Computational Robotics: An Alternative Approach for Predicting Terrorist Networks

E.M. Nwanga[1], K.C. Okafor[2,*], G.A. Chukwudebe[1] and I.E. Achumba[1]

[1]*Dept. of Electrical & Electronic Engineering Federal University of Technology, Owerri, Nigeria*

[2]*Dept. of Mechatronics Engineering, Federal University of Technology, Owerri, Nigeria*

Abstract: Increasing terrorist activities globally have attracted the attention of many researchers, policy makers and security agencies towards counterterrorism. The clandestine nature of terrorist networks have made them difficult for detection. Existing works have failed to explore computational characterization to design an efficient threat-mining surveillance system. In this paper, a computationally-aware surveillance robot that auto-generates threat information, and transmit same to the cloud-analytics engine is developed. The system offers hidden intelligence to security agencies without any form of interception by terrorist elements. A miniaturized surveillance robot with Hidden Markov Model (MSRHMM) for terrorist computational dissection is then derived. Also, the computational framework for MERHMM is discussed while showing the adjacency matrix of terrorist network as a determinant factor for its operation. The model indicates that the terrorist network have a property of symmetric adjacency matrix while the social network have both asymmetric and symmetric adjacency matrix. Similarly, the characteristic determinant of adjacency matrix as an important operator for terrorist network is computed to be -1 while that of a symmetric and an asymmetric in social network is 0 and 1 respectively. In conclusion, it was observed that the unique properties of terrorist networks such as symmetric and idempotent property conferred a special protection for the terrorist network resilience. Computational robotics is shown to have the capability of utilizing the hidden intelligence in attack prediction of terrorist elements. This concept is expected to contribute in national security challenges, defense and military intelligence.

Keywords: Robotic automation, Computational science, Counterterrorism, Network adjacency matrix.

1. INTRODUCTION

Computational Robotics (CR) refers to the use of predictive mathematical, and algorithmic constructs to seamlessly drive robotic agents for actionable intelligence based on complex datasets available. In terrorized locations, there is the need to understand the hidden model of criminal network behavior using CR and its agents for the aggregation of informative datasets.

The spate of organized criminal attacks in the world has been on the increase in the last few years and has posed the greatest threat to the societies across the globe. In the same range, Nigeria has experienced a lot of this organized criminal attacks by Boko - Haram (BH), Herdsmen and most recently the unknown gunmen (UGM). The aforementioned organized criminal group have been known to engage in kidnapping for ransom, abduction and raping, destruction of lives and property. These hidden activities of the terrorist element is difficulty to predict, trace and detect. Thus, the deployment of a computational intelligent agent (Robot) becomes imperative. This intelligent agent is capable of undertaking a remote surveillance mission of the clandestine activities of the group without their knowledge [1-2].

These groups constitute violent criminal attacks of state and non-state actors in their covert and overt interdependence [3]. It has the highest negative social and economic consequence to any nation as it hinders the economic development of any nation and degrades its gross domestic products [4]. Attacks of terrorist have great lethal and destructive impact on every nation in economic terms of lives and property. The recent successes recorded by the terrorist elements in many nations have been attributed to lack of actionable intelligence that would have enabled predictive and detective actions against them [5-6].

Hence, the traditional command and control techniques of tackling criminality has become ineffective [7]. In the wake of the present terrorist incidents in the world, a paradigm shift is necessitated to data - driven mindset via actionable intelligence. Then a transistion from the traditional method of “Sense and Response” (SaR); the command and control techniques to modern dimension of “Predict and Prevent” (PaP*)* using computational intelligence becomes vital with a novel computational robot.

Processing of intelligence/information within the organized terrorist networks to discover hidden links and structures is paramount for any successful

*Address correspondence to this author at the Dept. of Mechatronic Engineering, Federal University of Technology, Owerri, Nigeria;
Tel: +273-9094945960; E-mail: kennedy.okafor@futo.edu.ng

counterterrorism. The clandestine nature of the network makes it difficult to be detected [8], but these could be possibly detected through application of computational approach on the hidden links (HLs) [9-10]. This enables proper analysis of the terrorist adversaries' goals and intentions and further reveals new information about entities within the network. Every terrorist networks consist of interconnected criminal states (CS) in their covert nature [11], active internal communications (AIC), time frame of attack (TFA) and mapped states (MS) [12]. The criminal state is made up of Commander *(Cd),* Gatekeeper *(Gk)* and Foot-Soldiers *(Fs).*

Understanding the complex dynamics of terrorist network offers a great deal of probability of detection [13]. Computational intelligence for counterterrorism provides the structural and hierarchical knowledge of terrorist networks [14]. This approach is applied with Hidden Markov Model (HMM) for the purpose of surveillance and analysis. This is based on its stochastic and tractability with a data - driven architecture and could fuel smart security initiative to combat terrorism and other organized criminal networks syndicate [15].

According to Saini & Sunila Godara, (2014) [16], Hidden Markov model (HMM) is a partially hidden Markov Chain. The Markov Chain Model defines mathematical model for predicting the future state depending only on the current state [17-18]. HMM establishes finite set of states, each of which is associated with a probability distribution. Transitions among these states are governed by a set of probabilities called state transition probabilities [19]. In a particular state, an outcome or observation can be generated, according to the associated probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model [16, 19]. Terrorist activities is a time series event and occurs in two stages; that is planning and execution stages. It is pertinent to apply HMM based on its relative mathematical ease of immense versatility which makes it suitable for use as a stochastic process in the analysis of terrorist records [20].

