

Trust-based Secure Clustering in WSN-based Intelligent Transportation Systems

Tarek Gaber^{a,b,e,*}, Sarah Abdelwahab^a, Mohamed Elhoseny^{c,e}, Aboul Ella Hassanien^{d,e}

^a*Faculty of Computers and Informatics, Suez Canal University, Ismailia, Egypt*

^b*School of Computing, Science and Engineering, University of Salford, UK*

^c*Faculty of Computers and Information, Mansoura University, Mansoura, Egypt*

^d*Faculty of Computers and Information, Cairo University, Egypt*

^e*Scientific Research Group in Egypt, Cairo University, Egypt*

Abstract

Increasing the number of vehicles on roads leads to congestion and safety problems. Wireless Sensor Network (WSN) is a promising technology providing Intelligent Transportation Systems (ITS) to address these problems. Usually, WSN-based applications, including ITS ones, incur high communication overhead to support efficient connectivity and communication activities. In the ITS environment, clustering would help in addressing the high communication overhead problem. In this paper, we introduce a bio-inspired and trust-based cluster head selection approach for WSN adopted in ITS applications. A trust model is designed and used to compute a trust level for each node and the Bat Optimization Algorithm (BOA) is used to select the cluster heads based on three parameters: residual energy, trust value and the number of neighbors. The simulation results showed that our proposed model is energy efficient (i.e., its power consumption is more efficient than many well-known clustering algorithm such as LEACH, SEP, and DEEC under homogeneous and heterogeneous networks). In addition, the results demonstrated that our proposed model achieved longer

*Corresponding author

Email addresses: t.m.a.gaber@salford.ac.uk (Tarek Gaber),
mohamed_elhoseny@mans.edu.eg (Mohamed Elhoseny), aboitcairo@gmail.com (Aboul Ella Hassanien)

¹My present address is School of Computing, Science and Engineering, Newton Building, University of Salford, M5 4WT, UK

network lifetime, i.e., nodes are kept alive longer than what LEACH, SEP and DEEC can achieve. Moreover, the the proposed model showed that the average trust value of selected Cluster Head (CH) is high under different percentage (30% and 50%) of malicious nodes.

Keywords: Wireless Sensors Networks, WSN, Clustering, Trust, Intelligent Transportation System, Bat Algorithm.

1. Introduction

Increasing the number of vehicles on roads leads to congestion and safety problems. According to Texas-Transport-Institute [2015], in the USA, the burden of congestion due to fuel costs reached to 115 billion dollars. Also the Worldbank.org [2015] estimates that more than 1.2 million people lose their lives in road accidents each year. One of the possible solutions to this problem is the deployment of Intelligent Transportation Systems (ITS) to improve the efficiency and safety of the transportation. This would be achieved by utilizing advanced communications and information processing as well as control technologies.

Traditionally, to detect traffic flow, ITS systems use: intrusive sensors, non-intrusive sensors Klein [2001]. In the intrusive sensors-based ITS, the following technologies/tools are used: magnetometers, inductive loops, different types of weigh-in-motion sensors and pneumatic road tubes. Such technologies, however, suffer from high costs because they require large parts of the road being torn up to install the equipment, thus disrupting traffic flow Rawat et al. [2014]. In non-intrusive sensors-based ITS, radars, video cameras, and ultrasonic sensors can be used and these are located above ground. The main limitations of these technologies are large energy consumption, large size, and being prone to effects of environmental conditions. Moreover, both intrusive and non-intrusive monitoring sensors are expensive and difficult to install as well as requiring wired infrastructures supported by power lines Rawat et al. [2014]. Consequently, such sensors are limited at critical locations working independently of

each other, thus limiting the utilization of such systems for the applications of vehicle safety which requires quick or real-time response depending on the scenario. .

Wireless Sensor Network (WSN) is a relatively recent technology which has found many applications, e.g, military, healthcare, agriculture, smart buildings, and ITS Abdelwahab et al. [2017a], Elhoseny et al. [2015]. WSN is usually medium to large networks that use cheap wireless sensor nodes which has the capabilities to sense, process, and distribute data collected from the environment using a collaborative model among nodes Gaber and Hassanien [2014] and Fouad et al. [2015]. The main advantages of WSN is its low cost and distributed intelligence. The expenses of their installation and maintenance are reduced as they use cheap devices require no wiring. WSN distributed intelligence could enable the development of different applications supporting real-time traffic safety.

In the WSN-based ITS system, the WSN is composed of many Sensor Nodes, SNs, which are deployed along the roadside and Gateway Node (GN). The main function of a given SN is to monitor a section of road to collect data including vehicle count, direction, and speed. These collected data are sent to the GN which sends it to a Road Side Unit (RSU). the RSU then uses these data along with other traffic-related data received from alternative sources.

Usually, WSN-based applications (e.g., ITS application) incur high communication overhead to support efficient connectivity and communication Elhoseny et al. [2017a,b, 2018]. In ITS environment, clustering would help in addressing the high communication overhead problem. This is because of the following reasons: clustering only allows a Cluster Head (CH) to be involved in the communication Abdelwahab et al. [2017b] and it helps to provide: fault tolerance in a given system, load balanced system, reduced delay and increased connectivity, as well as reduced power consumption (Abdelwahab et al. [2017b]). This leads to maximizing network lifetime (i.e. minimizing the communication overhead thus less power consumption) all of which are required features of ITS applications. This paper aims to provide a trust-based secure selection of cluster head of WSN-based ITS systems.

