Ant Colony Optimization Algorithm Based Vehicle Theft Prediction-Prevention and Recovery System Model (Aco-Vtp^{2}rsm)

[1]Ajenaghughrure Ighoyota Ben,
Department of Computer Science
Vels University Pallavarm, chennai, 60017, India
ighoyotaben@yahoo.com

[2]Akazue Maureen I.
Mathematics and Computer Science
Delta State University,P.M.B.1, Abraka,330106,Nigeria
akazuem@gmail.com

[3]Onyekweli Charles O.
Mathematics and Computer Science
Delta State University,P.M.B.1, Abraka,330106,Nigeria
ogokweli@yahoo.com

ABSTRACT - Existing vehicle security technologies are either capable of theft, prevention or recovery or both. They lack the capability to predict theft occurrence and this makes the task of theft prevention or recovery unattainable. Therefore, this research paper focuses on the development of an advance vehicle security system that is based on ant colony optimization algorithm, to enhance vehicle theft prevention, through theft perception and prevention for parked vehicles. The proposed system is capable of predicting and preventing theft, through self learning, and automatic adjustment of in-vehicle security mechanisms, such as mechanical locks level, engine immobilization, and location tracking. This is made feasible with the aid of integrated GSM technology, GPS technology, DC-DC relay, Multi-level mechanical lock, RFID technology, proximity and touch sensor. Due to the limited resources in a typical embedded controller, an ant colony algorithm for vehicle theft prediction and prevention in addition to the system architecture was designed. Analysis of the algorithm clearly showed that the system optimum performance in the search for possible theft attempt and prevention mechanism enforcement, utilizing embedded processor time not more than n^2, was obtained. The analysis proved the promising capability of the system to improve vehicle theft prediction and prevention within the limited controller resources. Further work on experimentation will be done to realize the full product.

Keyword: Ant colony Optimization algorithm, Vehicle theft prevention, Vehicle theft prediction, GPS, RFID, touch sensor, proximity sensor

I. INTRODUCTION

There is a misconception in literature dealing with vehicle security and theft prevention, which include vehicle theft prevention, recovery, and prediction. First, theft prevention is totally concerned with all mechanism that makes it impossible to take temporary ownership or control of a vehicle illegally. Secondly, theft recovery of stolen vehicle is an aftermath act, to recover a stolen vehicle, and not a theft prevention strategy. Lastly, vehicle theft prediction is a sensory perceptibility of the possibility of vehicle theft occurrence.

Vehicle importance to human activities, especially transportation cannot be overemphasized. Hence, proliferation of vehicles in modern day society as a major means of transportation continues to increase. The cost associated with acquisition of a vehicle runs from few thousand to millions of dollars. Prompting its vulnerability to theft, either in motion or parked, to be on the increase. When vehicles are packed, owners are away irrespective of distance, with confidence on traditional mechanical vehicle door locks and other digitized solutions such touch alarm, hit alarm, in-vehicle surveillance camera, GPS locator, engine immobilization system and lots more. All these technologies are far from perfect in completely predicting or preventing vehicle theft, due to their vulnerability to false alarm, alternative by-passing mechanism, such as breaking the window glasses to open the door and stealing a vehicle, false alarm from touch of passerby without the intention to steal the vehicle, high cost deterring most vehicle owners from acquiring these systems, vehicle battery cut, and incapacitation of most non-energy efficient in-vehicle security system [1].

II OVERVIEW OF RELATED WORKS ON VEHICLE SECURITY SYSTEMS

[1] developed a vehicle security system that prevent vehicle theft with an advancement on vehicle battery cut system by-passing technique that prevents the use of this technique to bypass the security system. The system consists of GSM, GPS and biometric system.

[2] Developed a vehicle security system that automatically identifies all vehicles at check post using RFID technology. Each vehicle is armed with a read-only passive RFID tag with unique identification code that cannot be changed or purchased commercially. Despite the novelty of this system, it is only useful, after vehicle, theft has occurred and it has been reported.

Also, [3] designed a smart vehicle security system using GPS, GSM, and infra-red technology as major components alongside high voltage mesh for steering shock. The system keeps track of vehicle location and gives vehicle owners, the flexibility to lock-down and pen their vehicle using mobile technology.

In addition, [4] developed a GPS, GSM and web technology solution for tracking stolen vehicle location in real-time. The GPS obtains the location of stolen vehicle and delivers it through the GSM network from where the vehicle location is logged over the web application to track it location. It is most suitable for locating stolen vehicles and cannot aid in predicting and preventing vehicle theft.

Furthermore, [5] developed mobile solution for tracking stolen vehicles, as an enhancement to the continuous use of tracking technology as an effective solution to vehicle theft battle. This system does not include any module for perception of possible vehicle theft.

