charging on services obtained x 10. - Bank account withdrawals x 1. - Denial of service by failing to access services x 2.
Case 2	**Response**
Vendors (Airtime and e-wallet)	- Fake cash notes transaction x 1. - Spam and copy-cat applications x 1. - Interrupted connection while in the middle of a transaction x 6.
Case 3	**Response**
Operators	- Illegal accessing and changing social network account details x 1. - Unfixed (wrong) transacting charges x 3.
Case 4	**Response**
Shareholders (Owners)	- Hacking x 1. - Exorbitant transaction charges x 2.

All cases presented overcharging as the main remedy experienced. For some it came about as a result of repeated charging due to repeated transactions after repeating interrupted connections, while others – explicitly wrong transaction charges.

Question 3.6: Which method did you implement (suggest) to protect yourself from the recurrence of such an incident?

A summary of the respondents' indicated methods are provided in Table XI.

TABLE XI. The method implemented (suggested) to protect from recurrence of such an incident.

Case 1	**Response**
Customers (Users)	- Attaching both personal ID number and biometric details to mobile IT gadgets x 2. - Fingerprint scanning x 5. - Tracking x 1. - Attaching personal information to gadgets x 7. - Attaching other information, e.g. email and bank details to gadgets x 2.
Case 2	**Response**
Vendors (Airtime and e-wallet)	- Attaching personal information (ID) to gadgets x 5. - Stick to transacting only with familiar gadgets only x 1.
Case 3	**Response**
Operators	- Attaching personal information (ID) to gadgets x 3.
Case 4	**Response**
Shareholders (Owners)	- Continuous training of users on the use and importance of passwords handling x 1. - Withholding of personal details (ID, bank details, fingerprints and/or email) after every transaction x 2.

Attaching personal details to gadgets featured as the common recommendation in all the cases. Case 4 however added the importance of strictly capturing those details at every transaction, ostensibly for use in the later identification of the gadget whenever necessary

Question 4.6: What do you think could be the challenge in the maintenance of the alignment between the location of rogue mobile IT gadgets and the information that they dispatch?

The obtained responses were summarized in Table XII below.

TABLE XII. The challenges in the maintenance of the alignment between the location of rogue mobile IT gadgets and the information that they dispatch.

Case 1	**Response**
Customers (Users)	- Unavailability of easy access to technologies that discourage such practices x 3. - Availability of unregistered gadgets on the networks x 2. - The operation of inadequately controlled networks x 13.
Case 2	**Response**
Vendors (Airtime and e-wallet)	- Their constant and uninterrupted and untraceable mobility x 1. - Absence of prior clearance of gadgets by network providers x 1. - Absence of efficient mobile networks call centers x 5.
Case 3	**Response**
Operators	- Absence of efficient mobile networks call centers x 2.
Case 4	**Response**
Shareholders (Owners)	- Absence of an efficiently resourced law enforcement agent to fight the scourge x 2.

Case 1 attributes the unreliability of the networks, Case 2 and 3 – absence of efficient mobile network call centers, and Case 4 – absence of an efficiently resourced law enforcement agents to fight the scourge. All these challenges point to the need to produce a suitable approach for addressing the vise, drawing the attention of all stakeholders – users, vendors and operators.

C. Recommendations

From the captured results, the researcher recommended that in order to adequately address the problem of RMITGs, it is necessary to invest in the production and functionality of a MITGs software application that establishes their changing locations in real time. The application will be used in the production of a database that will be handy in determining the location of every MITG whenever necessary.

VI. CONCLUSIONS

These results reject the null hypothesis, in favor of the alternative hypothesis that there is an alignment between the location of rogue MITG and the information that they dispatch. The behavior of rogue MITG, the nature of information that they contain and their tracking method have a bearing on the relationship between their location and the information that they originate. Presented in a Coeb Douglas formula, the established model adopts the following equation which shows the predictive power of the studied variables onto the alignment being sort after:

Relationship between RMITG location and their information content = 1.005 MITG tracking + 2.877.

To conclude, this study has contributed in the determination of the alignment between the location of rogue mobile IT network gadgets and the information content that they dispatch. The more and/or better are the tracking methods applied, the better becomes the endeavor to establish their location.

The researcher however proposes that further studies can be pursued on the subject matter. These could focus on other factors such as designing the actual befitting RMITGs tracking applications that take into cognizance all their established

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.

factors such as mobility, varying behaviors and rich information content.