Considering the various research capabilities of HMM, this work is motivated to introduce a computational constructs to analyze the behavior of terrorist elements using intelligent surveillance agents.

This paper contributes to knowledge by providing the network relational intelligence within the terrorist networks through computation of the network adjacency matrix using artificial agent (robot). Thus, the aim of this research is to computationally characterize the process of modelling (by learning) how a proposed robotic surveillance framework executes a task for terrorist dissection in complex states/environments. It further provides some mathematical uniqueness of criminal networks from social networks that laid foundation for computational methods of counterterrorism.

From the generalized perspectives offered in this work, this paper will be approached from a distinct computational behavioral model. The model can offer reliable prediction of the behavioral pattern of terrorists in criminal networks.

The rest of the paper is organized as follows: Section 2 presents some existing research works on criminal (terrorist) networks, computational artificial surveillance agent, HMM for analysis of organized terrorist networks and computational approach to counterterrorism. Section 3 provides the methodology of the research. Section 4 presents and discusses the results and findings of the work. Section 5 concludes the paper and gives recommendations for future work.

2. LITERATURE REVIEW

2.1. Organized Terrorist Networks

There have been several studies on organized terrorist networks, Security surveillance system, Hidden Markov Model and computational approach to counterterrorism. Some of such recent literatures are reviewed and presented in this section. The work in, [21] presented the historical evolution of Boko Haram in Nigeria and stated the causes, recruitment, ideology, area of operation and the ways through which the problem can be solved. The authors further presented that more than six million Nigerians have been killed by this group while more than 300,000 people have been displaced. Similarly, [22, 11] discussed the threat of terrorism and the challenges in countering their operations on the set targets. They further stated that lack of a clear-cut counterterrorism strategy, dearth in technology and mutual trust between actors and locals in the management and utilization of intelligence were recommended as the major challenges for destabilizing the attacks of terrorism in Nigeria.

Lindelauf *et al*. (2011) [14] investigated the structural position of covert terrorist networks using secrecy versus information tradeoff characterization. The result shows that network structures are generally not small-worlds, in contrast to many overt social networks. This finding was backed by empirical evidence concerning Jemaah Islamiyah's Bali bombing and a heroin distribution network in New York. Similarly, the work of [23] presented a Mathematical framework for examining the strength of terrorist structures. The model illustrated the strength of different terrorist cell structures using the partially ordered set (poset) of terrorist cells. Algorithms were presented to implement and examine the structures of posets of seven elements that were observed in their analysis. The authors finally, presented their findings and the applicability of their work for government strategic operations.

Farooq, Khan and Butt, (2017) [24], proposed a model for finding the correlation of communication contents of all nodes with data directory and detects nodes based on a threshold correlation value. New network was drawn and its density was calculated. Also, the centrality measures were applied on the new network that produced different key players with different roles in the network. Seidler *et al*. (2017) [25] opined that a visual analytics support analysts could aid in monitoring a dynamics of complex system, and the authors approach systematically mapped relations on the user interface.

Nguyen (2016) [26], discussed the application of HMM for computational intelligence with mathematical proofs. The report focused on the three common problems of HMM such as evaluation problem, uncovering problem, and learning problem, in which learning problem with support of optimization theory was the main subject. Brogi & Di Bernardino (2019) [27] described a HMM for the evolution of an advanced persistent threat (APT). The model was to validate whether the evolution of the partially reconstructed attack campaigns were indeed consistent with the evolution of an APT. The score obtained enabled the comparing of APT fit of different lengths and was validated with the score using data obtained from experts. Valleriani, Li and Kolomeisky (2014) [28] stated that Complex Markov models are widely used as powerful predictive tools to analyze stochastic processes. The authors derived a complete Taylor expansion of the first-passage time distribution between two arbitrary states for a general Markov model using a combination of algebraic methods and graph theory approaches. Yang & An (2020) [29] research revealed that critical nodes identification in complex networks was significant for studying the survivability and robustness of networks. The authors leveraged the property of structural hole to design a heuristic algorithm based on local information of the network topology. This was used to identify node importance in undirected and unweighted network, whose adjacency matrix was symmetric. In the algorithm, a node with a larger degree and greater number of structural holes associated with it, achieved a higher importance ranking. In another development, robot has also played its role in security and alike scenarios. Anandravisekar *et al.*, (2018) [30] developed an IoT enable surveillance robot for uncovering hidden terrorist activities within a specified location. The size of the developed IoT surveillance robotic model was huge and visible, as such not fit for asymmetric warfare (terrorism), in that it is visible for the terrorist elements. Similarly, Bokade and Ratnaparkhe, (2016) [31] used video surveillance robot for video streaming which was capable of capturing 15 frames of images per second but the size was also much visible for hidden elements.

Another application of security surveillance robot was in military base where it was used for defense and border control activities. It was designed to play a multiple function such as threat investigations and remote signal transfer, but was designed specifically for border area security control. This surveillance robot was limited by its coverage area and was configured with 3G network [32]. The borders' surveillance robotic approach of combating insurgencies were further validated by [33-34].

2.1. Computational Approach

Computational intelligence found valuable applications in robotics and in combating organized terrorized network as a cognitive informatics [35-36]. Hung, Jayasumana and Bandara, (2019) [37] used graph trajectory analytics to understudy terrorist patterns with application in security warfare and other asymmetric warfare. Tundis, Kaleem and Mühlhäuser, (2019) [38] developed strategic intervention means of fighting terrorism through the use of IoT app that utilized an edge computing approach. The authors used the model/algorithm. The main idea is to operationalize and implement the system.