2. Related Work

Intelligent Transportation Systems (ITS) are gaining considerable momentum in different applications especially those used to increase the safety and improve the efficiency of overall movement of vehicles in traffic. Vehicular Ad-Hoc Network (VANET) represent an important component of ITS which provides communication between vehicles and roadside units using WSN. Substantial research work has been done on WSN secure routing in general and ITS integration with WSN in particular.

Security is an essential and challenging issue in Cluster-based WSN since sensors are usually deployed in hostile environments Elsayed et al. [2017]. The traditional security method cannot be applied for WSN due to its characteristics, such as being an open communication medium, limited computational capabilities of nodes, and the disadvantages of bandwidth constraint Ganesh and Amutha [2013], Sung and Ryou [2014], which make these network more susceptible to malicious attacks than other networks. To address these challenges, a large body of work based on traditional encryption schemes, e.g. Ganesh and Amutha [2013], Lu et al. [2014] attempted to tackle the problem of secure clustering in sensor networks focusing on issues such as dynamic key change, complexity, cluster head election criteria, and so on. For example, SLEACH Xiao-yun et al. [2005] was the first attempt to build a secure clustering model. It prevents sinkhole, selective forwarding and HELLO flooding attacks. However, traditional encryption-based methods in general and SLEACH, in particular, suffer from the required memory size as well as a problem related to network performance and lifetime. Subsequently, a new model was recently proposed Elhoseny et al. [2016a,b] to avoid these limitations and address the memory size problem. This model is based on homomorphic encryption and elliptic curve cryptography. The model greatly improves the network performance and achieves highly secure data aggregation results.

To improve the performance of ITS, Wang and Wang [2010] developed a model dubbed Traffic Infrastructure Based Cluster Routing Protocol with Hand-

off (TIBCRPH). It utilizes existing traffic infrastructures to form the cluster network. To improve packet delivery only one hop range at the node was used, while the entire packet transmission takes place through the intersection only. There were too many assumptions taken into account in the Wang and Wang study, and they were not able to simulate it in the real environment. The selection of dynamic cluster head for each vehicle that is based on handoff metric creates a time delay if the existing CH leaves the cluster.

Shoaib and Song [2013] proposed a zone based hierarchical routing protocol for reducing network overhead by optimization of the time interval for distribution of network control packets based on traffic awareness and mobility. Zones are formed by the division of geographical segments that focus on the 'inter' and 'intra-zone' topology for stability at high speeds which cause frequently changing topologies. The packet delivery ratio is suitable for a dense network but in a sparse network, its performance degrades. In addition, if a single link changes among the nodes (although the links are stable) it will broadcast the entire Link State Packet (LSP) in each zone in order to keep the routing table up-to-date which in turn increases the control overhead.

Bitam and Mellouk [2011] proposed a QoS Swarm Bee Routing Protocol (QoSBeeVanet) for Vehicular Ad-Hoc Networks. QoSBeeVanet is a multipath routing protocol which provides quality of service in VANET. It uses the principle of artificial bee communication. QoSBeeVanet outperforms DSDV and AODV in terms of packet delivery ratio, end-to-end delay, and overhead, in realistic urban settings. However, QoSBeeVanet does not address heterogeneous networks. Toutouh and Alba [2011] configured a Vehicular Data Transfer Protocol (VDTP) with five different NIBC algorithms; Particle Swarm Optimization, Differential Evolution, Genetic Algorithm, Evolutionary Strategy and Simulated Annealing. Results of experiments done on five different sizes of files showed that NIBC outperforms expert configured VDTP. An optimal node selection model was proposed in Elhoseny et al. [2016b] to allow vehicles to forward their messages. During the transmission process, vehicles verify the authenticity of the node to avoid malicious activities. Hashing techniques were used in Guo

et al. [2014], Wasef and Shen [2013] for real-time message authentication to establish a common secret key for private communication in ITSs.

3. Proposed Hierarchical Trust-based Secure Clustering (HiTSeC)

3.1. Problem Formulation

The proposed framework is designed based on the following considerations. Firstly, in a given IRS system, nodes are heterogeneous (using fixed roadside supported with power supply and battery-based sensors installed in the cars/buses). Also, as the vehicle is always moving, CH and cluster formation need be changed over time. Such clustering is unlike static clustering in which, once the cluster is created and CH is selected, they remain the same during the network lifetime. Secondly, ITS is naturally characterized by its mobility Alam et al. [2016]Mantri et al. [2016] which can be accomplished in a dynamic environment. Therefore, for a clustering problem, the selection of CH and cluster formation will be changed regularly with time intervals. Thirdly, usually in ITS environment, there are devices supplied by batteries (e.g., vehicle's sensors), thus saving batteries leads to a longer lifetime network. Fourthly, one of the major challenges of selecting CH is to elect the most trusted node by all cluster members. Otherwise, malicious/misbehaved nodes could be selected as a CH, thus affecting the accuracy and credibility of data received by BS and then the decisions made based on these data. Fifthly, the ITS system depends on the use of roadside supported with power supply (Powered-Node). Such node could be used to address the problem of battery harvesting for a given CH which is always required to perform data preprocessing and send many messages to the BS Mantri et al. [2016]Krishnan and Kumar [2016]. A Powered-Node will be responsible for collecting information and doing real-time processing to later send the processed information to the cloud for further processing and decision making. By adding this CHs Powered-Node, a single or two hops (at maximum) are needed for a message to reach a BS regardless of the nodes positions in the network. The model is designed to work in different environments and network

models. Although the proposed framework is designed to work with heterogeneous applications, energy consumption in the case of homogeneous applications will be reduced due to the balanced initial energy among all sensor nodes.