The use of face recognition image processing was employed by [6] in their system design. It reports unauthorized access to owners through multimedia message service and is scalable to allow authorization of user whose face is not recognized but owner wants to grant access to the vehicle. The system also includes an accident report module. [7] developed a face recognition vehicle security system for immobilization of vehicle ignition base on facial identify.

All existing systems lack the sensor perception capability to predict and prevent vehicle theft. Existing systems are either preventing or recovery or both using mostly tracking and access control technologies for mitigating the menace of vehicle theft. Unfortunately, vehicle theft prediction has received little or no attention and hence, this research paper integrates theft prediction and prevention strategies into vehicle theft security system based on ant colony optimization technique implemented on a low cost effective off the shelf hardware and sophisticated software solution.

III. ACO-VTP^{2}RSM Design

The ACO-VTP^{2}RSM design consists of two major phases; the design of the ant colony optimization algorithm that will be used for proposed system implementation. Next will be the physical hardware/software design.

A. Ant Colony Optimization Algorithm For ACO-VTP^{2}RSM

The ant colony optimization algorithm designed is based on the general principle of pheromone deposit by ant food search activities. The proposed algorithm mimics the same principle for vehicle theft prediction to enhance the proposed advance vehicle security system intelligence, with sensory perceptibility and accurate theft prevention action, on confirmed perceived vehicle theft threat. A simple algorithm considering all vehicle doors as a unidirectional connected graph G, with vertices V, and edges E is designed.

Such that G= (V, E)

Figure1 depicts the objective of predicting vehicle theft occurrences and accurate decision making to prevent the perceived theft threat.

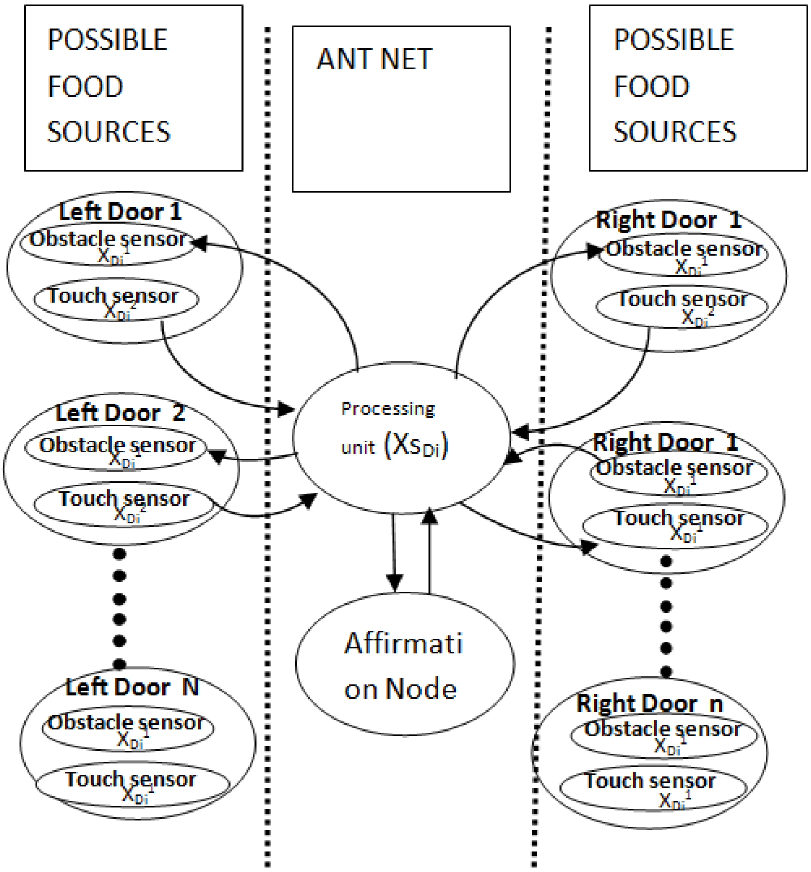

Fig 1 ACO based vehicle theft prediction and prevention model

- The proposed ant colony optimization algorithm for vehicle theft prediction-prevention model in figure1 above is defined mathematically as follows:

  $P = (S, \Omega, F)$

  Where F is the objective function aimed at predicting with high accuracy, vehicle theft threat based on some parameters from the solution search space (S). S is the problem solution search space defined over a finite set of discrete decision variable as $S= (X_i, A_i)$, and a set of constraint denoted as Ω over the finite set of discrete decision variables.