Chen *et al.* (2018) [39] proposed the use of deep learning for smart security surveillance but was limited only on the face information and on the available data of the eyes' region. The experimental results of the research work demonstrated that the proposed method can predict the terrorist elements based on eye-data only. Consequently, the work of Sutton, Willett and Bar-Shalom, (2021) [40] presented a computational approach to terrorist network insurgency with Hidden Markov Model. Threat model of probabilistic sequence analysis was used by the authors and the result inferred data association steps on the perceived threat.

Saeidi and Wang, (2019) [41] predicted terrorist attacks with computational robotics-based genetic algorithm. The researchers concluded that a computation of the shortest optimal path is possible with their model. The robot was incorporated with a scissor lift mechanism to lift both objects and humans during insurgency warfare disaster, at 360° rotation and was further fitted with 6 degrees of freedom. Another work of Lippiello, Siciliano and Villani, (2013) [42] highlighted the use of Intelligent computational approach to counterterrorism with mobile robot. The overall challenges with the use of these computational methods are the difficulty in predicting the level of communication among the terrorist elements due to vast geographical distribution and their clandestine nature. In a swift addition, the methods applied are deficit in internal communication and countermeasures with lack of appropriate optimization technique for effectiveness of the prediction accuracy.

The gap from the literature reviewed has shown that the security surveillance robot in use were visible for the terrorist attack perpetrators. Furthermore, lack of terrorist network operating dynamics as behavioral model have contributed to the difficulty of the terrorist attack prediction. In this research, the complex dynamics of terrorist network will be modeled by HMM for computational intelligence in counterterrorism.

3. METHODOLGY

In this section, the work discussed a proposed framework for computational intelligence gathering for cloud analytics. The various stages that generate the computational intelligence via the computational robotic survelliance is represented in the conceptual model. In Figure **1**, the system generates network information within terrorist elements from intelligent surveillance robot (*i.e.*, computational robotic nodes). This then computes the mathematical network adjacency matric that exist among the elements of criminal network from massive data gathered. The computation was based on trend, sequence of communications and intelligence

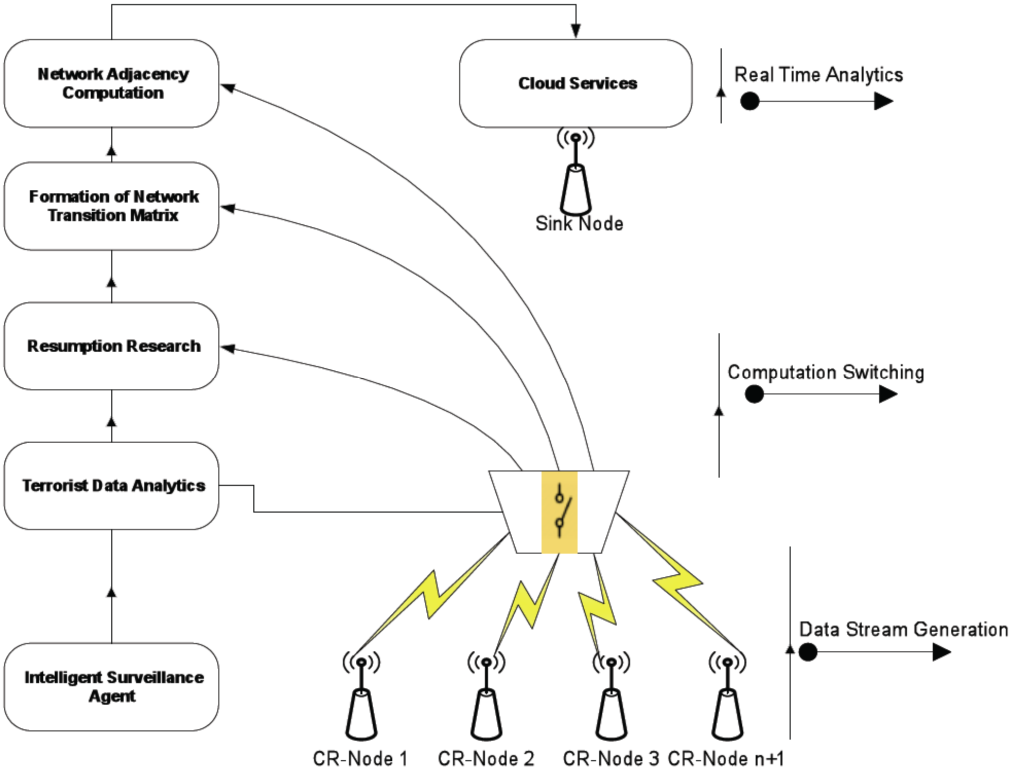

Figure 1: Framework for Computation Robotics Security Surveillance Architecture.

within the terrorist network. Due to the nature of terrorist elements and their activities, the data used in this study was collected from the global terrorism database (GTD) for the period of 2010 – 2016 [43]. The data contained the names of suspected criminal groups that carried out an attack, the targets of the attack, the target sub-type, description of the attack, geographic location of the attack among other events. The time frame of attack and terrorist states that carried the attacks were sieved out of the dataset and subsequently used to drive home some attack information (intelligence). The system architecture depicted in Figure **1** is made up of the following modules: Intelligent surveillance agent (ISA), Terrorist data analytics (TDA), Research assumption (RA), Formation of Network transition matrix (NTM), network adjacency matrix (NAM) and Cloud Services (CS).