3.2. Overview of HiTSeC

The HiTSeC method consists of two layers: Layer 2 (the lower layer) and Layer 1 (the higher layer). The Lower layer contains the devices (sensors, RFID devices, people, machines, etc with their ID, thus no IP is assigned). This means that these devices cannot directly access the cloud (Internet). However, as they are parts of an ITS system, they are a critical part of the network. Thus, the cluster head is important. In this layer, the selection of CH and formation of a dynamic cluster will be carried out. When this is done, each node will gather sensed data and send it to their respective CH which will aggregate these data and send to either to the Powered-Node which is resident in the higher layer or Layer 1. This layer consists of powerful IP-enabled devices supported with IoT functions including IEEE 802.15.4-2006 in the physical layer, IEEE 802.15.4e in MAC layer, 6lowpan supported network layer and an application layer with COAP protocol Palattella et al. [2013]. To do real-time processing and communication, the devices in Layer 1 are supposed to be supported with long battery life. Also, in this layer, it is supposed that the multiple base stations can cover all parts of a given network and they are connected in a mesh topology, hence enabling Layer 2 nodes to understand the scenario of the entire network.

The devices in both layer 1 and layer 2 can communicate in different possible ways. For example, one CH might communicate with one BS, two CH might communicate with one BS and one CH might communicate with two base stations, depending on whether the BS is within its radio range of transmission.

3.3. Details of HiTSeC Model

This section describes the details of the proposed HiTSeC Model. The design assumption is first described and then the trust model is presented. The output of the trust model is then used to form the cluster and select its CH.

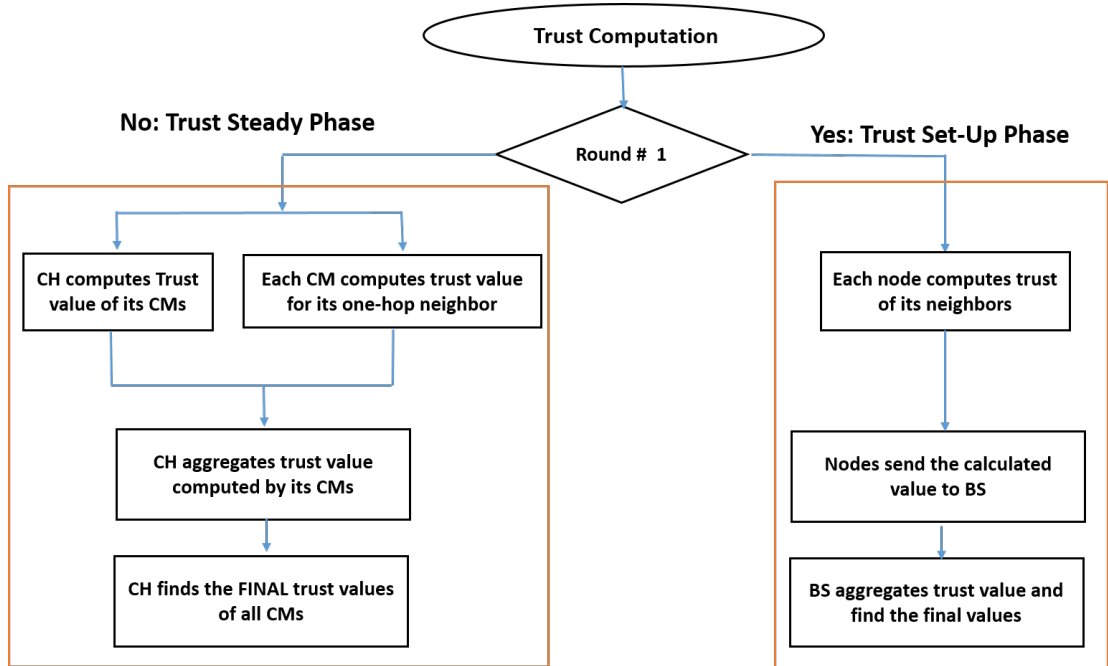
3.3.1. Assumptions

The proposed HiTSeC Model is based on the idea of neighbor counting and indicating the connectivity along with a node residual energy. In addition, it is designed based on the assumption that a cluster formation is made within the radio range of a node transmission. It is also assumed that all the nodes are randomly deployed in the network using UDGM (unit disk graph medium) model Huang et al. [2000]. The mobility is applied to the nodes to make the network dynamic.

3.3.2. Trust Model

A security-based trust mainly relies on the trust computation of a given node. Generally, there are two levels for calculating and managing trustworthiness of nodes in this proposed solution: node level (normal node and CH node) and BS level. Figure (1) shows the main steps of the proposed trust model.