- The problem solution search space (S) is thus defined as a collection of finite discrete variable corresponding to the number of nodes(vehicle doors, embedded processors), sensors, and affirmation node/RFID reader), the values of various sensors (tough sensor, proximity sensor, and RFID reader status). Mathematically the problem solution search space is defined as follows;

  $S = (X_i, A_i)$

  Where X_i is the nodes in the fig1 and A_i are the arcs connecting each node (X_i)

- The nodes of Figure1 are defined as X_i. Each X_i is a triplet, consisting of door nodes, source/destination node (also referred to hereafter as ant colony corresponding to the embedded controller in practical implementation) and a unique node called the affirmation node (in real life is the RFID reader). Mathematically X_i is defined as follows:

  $X_i = (X_{Di}, X_{SDi}, X_{DEC....i}) \; \forall \, i, \; i = 1,2,3,4, \ldots..n$

Where X_{Di} is door node, X_{SDi} is source-destination node or also referred to as ant net/ home, $X_{DEC....i}$ is a unique node that confirms any perceived threat. Door node is also referred to as food source node in ant colony and threat area in vehicle theft prediction X_{Di}

X_{Di} is defined as a pair wise set of node corresponding to food search which in practical implementation represents the two sensors (touch and obstacle proximity) attached to each vehicle door. Mathematically defined as

$X_{Di} = (X_{Di}^1, X_{Di}^2) \qquad \forall \, X_{Di} \in X_{i,} \; I = 1,2,\ldots.n$

n depends on the number of likely food source but in practical implementation, n is the number of vehicle doors being the possible source of invasion. Here X_{Di}^{1}, corresponds to obstacle proximity sensor node and X_{Di}^{2}, corresponds to capacitive touch sensor node

The pairs of X_{Di} values are a range of finite discrete non-negative integer values. They are critical to the algorithm and the entire system functioning, being the main source of input to the system. Their values are drawn from $X_{Di}= V_i^j \in D_i = (V_i^1, V_i^2, V_i^3, V_i^4, V_i^4, V_i^5, \ldots\ldots\ldots V_i^{Di})$, where D_i is a pool of non-negative integer values from minimum sensor values to maximum in implementation scenario but in ant colony, D_i corresponds to food availability and quantity.

An ANT colony/home is also referred to as embedded processor node. This is where the actual search for food begins in real life ant colony food search and discovered food is brought to same. Similarly, in vehicle theft prediction-prevention, the search for possible threat of vehicle theft begins from the embedded processor constantly monitoring each sensor after proper initialization and power supplied. Any discovered threat is returned to the embedded processor for further action. Hence, this node is referred to as source-destination node derived from the mode of operation. A search from this node through each X_{Di} and their corresponding sub-nodes X_{Di}^{1} and X_{Di}^{2} leads to a further search through the unique path to the affirmation node $X_{DEC\ldots.i}$. A final confirmation of vehicle being under real threat of theft is synonymous to an affirmation that food is present at any point in ant colony world. Due to the fact that affirmation may not be a guaranteed threat in the real world ant colony, it was included in the proposed model to reduce false alarm and increase accuracy of prediction. Furthermore, once prediction is confirmed, prevention is next on the line, which is a set of action that this node will perform, amongst which include, sending SMS messages to concerned authorities of vehicle theft threat, ignition shutdown, increasing vehicle security through multi-level mechanical lock, shutting down fuel, water and oil supply line in the system.

The values of X_{SDi} are Boolean values which are either true or false is stored in $D_i = (V_i^1, V_i^2)$. Where i=1,2,3…n for all search X_{SDi} has conducted.

The value of $X_{SDi} = V_i^1$ = true, if there is a successful path from $X_{SDi} \rightarrow X_{Di}$, for any $X_{Di,}$ such that, each pair of nodes in X_{Di} indicates positive to threat, such as object (human) is in close proximity to vehicle and a body contact is made on the door of the vehicle. Also, a further affirmation of the identity of the object(human) in question is conducted through a search from $X_{SDi} \rightarrow X_{DEC\ldots.i}$, if object identity is not confirmed, then, vehicle theft threat is confirmed. Else $X_{SDi} = V_i^1$ = false, if any sub node in any X_{Di} under consideration is not confirmed. Or in the case of both confirmed, but identify of object is confirmed correct, and then apparently it's the vehicle legitimate owner in close proximity.

Affirmation node ($X_{DEC\ldots.i}$) also referred to as RFID reader node from Fig1 is used by the algorithm to confirm a vehicle theft threat, through the request of vehicle owner identification code that is implemented on RFID technology. Although this affirmation node is not available in a typical ant colony world, but it's somewhat available, through ant's inspection of suspected food. The values of this node are Binary values indicating the presence or absence of the vehicle owner unique identification code, denoted mathematically as

$X_{DEC\ldots.i} = (V_i^1, V_i^2)$, where each triplet hold Binary values 1 and 0 respectively, corresponding to correct vehicle owner unique identification code and incorrect code respectively.

B. Arc Description.

This is the second component of the search space, connecting nodes together. It is defined as a triplet mathematically as follows

$A_i=(A_{Di}, A_{SDi}, A_{DEC\ldots.i})$, where each triplet corresponds to arcs connecting each sub nodes in each A_{Di}, arcs connecting $A_{SDi} \rightarrow A_{Di}$, and the arcs connecting $A_{SDi} \rightarrow A_{DEC\ldots.i}$ respectively.