From the computational perspective, the intelligent surveillance agent (ISA) is the phase I model. The role is to survey and gather threat information such as videos, pictures and audios within the attack vectors and attack payload. This data is transmitted for data analytics. Phase II Terrorist data analytics explains where the transmitted data from ISA is analyzed to sieve non-threat base information.

It further processes the security allies' data for intelligence generation and decision making. The research assumption module is very distinct in Phase III.

Clearly, every criminal network maintain high and low profile actors with the cross –ties emerging dormant after coordinated attack. The ergodic nature of terrorist network in space and time creates transition among the elements, with transitory shortcuts. This research assumption is made based on the criminal data analytics and the generated intelligence. There exist the network kingpin otherwise known as the commander *(Cd)*, the gatekeeper *(Gk)* and foot-soldiers *(Fs)* as the low profile actors. Therefore the hidden elements within the terrorist states H_s in eq. (1) is denoted as an association of three different nodes.

$$H_S = \left\{H_{Cd}, H_{Gk}, H_{Fs}\right\} \tag{1}$$

Then, how significant each node is as a conduit for information or influence becomes key and imperative. In a terrorist network, the strength of the network is the sequence of actions flowing from the commander to the foot soldiers. It is an ordered set or partially ordered set that measure the degree of the association of the hidden elements and the strength is represented in eq. 2. It is the sum of the contributions of the extreme elements.

$$S_\Psi = Fs + nCd \tag{2}$$

Where S_Ψ represent the strength of the network and n is the figure of merit that measures the weight of the commander and should be greater or equal to 1 ($n \geq 1$). This condition necessitated the following six (6) assumptions that guided the node classification, network formation and data analysis below.

1. There exist hidden active internal communication (AIC) in the network.

2. The flow of the communication is directed from the leader to the gatekeeper and from the gatekeeper to the foot-soldier.

3. There exist no feedback communication within the network.

4. The commander does not have any link with the foot-soldier in order to maintain a transitory shortcuts.

5. An attack always precede a particular active internal communication.

6. Commanding group and the gatekeeping group do not carry out suicide attack. Consequently only the foot-soldiers carry out suicide attacks which are usually masterminded by the *Cd* and *Gk.*

The existence of the states is now put to use in accordance with Hidden Markov Model (HMM) principles. Markov process is initiated since there is a possible step in movement of transition within the states. AIC originates from *Cd* to *Gk* and from *Gk* to *Fs*. A first order Markov Model is formed in eq. 3. In Hidden Markov Model, the future state depends only on the current state. That is, the probability of entering a certain state depends only on the last state and not on any earlier state.

$$p\left[s_{t+1} / s_t, ..., s_2, s_1\right] = p\left[s_{t+1} / s_t\right] \tag{3}$$

Where s_{t+1} is a state lower in rank in the terrorist network, given a next high state in rank with directional AIC.

Phase IV model is the formation of network transition matrix. This network transition matrix was formed base on the already developed terrorist network assumptions. In every terrorist network, there exist a transition within the networks due to changes in criminal state(s). The network transition matrix is a conditional probabilities that a criminal attack was carried out by *state j* given that an active internal communication was made by *state i*. It is the probability that the stochastic event (terrorist action) changes current states s_i to next state s_j. Statistically, the sum of the probabilities of transitioning from any given state to other next state is 1. The above statements are illustrated in eq. 4 and eq. 5.

$$p_{ij} = p\left({}^{s_i}\!/_{s_j} \right) \tag{4}$$

$$\forall s_i \in S, \sum_{s_j \in S} p_{ij} = 1 \tag{5}$$

The initiating state of the terrorist action is s_i, s_j is the execution state of the network, S represent the terrorist states variables and S the terrorist computational space.

The eq. 6, is used to represent the formation of the transition matrix of the terrorist network.

$$\begin{pmatrix} (CdCd) & (CdGk) & (CdFs) \\ (GkCd) & (GkGk) & (GkFs) \\ (FsCd) & (FsGk) & (FsFs) \end{pmatrix} \tag{6}$$

The transition matrix is then computed from the data obtained on the various attack traces of the terrorist elements using the above assumptions. Total of 269 attacks were observed for the period and the result is presented in Table **1** of section IV.

In Phase V, the framework depicts the Computation of network adjacency matrix. In this case, the importance of adjacency matrix in a criminal network is to dissect the dynamics of the network. It helps to determine the level of interactions and flow of command among the hidden elements of any terrorist network. It is a dependent factor in determining the secrecy and efficiency within the network operation and its resilience.

Generally, given a criminal network G in eq.7, an adjacency matrix A is formed in eq. 8.

$$G = (V, E) \tag{7}$$

Where V is the criminal (terrorist) elements while E is the AIC.

$$A_{ij} = \begin{cases} 1 \\ 0 \end{cases} \tag{8}$$

Here, $a_{ij} = 1$, if i is adjacent to j and 0, if i is not adjacent to j.

A node as a terrorist element is adjacent to another node if the two nodes share a common tie. In criminal network, on the bases of its nature and mission, there exist two levels of ties (relationship).

1. Relationship with criminal elements (actors) themselves
2. Relationship that each criminal element (actor) has with one another

In phase VI, the Cloud Services interface defines the brainbox of the solution set. The secured data generated by intelligent surveillance robot is been further analyzed to yield terrorist information for intelligence and stored in a secured private cloud infrastructure. The confidentiality, protection and availability of the data is ensured with this cloud services.

Algorithm I shows the design pseudo code depicting the computational robotic state procedures for the various phases discussed.