Figure 1: Trust computation model at setup and steady phases



3.3.2.1. *Trust on Node Level.* In this level, every node is responsible for monitoring the behavior of its neighbors and calculating their trust values based on specific metrics. Every trust metric has a certain weight which gives the ability to control or adjust the priority of each metric according to the required application. Equation 1 defines how direct trust value is calculated by node i for node j .

$$DT(i, j) = \sum_{k=1}^m W_k * T_k(i, j) \quad (1)$$

Where m refers to the number of trust metrics ; W_k denotes the weight value of the metric k such that $\sum_{k=1}^m W_k = 1$; $T_k(i, j)$ is the trust value set by node i on metric k for node j .

CH calculates trustworthiness of nodes in its cluster using Equation 1 then asks each member in its cluster to send it the values they computed about their neighbors in the same cluster. Using Equation 2, CH computes the aggregated trust value of each node. Then, it gets the total trust values of nodes in its clusters via Equation 3.

$$AT(j) = \frac{1}{h} * \sum_{r=1}^h DT(r, j) \quad (2)$$

Where h is the number of neighbors of node j ; $DT(r, j)$ represents the direct trust value computed by node r for node j .

$$TT(j) = W_a * DT(CH, j) + W_b * AT(j) \quad (3)$$

Where W_a and W_b are weighting factors such that $W_a + W_b = 1$.

3.3.2.2. Trust on BS Level. In this level, nodes send the calculated values to the nearest BS to aggregate them and find the final trust values then evaluate which nodes are trusted and which ones are malicious using user-defined threshold. Equation 2 shows the aggregated value is computed for node j . Every BS also collects trust values aggregated by the other BS to be used as indirect trust observations. In addition, the accuracy of data sent from every CH will be evaluated in BS by users, if data are correct, CH and its CMs will get a reward by increasing their trust value. Otherwise, they will be punished by reducing their trust values.

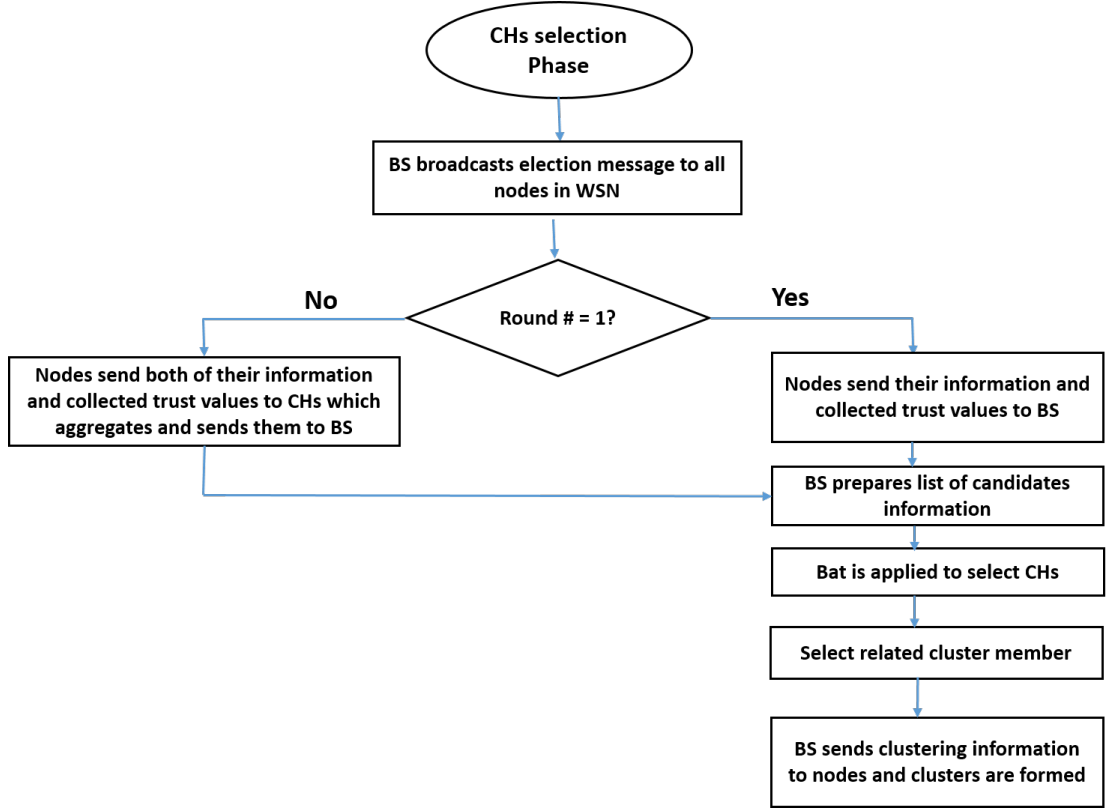
3.3.3. Clustering Model: BOA-based Clustering

The clustering model suggested in this paper is based on the trust level (presented above) and Bat Optimization Algorithm. As the clustering problem is generally aimed to find the best solution from all feasible solutions, thus it can be considered as an optimization problem. Bat Optimization Algorithm (BOA) will be used as it is much superior to other algorithms in terms of accuracy and efficiency Yang [2010]. Additionally, as reported in Yang [2013], Bat algorithm is more powerful than PSO, GA and harmony search because BOA uses a good combination of major advantages of these algorithms in a certain way.