- Door node arcs A_{Di} ($A_{Di}^{1}, \rightarrow A_{Di}^{2} \rightarrow A_{SDi}$): This is also referred to as the return path after successful food discovery, which in vehicle theft prediction-prevention application corresponds to a set of successive search, verifying the closeness of an object (human) to vehicle, and verifying object contact to vehicle. Finally, a suspicion is registered. The weight on each arc here denoted by W, are set of discrete non-negative integer values corresponding to senor values. A successive move from $X_{Di}^{1}, \rightarrow X_{Di}^{2}$ ($A_{Di}^{1}, \rightarrow A_{Di}^{2}$) is possible if the sensor values in sub node X_{Di}^{1} exceed the normal value indicating object closeness to the vehicle, and similarly for $X_{Di}^{2} \rightarrow X_{SDi}$ ($A_{Di}^{2} \rightarrow A_{SDi}$).
  W = 1, 2, 3, 4, ……. (n being the maximum sensor value)
- Source destination arcs $A_{SDi} \rightarrow A_{Di}$ (pheromone node): this is the arc from source-destination node to door node (possible food location node) marking the beginning of the search for food. This arc returns to source destination on two conditions, either on a successful search, through a path from food location node (door node) to source destination node, or an outright termination of food search, through continuous search of food location node (door node) until food is found (threat is detected). An event of successful search (threat

found), a numeric integer one (1) is added to the weight of the source destination arc. While the door node arcs(food location arc) holds values from their corresponding sensor

- Affirmation arcs $A_{SDi} \rightarrow A_{DEC....i}$

C. Constrain function:

- For each transition from source destination node to any door node, it is automatic and continuous as in the case of ant random beginning for food search, without constrain or clue on where to go. The weight on the arc connecting these nodes are non-negative integer values from zero(0) to nth, depending the number of threat perceived continuously on a door
- For each move from a door node back to the source destination $X_{Di}^1, \rightarrow X_{Di}^2 \rightarrow X_{SDi}$, the sensor threshold value which can vary among various sensor calibration, must be satisfied, as it indicates object in close proximity with vehicle and object in contact with vehicle, for both obstacle sensor and touch sensor respectively. When sensor threshold value is enforced, it establishes the basis for creating a partial solution or not depending on the on the state of transition from door node to source destination node which can be either successful or failed.
- For each transition from a source destination node to decision node, for confirmation of the perceived threat, the arc from source destination directed to decision node will always be zero(0), while the main factor for confirmation the perceived threat will either zero(0) or one(1), corresponding to false and true respectively. Each threat confirmation request, reinitializes the weight on the return arc from decision node to source destination node to zero(0).
  - $F(X_{SDi} \rightarrow X_{Dec...i}) \rightarrow A_{SDi} \rightarrow A_{DEC....i} = 0$
  - $F(X_{Dec...i} \rightarrow X_{SDi}, A) \rightarrow A_{DEC....i} \rightarrow A_{SDi} = 1$

IV. ALGORITHM PSEUDOCODE

The pseudocode for the ant colony optimization algorithm based vehicle theft prediction prevention:

1. **input:** An instance *P* of a CO problem model *P = (S, f,)*
2. $\mathbf{W_i (A_{SDi} \rightarrow A_{Di}) = 0}$ //Initialize Pheromone Values the weight on each arc from source destination node to all door node
3. $\mathbf{s_{i....partial} \leftarrow NULL}$
4. **while** S_i != true // that is Si not holding a complete set of nodes and arcs which satisfies the constrain
5. **do**
6. **Siter** ← ∅ // all iteration search for possible threat (food source) just began from null, since none has been executed before now.
7. **for** ***j*** = 1, . . . , *n // begin search through all door nodes from source-destination node*
   {
8. $\mathbf{FOR\ (X_{SDi} \rightarrow X_{Di}^1, AND\ A_{SDi} \rightarrow A_{Di} = w\ )}$ *//for all search from source-destination node to door node*
9. **{**

/ / if there is no successful transition from any door node to its sub node with arc weight exceeding the threshold limit for threat indication satisfying the constrain on such transition

10. $\mathbf{IF\ (!\ X_{Di}^1, \rightarrow X_{Di}^2, AND\ !\ A_{Di}^1 \rightarrow A_{Di}^2 = w)}$

{

11. **Return to 8.** / */no possible perceived threat*

// else if 10 is true and there is no successful transition from a door sub node to source destination node with arc weight exceeding the threshold for threat indication satisfying the constrain on such transition

12. $\mathbf{ELSE\ \ IF(!\ X_{Di}^2 \rightarrow X_{SDi}\ AND\ !\ A_{Di}^2 \rightarrow A_{SDi} = w)}$