Algorithm I: CR Predictor Construct

```
Procedure: construct Graph (computational robotic agents (i,……i+1)
State. Parameters: commander (Cd), the gatekeeper (Gk) and foot-soldiers (Fs)
Input: pool phase. labels // Phase 1 to Phase 5.
Output: Cloud Services. graph structure ( )
Begin function ( )
initialize C Rgraph.phases ( )
for all CR ( ) do
    if Map (intelligence) > 0 then
        increase agents to CR
    end if
end for
```

```
for all (phase.labels) do
concatenate. all ( )
if phase. labels (1:5) < Asymmetric & Symmetric adjacency matrix then
increase agents to CR
end if
end for
end for
return CR
```

4. RESULTS AND DISCUSSION

In this section, the initial computational results obtained are shown in the Table 1 and 2. A total of 269 attacks were recorded for the period of 2010 to 2016 [44]. Table **1** presents the terrorist state attack statistics derived. It is shown that the commander *(Cd),* carried out a total of 6 attacks, gatekeeper *(Gk)* carried out 19 attacks and 244 attacks were done by the foot soldiers (Fs). This shows that the commander only carries out high profile and strategic attacks while gatekeeper and foot soldiers are both responsible for 97.8% of all the terrorist attacks that took place within the period. This further reveals that foot soldiers are more prevalent and vulnerable in every terrorist actions as seen in Figure **2**.

Table 1: Terrorist States Attack Statistics

State (i, j)	Frequency	Percent
Cd	6	2.2
Fs	244	90.7
Gk	19	7.1
Total	269	100

Considering the assumption of active internal communication within the network (AIC), Table **2** is generated with the terrorist network assumptions applied. The table presents the results of transitions of the terrorist hidden elements. The computation of the transition matrix as contained in Table **2** is based on the fact that the probability of entry a certain state in Markov chain depends only on the current state. This result shows a square matrix taking into cognizance the state dependence within the terrorist network. In network centrality, the importance score of a node (terrorist element) is the fraction of AIC made by the criminal element. It is assumed that all attacks are masterminded by the commander, thus having the highest centrality score of 269, followed by the gatekeeper with a centrality score of 263 and foot-soldier with 244. The result is used to compute the transition probabilities of the network in eq. 9 as a stochastic matrix. That is the matrix in which all the rows are nonnegative and all the rows sums up to 1.

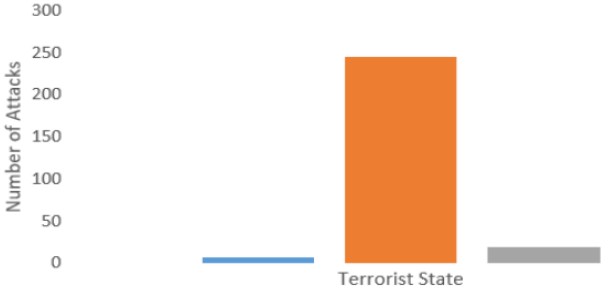

Figure 2: Attack per criminal state.

Table 2: Network Centrality Scores

State (i, j)	Cd	Gk	Fs	Total
Cd	269	19	0	288
Gk	263	263	244	770
Fs	0	244	244	488
Total				1546

Precisely the edge weights of the criminal network can be altered by changing the matrix appropriately [44]. Normalizing the rows of the network matrix and applying eq. 4 and eq.5, we obtained the result in eq. 9.

$$p_{ij} = p\begin{pmatrix} 0.934 & 0.066 & 0 \\ 0.3416 & 0.3416 & 0.3168 \\ 0 & 0.5 & 0.5 \end{pmatrix} \tag{9}$$

The result shows that the conditional probability of an attack by a commander given that AIC from the foot-soldier is 0 and conversely the same. This is because terrorist network maintained transitory shortcut to avoid been uncovered as internal communication between the leader and foot-soldier is completely avoided. The computation of the network adjacency matrix is done based on these analysis and is used to differentiate terrorist network from social network. The network adjacency symmetric matrix (sym) in eq. 10 is computed using eq.8 and eq. 9.

$$a_{ij}(sym)_{cn} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \tag{10}$$

It shows that the a_{ij} (adjacency matrix) of a terrorist network has its leading diagonal elements as 1's and is a symmetrical matrix (sym). This gives rise to the uniqueness of terrorist network as this study set to identify. Here, both the upper and lower half of the matrix are the same. Figure **3**, highlights the symmetric behaviors of terrorist network. Point 1, 2 and 3 at the X-axis represent the three elements of the network, the commander, gatekeeper and foot-soldiers respectively. It shows the existence of two ties in terrorist network. Thus terrorist network exhibits these unique properties of symmetric and idempotent. Idempotent accounts for the resilience in every organized criminal network and confers its ability to reorganize or regroup after external attack.

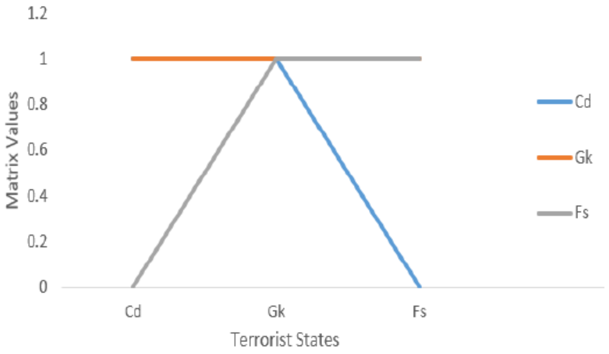

Figure 3: Symmetric adjacency matrix of terrorist network.