As shown in Figure (2) Bat-based clustering model generally consists of the following steps:

1. **Initiation of cluster head election process:** BS starts the cluster head election process by broadcasting a message to all nodes in the network to send it their IDS , list of neighbors, residual energy level and the calculated trust values for their neighbors.
2. **Preparing a list of candidates information:** BS calculates the final trust value for all nodes by aggregating the collected trust values about each one. Then, it prepares a final list that contains node id (N_{id}), residual energy (RE_i), final trust value (T_i) and number of neighbors ($Neighbors_{number}$).

Figure 2: Bat-based CH Selection Model



3. **Applying BOA algorithm:** BS apply BOA algorithm to select the set of trusted nodes which will cover all nodes in the network and have a sufficient energy level to achieve the mission of CHs. Equation 4 defines fitness function used by BOA to compute the cost of each generated set of cluster heads. BOA searches for the best set which should have zero cost to be the selected one. The following steps show how the BOA algorithm works to find this best set:

- (a) BOA algorithm takes a set of parameters needed for search process: number of nodes (n), minimum number of required cluster head (Min_{CHs}), maximum number of required cluster head (Max_{CHs}), list of candidates information which is prepared in Step 3, residual

energy threshold (RE_{th}), trust threshold (T_{th}), probability of discovering bat's preys (p_a) and the maximum number of iterations (Max_{itr}).

- (b) The algorithm begins by generating an initial random set of solutions (S).
- (c) The cost of each solution is calculated.
- (d) BOA initializes iteration number t with zero and starts loop end when t is larger than or equal Max_{itr} .
- (e) In each iteration, a new solution (J) is randomly generated, then its cost is computed. After that, solution (I) in S is randomly selected and its cost compared to solution J . If the cost of J is less than the cost of I , then solution I is replaced by solution J .
- (f) A fraction p_a of worse solutions is abandoned and replaced by new ones. Then, high-quality solutions are kept and all solutions are ranked to find the best one.
- (g) Iteration number t is incremented by one and if it is still smaller than Max_{itr} , the two previous steps are repeated; otherwise, BOA algorithm returns the best solution.

$$f(S) = \begin{cases} 0, & \forall (CH_e \in S) \in A, \bigcup_{e=0}^z neighbors(CH_e) = n \\ 1, & Otherwise \end{cases} \quad (4)$$

In Equation 4, S represents a solution and consists of set of randomly selected cluster heads, CH_e refers to cluster head in S containing bat's prey e , z is the number of cluster heads in S , n is the number of nodes in the network and A is the set of nodes that have $RE \geq RE_{th}$ and $T \geq T_{th}$.

4. **Selecting related cluster members:** After selecting CHs, for each node, BS chooses the nearest elected CH to it to be its CH.
5. **Sending clustering information and forming clusters:** A message is sent to every node selected as CH to inform it about its selection and to

the other non-CHs nodes to inform them about their related CHs. After that, cluster members should send the sensed data periodically to CH to aggregate them and later send the collected data to BS. CH should include its ID and the IDs of its related CMs with the disseminated data because this is needed in the data accuracy evaluation process.

6. **New election process:** After t time or when the energy level of one or more of cluster heads become below a user-defined threshold, BS starts a new cluster head election process by broadcasting a *new election* message to all CHs. After that, each CH should aggregate the required information for the election process from nodes in its cluster and send it to the base station to choose the new CHs through Steps: 2,3,4 and 5.

4. Results and Discussion

In this section, the evaluation of proposed cluster model is presented. All the conducted experiments are performed using MATLAB (R2015a). The proposed model is tested under heterogeneous network with the following characteristics. The number of nodes in the network is 100 nodes which are randomly distributed and deployed in region of $100 \text{ m} \times 100 \text{ m}$. The evaluation is performed under different metrics: network lifetime, average residual energy and average trust value of CHs.

Different scenarios were designed to evaluate the proposed model. Firstly, we investigated the effect of BS location on the performance of clustering model by trying two different location of BS in our experiments. This is because the used network model is centralized and depends mainly on BS in clustering WSN. Secondly, the performance of three benchmark models (SEP and DEEC supporting heterogeneity and LEACH supporting homogeneous networks) were compared with our proposed one under the same network type/model and the same parameters listed in table 1.

Table 1: Simulation parameters and their values

Parameter	Value
Area (Length \times Width)	100 \times 100
Network Size (number of nodes)	100
Initial energy of normal node	0.5 J
Initial energy of advanced node	1 J
Electronics of transmitter (E_{TX})	50 nJ/bit
Electronics of receiver (E_{RX})	50 nJ/bit
Transmitter amplifier (E_{fs})	10 pJ/bit/m ²
Transmitter amplifier (E_{mp})	0.0013 pJ/bit/m ⁴
Data aggregation energy (EDA)	5 nJ/bit
Packet length from sensor node/CH to BS	4000 bits
Packet length from sensor node to CH	4000 bits
Packet length from BS to CH/sensor node	200 bits
Trust value range	[0,1]
Percentage of nominated cluster heads (p)	0.1
Discovery rate of alien solutions p_a	0.25
Weighting factor W_a	0.5
Weighting factor W_b	0.5

4.1. Network Lifetime

The main purpose of network clustering techniques is increasing network lifetime, i.e., reducing the number of nodes which die during network working time. This will lead to an extension of the network lifetime. We measure the lifetime of WSN based on the number of alive nodes over rounds. Also, for better performance evaluation, network lifetime is measured under both homogeneous and heterogeneous networks as LEACH supports homogeneous networks while both SEP and DEEC support heterogeneity.