{

13. **Return to 10.** // *no possible perceived threat*

// else if 12 is true, threat is perceived (possible food availability in source is perceived in ant colony case), forming a partial solution that needs further verification

14. **ELSE** $\mathbf{s_{i...partial} = (0.5)}$ // is a possible valid solution, half because threat perceived need confirmation

}

}

//BEGIN LOCAL SEARCH*: request for owners identification to confirm that close object to vehicle is not a theft threat and object in contact with vehicle is not also a theft threat, this request arc weight is always zero(0). In the practical implementation of the system RFID subsystem corresponds to this node*

15. $\mathbf{X_{SDi} \rightarrow X_{Dec},\quad A_{SDi} \rightarrow A_{DEC}=w(0)}$ // *REQUEST CONFIRMATION OF THREAT FROM SOURCE DESTINATION NODE TO CONFIRMATION NODE*

//Reinitialize the weight of the arc $\mathbf{A_{DEC....i} \rightarrow A_{SDi}}$ connecting decision/affirmation node to source destination node also referred to as the response node ($\mathbf{X_{Dec...i} \rightarrow X_{SDi})}$ zero(0) to enable the current request decision to be updated and sent back to source destination node

16. $\mathbf{X_{Dec...i} \rightarrow X_{SDi}\ ,\ A_{DEC....i} \rightarrow A_{SDi} = w(0)}$

// response verifying vehicle owner identity is returned from affirmation or confirmation node to source destination node with arc value varying from zer(0) and one(1)

17. **IF** $\mathbf{(X_{Dec...i} \rightarrow X_{SDi},\ AND\ A_{DEC....i} \rightarrow A_{SDi} = W(0))}$
    {
18. **THEN** $\mathbf{s_{i...partial}}$ **= 0(false)** *//0.5-05=0 // perceived threat is false,*
19. **return to 8**
20. **ELSE IF** $\mathbf{(X_{Dec...i} \rightarrow X_{SDi},\ AND\ A_{DEC....i} \rightarrow A_{SDi} = W(1))}$ / / *threat is confirmed*
    {
21. $\mathbf{s_{i...partial}}$ **= 1(true)** */ /0.5+0.5 = 1*

// store the final confirmed solution in our confirm solution array

22. $\mathbf{s_{confirmed} = s_{i...partial}}$
23. $\mathbf{s_{i...partial} \in s_{confirmed}}$
    }//end if
    }//end if
    }//end for
    }//end for
    //determine point to focus search on
24. **ApplyPheromoneUpdate(**w_i **,**$\mathbf{S_{iter}}$ **,** $\mathbf{S_i}$**….partial)** */ / add two(2) to the weight of the arc from source destination to the door node where threate was perceived but not yet confirmed(*$s_{i...partial}$ *) and add one(1) to the weight of the arcs connecting source destination node to other door nodes*
25. **FOR (I =1 to n)**

{

26. IF(ARC ($A_{SDi} \rightarrow A_{Di}$)∈ $\mathbf{s_{i...partial}}$**,)***//check each arc from sourcedestination node to door nodes, if it is part of the sequence of arcs that leads to the confirmed threat*
    {
27. THEN W= W+2//*increase the weight of the arc by 2*
28. ELSE
29. W= W+1//*if the arc is not part of the sequence of arcs that leads to the confirmed threat, then increase the weight by 1, this is because threate has been discpvered and punitive measures must be employed to keep all doors safe*
    }*//end if*
    }*//end for*
30. **end while**
31. $\mathbf{S_{iter} \leftarrow S_{iter} \cup \{s_{confirmed}\}}$ *//continue searching for threat in door node where threat has been perceived only, until another door node returns perceived threat.*
32. **output:**
33. Increase vehicle security level, for all doors
34. Enforce security measures (send sms, increase mechanical lock level from one to three, cutoff fuel, water and oil supply line, shutdown vehicle ignition)
35. END

V. ALGORITHM ANALYSIS

The time and memory space complexity of the proposed ACO algorithm for prediction and prevention of vehicle theft is given in Table1. We assume that each input operation requires one byte of memory and is equal to 1milisecond processor time respectively.