Social network has 0's along its diagonal since the ties of the social network actors with themselves are always ignored. An adjacency matrix of social network can be an asymmetric matrix (asym) or symmetric matrix (sym). In asymmetric matrix the top right half of the diagonal does not match the bottom left half. The symmetric and asymmetric adjacency matrix of the social network base on the above is represented in eq. 11 and eq. 12 respectively. Figure **4** and Figure **5**, respectively further illustrate the symmetric and asymmetric behaviors of social network elements. This shows that in social network, there is an existence of a single tie (*i.e.* the relationship between the social actors among themselves). In symmetric social adjacency matrix, both the network leader and the foot soldiers do not communicate despite the nature of ties in the network. While in asymmetric the leader does communicate with the foot soldiers.

$$a_{ij}(sym)_{sn} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad (11)$$

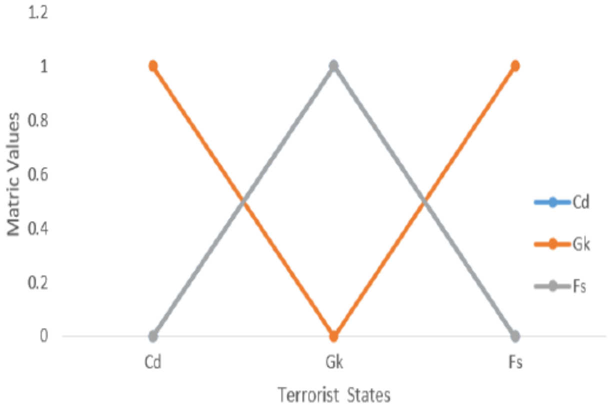

Figure 4: Symmetric adjacency matrix of social network.

$$a_{ij}(asym)_{sn} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad (12)$$

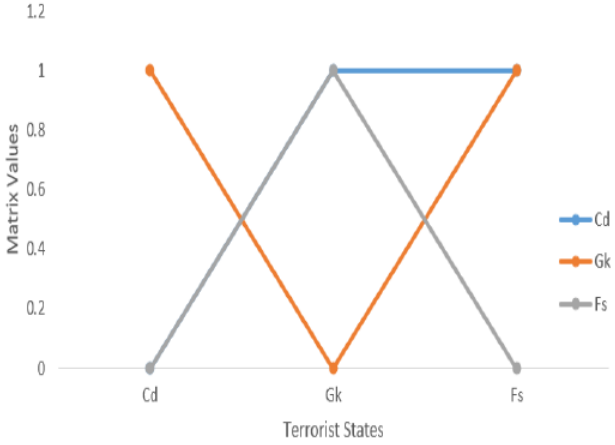

Figure 5: Asymmetric adjacency matrix of social network.

In the foregoing results, the nature of intelligence within the terrorist and social networks differs. Performing the classical analysis of the network matrix through row matrix (R- M) analysis and column matrix (C-M) analysis, the nature of information symmetries within the two networks will be clearly strengthened.

In terrorist network, adjacency matrix is symmetric $a_{ij}\langle sym\rangle_{cn}$:

$a_{ij}\langle sym\rangle_{tn}$ R - M analysis has Cd elements as (110), Gk has (111) and Fs has (011)

C - M analysis has Cd elements as (110), Gk has (111) and Fs has (011).

Social network has symmetric adjacency matrix

$a_{ij}\left\langle sym\right\rangle_{sn}$ and asymmetric adjacency matrix $a_{ij}\left\langle asym\right\rangle_{sn}$:

In $a_{ij}\left\langle sym\right\rangle_{sn}$, R-M analysis has Cd elements as (010), Gk has (101) and Fs has (010)

C – M analysis has Cd elements as (010), Gk has (101) and Fs has (010).

In $a_{ij}\left\langle asym\right\rangle_{sn}$, R-M analysis has Cd elements as (011), Gk has (101) and Fs has (010)

C – M analysis has Cd elements as (010), Gk has (101) and Fs has (110).

The analysis shows that row matrix and column matrix in symmetric adjacency matrix have the same values for both terrorist and social network elements. Further computation of the characteristic determinant of the symmetric and asymmetric matrix of the two networks gave these values: $\left|a_{ij}\left\langle sym\right\rangle_{tn}\right| = -1$, $\left|a_{ij}\left\langle sym\right\rangle_{sn}\right| = 0$ and $\left|a_{ij}\left\langle asym\right\rangle_{sn}\right| = 1$. The determinant value of terrorist network symmetric matrix was -1 and posit the complex connections and interactions among the criminal actors. Social network has 0 and 1 in the determinant value of its symmetric and asymmetric matrix respectively. The determinant value of 1 implies real and orderly pair of communication in social networks while the value of 0 shows non-existence of communication pairs (the leader and the foot soldiers do not communicate despite the nature of ties in the network). The use of field programmable gate arrays to achieve CR implementation is the next focus using a preliminary work in [45, 46].

5. CONCLUSION

This paper has applied Hidden Markov Model for a computational robotics based terrorist network surveillance analysis. The data acquired by the surveillance robot was used to determine the intrinsic behaviors of the terrorist elements within the context of their active internal communications and strategic alliance. The information symmetry was computed and analyzed which differentiate the terrorist network from social networks using classical matrix dimension. The network adjacency matrix computed from the network transition matrix shows that terrorist network exhibits special features from social networks. The results illustrated the uniqueness of terrorist network in making incessant attacks while remaining resilient after every perturbation. The study laid a good foundation to computational methods for counterterrorism and mathematical counterterrorism in the wake of the current terrorism globally. The work provides vital information and useful intelligence needed for proper understanding of asymmetric warfare. The result would be applied in developing a drone - based military intelligent agent for combating terrorism. Future work on this will focus on Hidden Markov based swarm optimization technique for computational robotics application in counterterrorism.