4.1.1. Scenario of Homogeneous Networks

A homogeneous network is a network that consists of nodes with the same capabilities. Here, all nodes start with the same initial level of energy (0.5 J). Table 2 shows four figures for network lifetime of four different models when BS is, firstly, in the center of the environment, and secondly, when it is located in position (100,50), thirdly and fourthly when BS is located at position (100,50) and (100,100) respectively. The results illustrate that HiTSeC outperforms LEACH, SEP, and DEEC when WSN is homogeneous, even when the location of BS is changed. Dead nodes appear firstly in SEP and LEACH respectively, and over rounds, the number of alive nodes in both becomes closer. When BS is at (100,50), HiTSeC begins to have dead nodes before DEEC while at (100,100), they start having dead nodes at a similar time. After 900 rounds, network lifetime of HiTSeC become significantly better than the three models as the decay in the number of alive nodes over time using HiTSeC is the slowest.

4.1.2. Scenario of Heterogeneous Networks

A heterogeneous network is a network which consists of two types of nodes: advanced nodes and normal nodes. The advanced nodes have resources and capabilities higher than normal ones. In this scenario, we set the percentage of the advanced nodes in the four models (HiTSeC, LEACH, SEP, and DEEC) at 10%. Also, the initial energy level of the advanced nodes is $1J$ while in the normal nodes, it is $0.5J$. The results of this scenario are shown in Table 3. This table illustrates four figures (e,f,g, and h) for network lifetime of four different models when BS is at (50,50), (50,100), (100,50), and (100,100), respectively. These results prove that HiTSeC also works well with heterogeneity. It can be noticed that over rounds, the lifetime of WSN using HiTSeC is considerably better than LEACH and SEP. While the results illustrate that LEACH starts to have dead nodes before SEP but, the performance of SEP becomes worse than LEACH after round number 800. In the two figures, dead nodes appear in HiTSeC before DEEC but after 1000 rounds, the number of alive nodes in HiTSeC becomes highly better than in DEEC. The results also show that dead

Table 2: Network Lifetime Comparison: Homogeneous Network

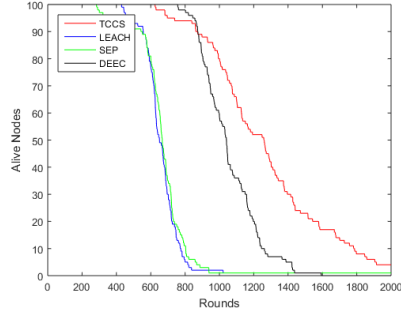


Figure (a): Network lifetime when WSN is homogeneous and BS is located at (50,50)

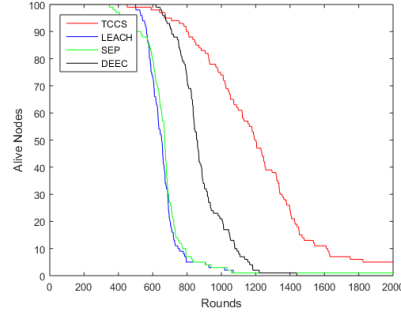


Figure (b): Network lifetime when WSN is homogeneous and BS is located at (50,100)

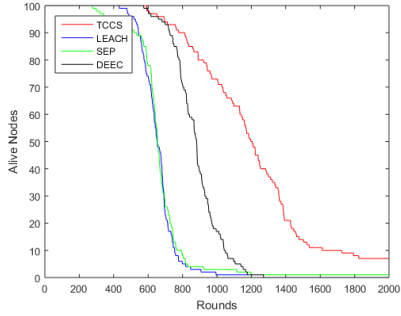


Figure (c): Network lifetime when WSN is homogeneous and BS is located at (100,50)

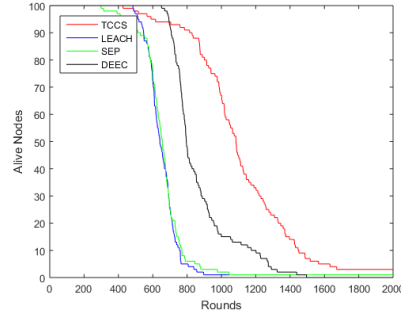


Figure (d): Network lifetime when WSN is homogeneous and BS is located at (100,100)

nodes appear earlier when BS located in the center of the area (figure (e)) than when BS is located in the north of the area at position (100,50) (figure (g)). However, over rounds, the decrease in the number of alive nodes at BS location (100,50) is much faster than that the rate at BS location (50,50).