Table 1: Analysis of the Time and memory space complexity of proposed system ACO algorithm

S/N		FIRST SUCCESS	
		TIME(S)	COST
	input: An instance *P* of a CO problem model *P = (S, f,).*	1	C1
	$W_i(A_{SDi} \rightarrow A_{Di}) = 0$ //InitializePheromoneValues	1	C2
	$s_{i....partial} \leftarrow$NULL	1	C3
	while S_i != true // that is Si not holding a complete set of nodes and arcs which satisfies the constrain	**	C4
	Do		
	Siter ← ∅ // all iteration search for possible threat (food source) just began from null, since none has been executed before now.	1	C5
	for *j* = 1, . . . , *n {*	n+1	C6
	FOR ($X_{SDi} \rightarrow X_{Di}^1$, AND $A_{SDi} \rightarrow A_{Di}$ = w) {	n*(n+1)	C7
	IF (! $X_{Di}^1, \rightarrow X_{Di}^2$, AND ! $A_{Di}^1 \rightarrow A_{Di}^2$ = w)	n*n	C8
	Return to 8. / */no possible perceived threat*	n*n	C9
	// else if 10 is true and there is no successful transition from a door sub node to source destination node with arc weight exceeding the threshold for threat indication satisfying the constrain on such transition **ELSE IF (! $X_{Di}^2 \rightarrow X_{SDi}$ AND ! $A_{Di}^2 \rightarrow A_{SDi}$ = w)** **{**	n*n	C10
	Return to 8. / */no possible perceived threat*	n*n	C26
	// else if 12 is true, threat is perceived, forming a partial solution that needs further verification **ELSE $s_{i...partial}$ = (0.5)** / / is a possible valid solution, half because threat perceived need confirmation }*//end if* }*end if* }*end for*	n*n	C11
	//BEGIN LOCAL SEARCH*: request for owners identification to confirm that close object to vehicle is not a theft threat and object in contact with vehicle is not also a theft threat, this request arc weight is always zero(0). In the practical implementation of the system RFID subsystem corresponds to this node* **$X_{SDi} \rightarrow X_{Dec,}$ $A_{SDi} \rightarrow A_{DEC}$=w(0)** / */request confirmation of threat from source destination node to confirmation node*	N	C12
	//Reinitializethe weight of the arc $A_{DEC....i} \rightarrow A_{SDi}$ connecting decision/affirmation node to source destination node also reffered to as the response node ($X_{Dec...i} \rightarrow X_{SDi)}$ zero(0) to enable the current request decision to be updated and sent back to source destination node **$X_{Dec...i} \rightarrow X_{SDi}$, $A_{DEC....i} \rightarrow A_{SDi}$ = w(0)**	n	C13
	// response verifying vehicle owner identity is returned from affirmation or confirmation node to source destination node with arc value varying from zer(0) and one(1) **IF ($X_{Dec...i} \rightarrow X_{SDi,}$ AND $A_{DEC....i} \rightarrow A_{SDi}$ = W(0))** **{**	n	C14
	THEN $s_{i...partial}$ = 0(false) *//0.5-05=0 // perceived threat is false,*	n	C15
	return to 8.	n	C16
	ELSE IF ($X_{Dec...i} \rightarrow X_{SDi,}$ AND $A_{DEC....i} \rightarrow A_{SDi}$ = W(1)) / / *threat is confirmed* {	n	C17
	$s_{i...partial}$ = 1(true) */ /0.5+0.5 = 1*	n	C18
	// store the final confirmed solution in our confirm solution array 1. **$s_{confirmed} = s_{i...partial}$** 2. **$s_{i...partial} \in s_{confirmed}$** }*//end if* }*//end if*	n	C19

	}*//end for*		
	ApplyPheromoneUpdate(w_i ,S_{iter} , S_i….partial) */ / add two(2) to the weight of the arc from source destination to the door node where threat was perceived but not yet confirmed($s_{i…partial}$) and add one(1) to the weight of the arcs connecting source destination node to other door nodes* **FOR (I =1 to n) {**	n+1	C20
	IF(ARC ($A_{SDi} \rightarrow A_{Di}$)∈ $s_{i…partial}$,) {	n	C21
	THEN W= W+2 *//increase the weight of the arc by 2*	n	C22
	ELSE W= W+1 *//if the arc is not part of the sequence of arcs that leads to the confirmed threat, then increase the weight by 1* }*//end if* }*//end for*	n	C23
	$S_{iter} \leftarrow S_{iter} \cup \{s_{confirmed}\}$ *//update search path and continue searching for threat in door node where threat has been perceived only, until another door node returns perceived threat.*	1	C24
	output:		
	Increase vehicle security level, for all doors Enforce security measures (send SMS, increase mechanical lock level from one to three, cut-off fuel, water and oil supply line, shutdown vehicle ignition)	1	C25
	END		

A. Time and space requirements of the ant colony optimization algorithm for ACO-VTP^{2}R system model

- First successful search with threat detected and necessary security measure executed without failure/termination

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+c9*(n*n)+c10*(n*n)+c11*(n*n)+C12*n +c13*n +c14*n +c17*n +c18*n +c19*n + C20*(n +1)+C21*n +C22*n+c23*n+c24*1+c25*1

= (C1+c2+c3+c5+c6+c7+c20+ c24+c25)+c4*∞ + (C6+C7+C12+c13+c14+c17+c18 +c19 + C20+C21 +C22+c23)n+ (c9+c10+c11)n^2

Thus proportional to n^2

- First successful search with threat detected and necessary security measure executed with failure/termination