REFERENCES

[1] Sethuraman SC, Kompally P, Reddy S. VISU: A 3-D Printed Functional Robot for Crowd Surveillance. IEEE Consum. Electron Mag. 2021; 10(1): 17-23. https://doi.org/10.1109/MCE.2020.3029769

[2] Fong J, Ocampo R, Gross DP, Tavakoli M. Intelligent Robotics Incorporating Machine Learning Algorithms for Improving Functional Capacity Evaluation and Occupational Rehabilitation. J Occup Rehabil [Internet]. 2020; 30(3): 362-70. https://doi.org/10.1007/s10926-020-09888-w

[3] Andrew S, Bouhana N, Malthaner S, Schuurman B, Lindekilde L, Thornton A, *et al*. Lone-actor terrorism. In: Routledge Handbook Of Terrorism And Counterterrorism. 2018. https://doi.org/10.4324/9781315744636-10

[4] Gao Y, Wang X, Chen Q, Al. YG *et al*. Suspects Prediction towards terrorist attacks based on machine learning. 2019; 10. https://doi.org/10.1109/BigDIA.2019.8802726

[5] Budur E, Lee S, Kong VS. Structural Analysis of Criminal Network and Predicting Hidden Links using Machine Learning. 2015.

[6] Taha K, Yoo PD. Using the spanning tree of a criminal network for identifying its leaders. IEEE Trans Inf Forensics Secur. 2017; 12(2): 445-53. https://doi.org/10.1109/TIFS.2016.2622226

[7] Ogunleye J. The concepts of predictive analytics. Int J Dev Big data Anal. 2014; 1(1): 86-94.

[8] Gerdes LM. MAPPing dark networks: A data transformation method to study clandestine organizations. Netw Sci. 2014 Aug 1; 2(2): 213-53. https://doi.org/10.1017/nws.2014.8

[9] Marciani G, Porretta M, Nardelli M, Italiano GF. A data streaming approach to link mining in criminal networks. In: Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017. 2017. https://doi.org/10.1109/FiCloudW.2017.88

[10] Uzlov D, Vlasov O, Strukov V. Using Data Mining for Intelligence-Led Policing and Crime Analysis. In: 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings. Institute of Electrical and Electronics Engineers Inc.; 2019. p. 499-502. https://doi.org/10.1109/INFOCOMMST.2018.8632122

[11] Maza KD, Koldas U, Aksit S. Challenges of Countering Terrorist Recruitment in. 2020;

[12] Gerdes LM. Illuminating dark networks: The study of clandestine groups and organizations. Illuminating Dark Networks. Cambridge University Press; 2015. 1-255 p. https://doi.org/10.1017/CBO9781316212639

[13] Dey PJ, Medya S. Covert networks: How hard is it to hide? In: Proceedings of the International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS. 2019.

[14] Lindelauf RHA, Borm PEM, Hamers H. Understanding Terrorist Network Topologies and Their Resilience Against Disruption. SSRN Electron J. 2011; https://doi.org/10.1007/978-3-7091-0388-3_5

[15] Franzese M, Iuliano A. Hidden Markov Models. In: Encyclopedia of Bioinformatics and Computational Biology. Elsevier; 2019. p. 753-62. https://doi.org/10.1016/B978-0-12-809633-8.20488-3

[16] Saini P, Sunila Godara M. Modelling Intrusion Detection System using Hidden Markov Model: A Review. Int J Adv Res Comput Sci Softw Eng [Internet]. 2014; 4(6): 2277-128. Available from: https: //pdfs.semanticscholar.org/96dd/5080aca855d1d95a0aa2dbf00147548af17d.pdf

[17] Visser I, Speekenbrink M. Package "depmixS4." CRAN. 2020.

[18] Farag MMM, Elghazaly T, Hefny HA. Face recognition system using HMM-PSO for feature selection. In: 2016 12th International Computer Engineering Conference, ICENCO 2016: Boundless Smart Societies. 2017. https://doi.org/10.1109/ICENCO.2016.7856453

[19] Yin X, Jiang XT, Chai B, Li L, Yang Y, Cole JR, *et al*. ARGs-OAP v2.0 with an expanded SARG database and Hidden Markov Models for enhancement characterization and quantification of antibiotic resistance genes in environmental metagenomes. In: Bioinformatics. 2018. https://doi.org/10.1093/bioinformatics/bty053

[20] Raghavan V, Galstyan A, Tartakovsky AG. Hidden Markov models for the activity profile of terrorist groups. Ann Appl Stat. 2013; https://doi.org/10.1214/13-AOAS682

[21] Shuaibu SS, Salleh MA. Historical Evolution of Boko Haram in Nigeria : Causes. Proc Icic 2015. 2015; (September): 217-26.

[22] Bello HS, Galadima IS, Aliyu BI. An Assessment of the Effects of Boko-Haram Insurgency on Business Development in North-Eastern States of Nigeria. Bus Ethics Leadersh. 2018; https://doi.org/10.21272/bel.2(1).70-77.2018

[23] Braynov S. Adversarial planning in networks. In: Computational Methods for Counterterrorism. 2009. https://doi.org/10.1007/978-3-642-01141-2_14

[24] Farooq E, Khan SA, Butt WH. Covert network analysis to detect key players using correlation and social network analysis. In: ACM International Conference Proceeding Series. 2017. https://doi.org/10.1145/3018896.3025142

[25] Seidler P, Haider J, Kodagoda N, William Wong BL, Pohl M, Adderley R. Design for intelligence analysis of complex systems: Evolution of criminal networks. In: Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016. 2017. https://doi.org/10.1109/EISIC.2016.036

[26] Nguyen L. Tutorial on Hidden Markov Model. Appl Comput Math. 2016; 6(4): 16.