REFERENCES

[1] P. Aditya, B. Bhattacharjee, P. Druschel, V. Erdélyi, and M. Lentz, "Brave new world: privacy risks for mobile users," In *Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments*, pp. 7-12, ACM, 2014.

[2] S. Ahmad, D. Winchester, L. Land, and R. Jamieson, "Nature and extent of identity crime through wireless technology abuse and its impact on individual and organizational levels," *International Conference on Information Resources Management (CONF-IRM)*, pp. 1-11, 2010.

[3] A. F. Almutairi, G. E. Gardner, and A. McCarthy, "Practical guidance for the use of a pattern-matching technique in case-study research: A case presentation," *Nursing & Health Sciences*, vol. 16(2), pp. 239-244, 2014.

[4] E. Asamoah-Okyere, "The changing face of Cybercrime: How mobile devices have changed the approach to committing cybercrime," 2014.

[5] S. I. Augustine, "Communication style in the information age," *Corporate Communications: An International Journal*, vol. 6(4), pp. 199 – 204, 2001.

[6] L. Buttyan, and J. P. Hubaux, "Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing," *Cambridge University Press*, 2007.

[7] R. Y. Buyya, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future generation Computer Systems*, pp. 599-616, 2009.

[8] A. Crane, "In the company of spies: When competitive intelligence gathering becomes industrial espionage," *Business Horizons*, vol. 48(3), pp. 233-240, 2005.

[9] A. M. De Paula, "Security aspects and future trends of social networks," In *Proceedings of the Fourth International Conference of Forensic Computer Science*, pp. 66-77, 2009.

[10] C. Edwards, "Mobile gadgets catch the dreaded lurge," *IEE Review*, Jan 2005, vol. 51, issue 1, pp. 26-27, 2005.

[11] R. Gazan, Understanding the rogue user, *Information and Emotion: The Emergent Affective Paradigm in Information Behavior Research and Theory. Information Today*, pp. 177-185, 2007.

[12] A. K. Gosh, and T. M. Swaminatha, "Software security and privacy risks in emerging payments markets: A case study of Zimbabwe," 2001.

[13] G. S. Kearns, "Countering Mobile Device Threats: A Mobile Device Security Model," *Journal of Forensic & Investigative Accounting*, vol. 8(1), 2016.

[14] A. C. Kooser, Rogue Links, *Entrepreneur*, vol. 34, Issue 6, pp. 36-36, 2006.

[15] P. Krishnamurthy, "Position location in mobile environments," In *NSF Workshop on Context-Aware Mobile Database Management (CAMM)*, 2002.

[16] M. Mago, "An evaluation of the importance of security in mobile Information Technology gadgets," 2016.

[17] M. Mago, T. Matekenya, and D. Madzikanda, "Determining ICT Impediments to the Success of Mobile Financial Transactions in Rural Zimbabwe," *International Journal of Research in Information Technology*, vol. 4(7), pp. 22-39, 2016.

[18] T. Mantoro and C. Johnson, "Location history in a low-cost context awareness environment," In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, vol. 21, pp. 153-158, Australian Computer Society, Inc., 2003, January.

[19] M. B. Miles and A. M. Huberman, "Drawing valid meaning from qualitative data: Toward a shared craft," *Educational Researcher*, pp. 20-30, 1984.

[20] L. Mohr, "The qualitative method of impact analysis." *American Journal of Evaluation*, vol. 20(1), pp. 69-84, 1999.

[21] M. Q. Patton, "Two decades of developments in qualitative inquiry a personal, experiential perspective," *Qualitative Social Work*, 1(3), pp. 261-283, 2002.

[22] Robson. A critical discussion of research methods and approaches, The WritePass Journal, 2002.

[23] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, fifth edition, 2009.

[24] J. A. Scott, "Politics and Paradigms: Conservatism and Media Convergence," *The Challenge: The Divided Conservative Mind*, pp. 399, 2012.

[25] S. Thorne, "Data analysis in qualitative research," *Evidence Based Nursing*, 3(3), pp. 68-70, 2000.

[26] R. Vamosi, *When Gadgets Betray Us: The Dark Side of Our Infatuation with New Technologies*, Basic Books, *2011*.

[27] R. K. Yin, *Case Study Research, Design and Methods*, Fourth Edition, vol. 5, 2009.

Maxwell Mago, "Evaluation of the alignment between the location of rogue mobile information technology (IT) gadgets and the nature of information that they dispatch," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 136-143, 2017.