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+c9*(n*n)+c10*(n*n)+ c11*(n*n)+C12*n +c13*n +c14*n + c17*n +c18*n +c19*n + C20*(n +1)+C21*n +C22*n+c23*n+c24*1+c25*1

Thus proportional to n^2

- First possible threat perceived without failure

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+ c9*(n*n)+c10*(n*n)+ c11*(n*n)

Thus proportional to n^2

- False threat perceived without failure/termination

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+ c9*(n*n)+c10*(n*n)+ c11*(n*n)+C12*n +c13*n +c14*n +c15*n +c16*n

Thus proportional to n^2

- False threat perceived with failure termination

C1*1+c2*1+c3*1+c4*∞+c5*1+C6*(n+1)+C7*(n+1)+C8*(n*)+c9*(n*n)+c10*(n*n)+c25*(n*n)+c11*(n*n)+C12*n +c13*n +c14*n +c15*n +c16*n

Thus proportional to n^2

- True perceived threat without failure/ termination

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+c9*(n*n)+c10*(n*n)+c11*(n*n)+C12*n +c13*n +c14*n +c17*n +c18*n +c19*n

Thus proportional to n^2

- True perceived threat with failure/ termination

C1*1+c2*1+c3*1+c4*∞+c5*1+ C6*(n+1)+C7*(n+1)+ c9*(n*n)+c10*(n*n)+ c11*(n*n)+C12*n +c13*n +c14*n + c17*n +c18*n +c19*n

Thus proportional to n^2

VI. SYSTEM ARCHITECHURE

The overall system architecture is given in Figure 2, showing all the hardware components of the system and their interaction. The system inputs are the touch sensor unit, RFID reader unit, GPS unit and proximity sensor unit. The touch sensor is integrated to the handle of the vehicle door to monitor vehicle access attempt. Also, the infrared proximity sensor fitted to the vehicle door monitors the vehicle door surrounding for objects (humans) closeness to the vehicle, which can translate into many meanings. these two sensor parameters when combined as positive indication of suspicious attempted vehicle theft with the absence of vehicle owner unique identification code stored in a RFID tag, obtained through the RFID reader, is a clear indication of vehicle theft attempt. This process is also known as theft prediction. Further action is executed by the system through its various output operation. First the door with the perceived intrusion, security level is raised from level 1 to level three by the mechanical lock increasing the lock move from one(1) to three(3), while other doors mechanical lock move from one(1) to two(2). Secondly, the GPS data of the vehicle location is sent to local police department, informing them of vehicle theft attempt with the location of the vehicle. This same alert is sent to the vehicle owner. Finally, vehicle ignition is locked down to immobilize the vehicle completely, as well as vehicle engine fuel and oil supply line cutoff, through the stepper motors connected to the supply lines and the embedded microcontroller. The brain behind the entire processing, intelligent decision-making is the embedded microcontroller unit.