[27] Brogi G, Di Bernardino E. Hidden Markov models for advanced persistent threats. Int J Secur Networks. 2019; 14(4): 181-90. https://doi.org/10.1504/IJSN.2019.103147

[28] Valleriani A, Li X, Kolomeisky AB. Unveiling the hidden structure of complex stochastic biochemical networks. J Chem Phys. 2014; https://doi.org/10.1063/1.4863997

[29] Yang H, An S. Critical Nodes Identification in Complex Networks. Mdpi. 2020; 1-15. https://doi.org/10.3390/sym12010123

[30] Anandravisekar. G, Anto Clinton. A, Mukesh Raj. T, Naveen. L, M. Mahendran. IoT Based Surveillance Robot. Int J Eng Res. 2018; V7(03): 84-7. https://doi.org/10.17577/IJERTV7IS030061

[31] Bokade AU, Ratnaparkhe VR. Video surveillance robot control using smartphone and Raspberry pi. Int Conf Commun Signal Process ICCSP 2016. 2016; 2094-7. https://doi.org/10.1109/ICCSP.2016.7754547

[32] Kaur T, Kumar D. Wireless multifunctional robot for military applications. 2015 2nd Int Conf Recent Adv Eng Comput Sci RAECS 2015. 2016; (December). https://doi.org/10.1109/RAECS.2015.7453343

[33] Balaji M, Karthick S, Manikandan V, J BE, Ct VN. Surveillance and Target Engagement using Robots. In: Journal of Electronics and Communication Engineering. 2017; p. 1-6.

[34] Selvi S, Fathima MF, Dhivyuaa S, Mouriya S. SURVEILLANCE ROBOT USING RASPBERRY PI FOR. Int J Curr Eng Sci Res. 2019; 6(3): 394-9.

[35] Wang Y, Howard N, Kacprzyk J, Frieder O, Sheu P, Fiorini RA, *et al*. Cognitive Informatics. Int J Cogn Informatics Nat Intell. 2018; https://doi.org/10.4018/IJCINI.2018010101

[36] Dwarakanath L, Kamsin A, Rasheed RA, Anandhan A, Shuib L. Automated Machine Learning Approaches for Emergency Response and Coordination via Social Media in the Aftermath of a Disaster: A Review. IEEE Access. 2021. https://doi.org/10.1109/ACCESS.2021.3074819

[37] Hung BWK, Jayasumana AP, Bandara VW. Finding Emergent Patterns of Behaviors in Dynamic Heterogeneous Social Networks. IEEE Trans Comput Soc Syst. 2019; https://doi.org/10.1109/TCSS.2019.2938787

[38] Tundis A, Kaleem H, Mühlhäuser M. Tracking criminal events through IoT devices and an edge computing approach. In: Proceedings - International Conference on Computer Communications and Networks, ICCCN. 2019. https://doi.org/10.1109/ICCCN.2019.8846956

[39] Chen X, Qing L, He X, Su J, Peng Y. From Eyes to Face Synthesis: A New Approach for Human-Centered Smart Surveillance. IEEE Access. 2018; https://doi.org/10.1109/ACCESS.2018.2803787

[40] Sutton Z, Willett P, Bar-Shalom Y. Target Tracking Applied to Extraction of Multiple Evolving Threats from a Stream of Surveillance Data. IEEE Trans Comput Soc Syst. 2021; https://doi.org/10.1109/TCSS.2021.3051941

[41] Saeidi H, Wang Y. Incorporating trust and self-confidence analysis in the guidance and control of (semi) autonomous mobile robotic systems. IEEE Robot Autom Lett. 2019; https://doi.org/10.1109/LRA.2018.2886406

[42] Lippiello V, Siciliano B, Villani L. A grasping force optimization algorithm for multiarm robots with multifingered hands. IEEE Trans Robot. 2013; https://doi.org/10.1109/ICRA.2012.6224915

[43] Zuo B, Zhu W, Li F, Zhuo J. Modeling and Quantitative Analysis of Terrorist Attack Task List. In: Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020. 2020. https://doi.org/10.1109/ITNEC48623.2020.9084780

[44] Skillicorn D. Extracting Knowledge from Graph Data in Adversarial settings". In Memon. N., David F.Y., Hicks D.L., Rosenorn T. (eds) Mathematical methods in counterterrorism. J Comput Anal Appl. 2009; 34-40. https://doi.org/10.1007/978-3-211-09442-6_3

[45] KC. Okafor, "Dynamic reliability modeling of cyber- physical edge computing network", Int'l J. of Computers and App.

[46] KC. Okafor; Guinevere, E.C.; Akinyele, O.O, "Hardware Description Language (HDL): An Efficient Approach to Device Independent Designs for VLSI Market Segments", In 3rd IEEE Int'l Conf., Adaptive Science and Techy (ICAST), 2011, Abuja, 24th-26th, Nov.2011. Pp. 262- 267.

Received on 07-06-2021 Accepted on 17-08-2021 Published on 04-09-2021

DOI: https://doi.org/10.31875/2409-9694.2021.08.1