4.2. Efficient Use of Energy

An efficient use of network energy could be measured by Residual Energy (RE). DR of a node refers to the current remaining amount of energy it has. As energy efficiency is one of our model goals, here we measured it using the average residual energy of nodes in the network. The model will be energy efficient if the amount of residual energy in the network declines slowly over rounds. The

Table 3: Network Lifetime: Heterogeneous

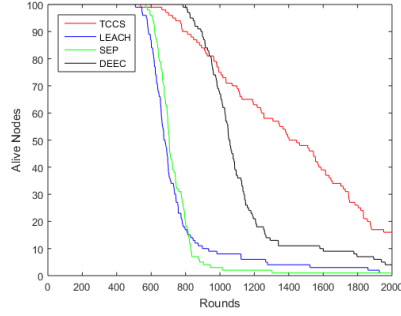


Figure (e): Network lifetime when WSN is heterogeneous and BS is located at (50,50)

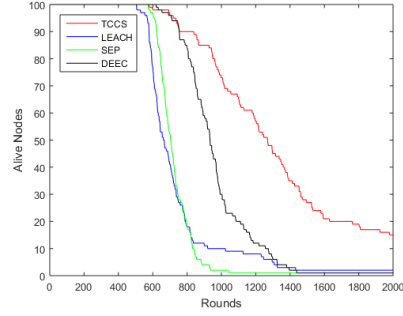


Figure (f): Network lifetime when WSN is heterogeneous and BS is located at (50,100)

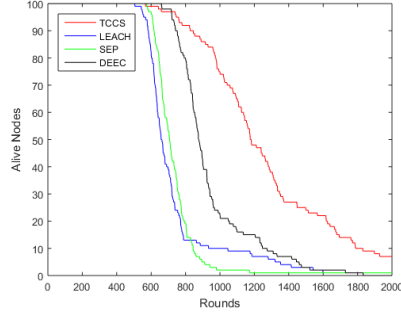


Figure (g): Network lifetime when WSN is heterogeneous and BS is located at (100,50)

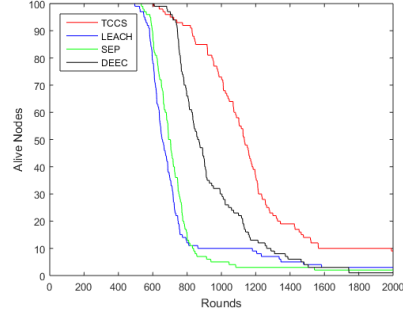


Figure (h): Network lifetime when WSN is heterogeneous and BS is located at (100,100)

average residual energy in WSN can be computed as follows:

$$AverageResidualEnergy = \frac{1}{n} * \sum_{i=1}^n RE_i \quad (5)$$

Where n is the number of nodes in a network; RE_i refers to residual energy of node i (N_i)

Table 4 shows four figures (i,k,l,and m) for the average residual energy of the four models where the network is homogeneous and BS is loctated at (50,50), (50,100), (100,50), and (100,100), respectively. While table 5 illustrates results of the average residual energy when the network is heterogeneous with 10% advanced nodes. As shown in all figures, reflected best performance followed

by DEEC, and finally, we find LEACH and SEP which share approximately the same amount of the average residual energy. Also, results show that the average of remaining energy in the heterogeneous network is higher than that in the homogeneous networks. The reason is homogeneous networks have only normal nodes while the heterogeneous network has a percentage of advanced nodes which have energy higher than normal nodes so the average of remaining energy of nodes in the heterogeneous network will be the higher.

Table 4: Residual Energy: Homogeneous

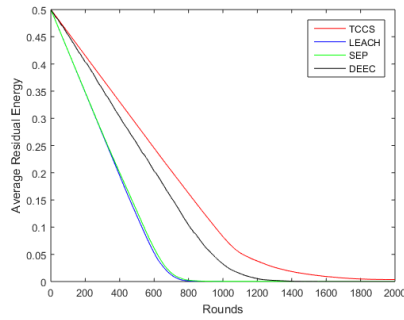


Figure (j): Average RE when WSN is homogeneous and BS is located at (50,50)

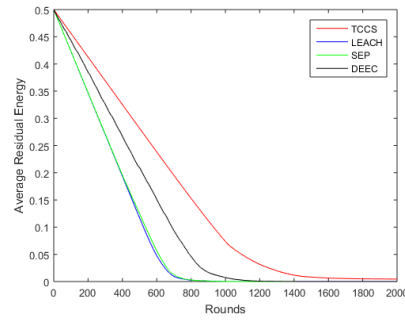


Figure (k): Average RE when WSN is homogeneous and BS is located at (50,100)

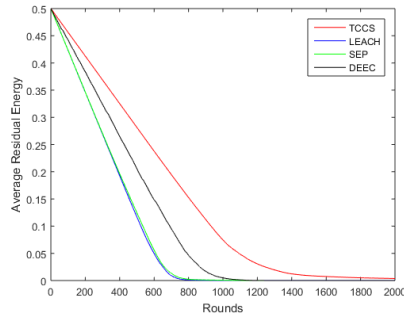


Figure (l): Average RE when WSN is homogeneous and BS is located at (100,50)