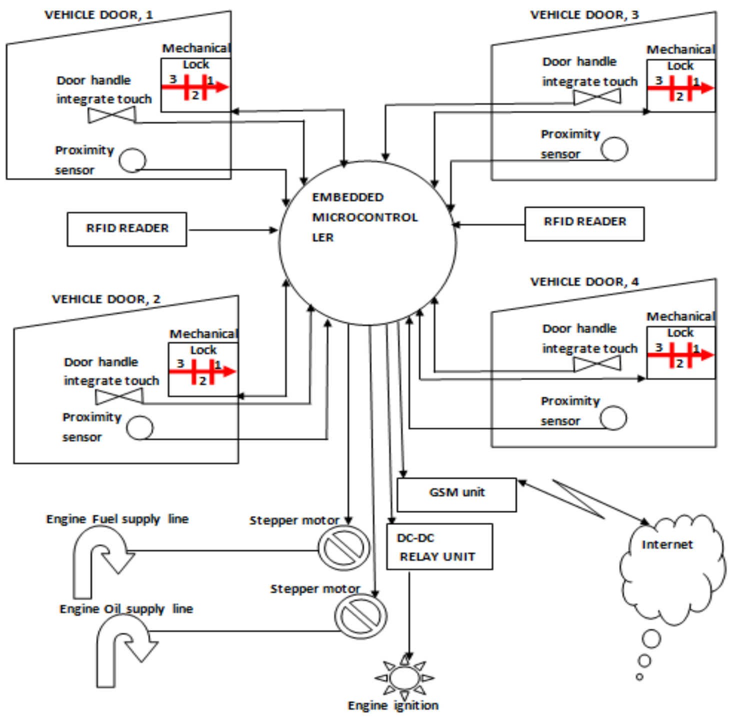

Figure 2: architecture of the proposed model

A. COMPONENT OF THE PROPOSED SYSTEM

- **GPS MODULE** is an output media for the proposed system, responsible for communicating detected threats of vehicle theft to owner, as well as relevant authority for appropriate action.
- **EMBEDDED MICROCONTROLLER** is likened to the ant colony in real world ant colony, with a specialized task. It is the brain of the system on which the ant colony algorithm was implemented. Therefore, the embedded controller performs all the task of monitoring all nodes, verifying the correctness of perceived theft and execution of relevant measure to enhance and ensure the security of the vehicle.
- **STEPER MOTOR** is an output unit that compliments other components in ensuring the security of the vehicle under confirmed theft threat, by shutting down water, fuel and engine oil supply line. These actions are likened to the food consumption activities in real-world ant colony.
- **DC-DC** RELAY switch is responsible in shutting down the ignition to immobilize the vehicle under confirmed the DC-DC relay switch does theft threat. It acts as an interface between the embedded microcontroller and the vehicle power source and ignition unit.
- **TOUCH SENSOR** confirms that an attempt to open vehicle door, or a contact was made on the vehicle through the help of the capacitive touch sensor, which is part of the search for theft threat.

- **INFRARED PROXIMITY SENSOR** is used to augment the touch senor theft threat confirmation, as closeness to vehicle is also needed to ascertain theft threat. It confirms when any human or object is very close to the vehicle. Although this is not enough to confirm vehicle theft, but when combined to the touch sensor results, significant theft threat is given.
- **RFID READER** confirms the identity of the perceived threat through the infrared proximity sensor and touch sensor, confirming a theft threat or not, depending on the outcome of the identification process.
- **ELECTONIC MECHANICAL LOCK** is a security measure that is synonymous to existing vehicle door locks, but with three level mechanical lock steps, controlled electronically. By default only level one lock is used, once threat is confirmed, all door lock increase to level two. As threat continues, the lock advances to its highest level, which is three. Similarly, as threat decreases, so the locks level decreases, but not blow one, which corresponds to open state.

VII. DISCUSSION

The designed ACO based vehicle theft prediction and prevention enhanced security model, promises to improve vehicle security, through theft prediction and prevention efficiently, through proper utilization of system resources, due to the constraint on embedded processors resources. This can be evidently seen in the ACO algorithm analysis, as all condition in worst case requires only n^2 processor time, while memory usage depends on the value of n. Furthermore, the use of ACO algorithm will enable consistent monitoring of all door nodes with more emphasis on those with known threats kept on closer watch than the others with lesser threat occurrences. Often times, there is always more threat on the driver's side door and so emphasis should be on the driver's door rather than waste resources monitoring all doors.

VIII. CONCLUSION

The proposed system when implemented promises a revolution to vehicle theft prevention technologies due to it novelty and sophistication in detecting threat, using network communication to disseminate the information and taking immediate self action on enhancing vehicle security through increasing mechanical locks level, shutting down ignition, water, oil and fuel supply line to immobilize vehicle, while awaiting response from vehicle owner and relevant authorities.

REFFERENCES

[1] N. Kiruthiga a, L. latha b, S. Thangasamy c., "Real Time Biometrics based Vehicle Security System with GPS and GSM Technology", Procedia Computer Science Vol. 47, pp.471 – 479, 2015.

[2] Mahesh Kumar Shakya, "Catching Of Stolen Vehicles With Unique Identification Code Using Embedded System", International Journal of Electronics Communication and Computer Technology (IJECCT) Vol. 2, Issue 6, pp. 262-266, November 2012.

[3] Pritpal Singh, Tanjot Sethi, Bibhuti Bhusan Biswal, and Sujit Kumar Pattanayak, "A Smart Anti-theft System for Vehicle Security", International Journal of Materials, Mechanics and Manufacturing, Vol. 3, Issue 4, pp.249 -254, November 2015

[4] Pankaj Verma and J.S Bhatia, "design and development of gps-gsm based tracking system with googlemap based Monitoring", International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.3, issue 3, pp .33-40, June 2013.

[5] Rohitaksha K , Madhu C G , Nalini B G and Nirupama C V, "Android Application for Vehicle Theft Prevention and Tracking System", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, issue 3, pp. 3754-3758, 2014.

[6] Priti K. Powale and G. N. Zade, "Real time Car Antitheft System with Accident Detection using AVR Microcontroller; A Review" International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 1, pp.509-512, January 2014.

[7] Vishal P. Patil and K.B. Khanchandani, "Car theft detection and prevention system", international journal of innovative research and development", Vol. 2, issue 2, pp. 346-355, February 2013.

[8] Tobias Hoppe n, StefanKiltz, and Jana Dittmann, "Security threats to automotive CAN network practical examples and selected short-term countermeasures" Reliability Engineering and System Safety Vol. 96, pp11–25, 2011.

[9] Sachin S. Aher, and Kokate R. D.," Fuel Monitoring and Vehicle Tracking", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 3, pp.166-169, March 2012.