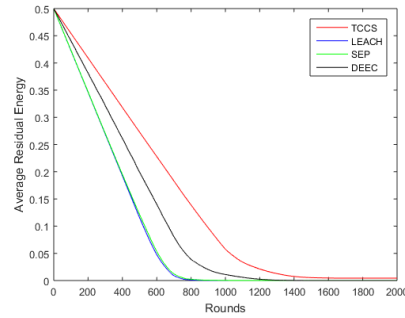
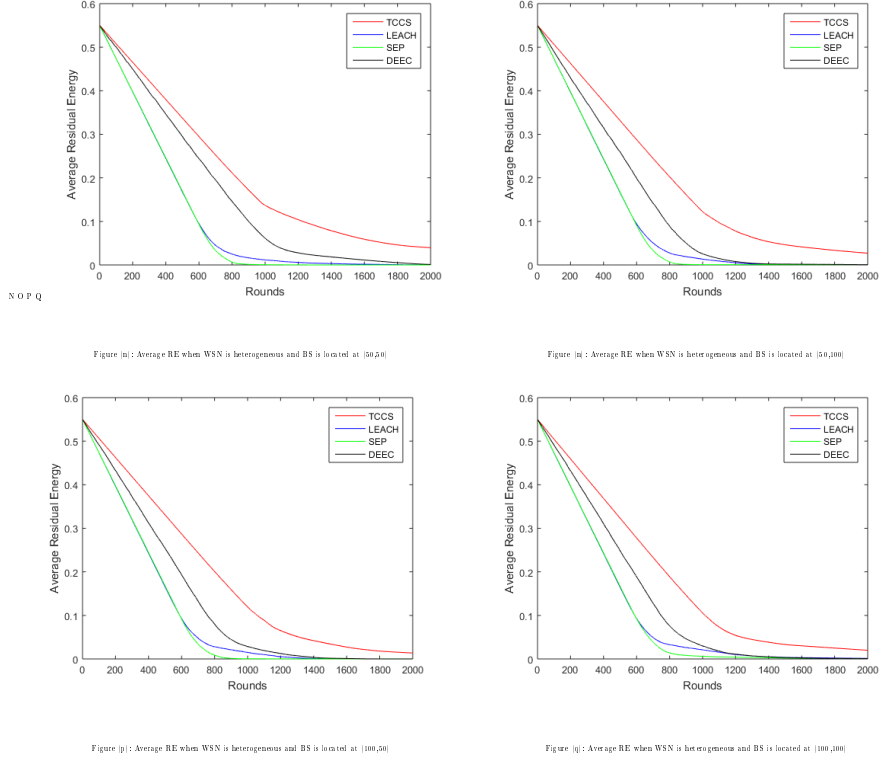


Figure (m): Average RE when WSN is homogeneous and BS is located at (100,100)

4.3. Average Trust Value of Cluster Heads

HiTSeC is designed to ensure trustworthiness of CH, and this goal is achieved using the defined cost function of BOA algorithm which makes the CS only

Table 5: Residual Energy: Heterogeneous



selects nodes having trust value larger than or equal to trust threshold T_{th} to be the CHs. We use the average trust value of CH over rounds and under a different percentage of compromised nodes in the network for evaluating the success of our model in electing trusted CHs. The average trust value of selected CHs is calculated as follows:

$$AverageTrustValueofCHs = \frac{1}{cn} * \sum_{i=1}^{cn} T_{CH_i} \quad (6)$$

Where cn is the number of the cluster heads and T_{CH_i} is the trust value of CH_i

In our experiments, trust value of nodes is computed as a value between 0

and 1. While, malicious nodes in Figures 3,4 and 5 are set at 10% , 30% and 50%, respectively. Additionally, we inputted T_{th} in Figure 4 at 0.35 which is less than T_{th} in Figures 3 and 4 that equal to 0.5 . The reason is 50% of the nodes in Figure 5 are attacked so there is a need for minimizing the value of T_{th} , specially over time and when residual energy is low, to enable CS to find trusted CHs, which have a sufficient level of energy and together cover all nodes in the network. The results depicted in three figures demonstrate that the average trust value of selected CHs using HiTSeC is high over rounds and always larger than the specified T_{th} value even if the half the nodes in WSN are compromised.

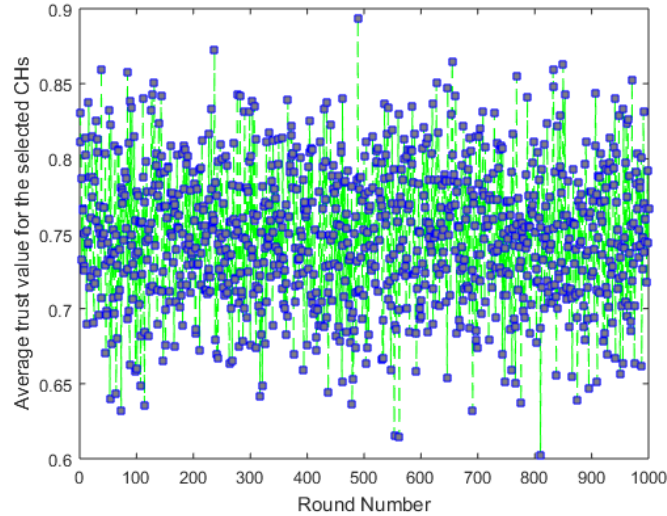


Figure 3: Average trust value of the cluster heads when the percentage of malicious nodes is 10% and $T_{th} = 0.5$

5. Conclusion and Future Work

In this paper, we presented a bio-inspired trust based cluster head selection approach for WSN used in ITS. The used bio-inspired optimization algorithm is the BOA algorithm. Cluster heads are selected based on three parameters which are residual energy, trust value and the number of neighbors. BOA algorithm

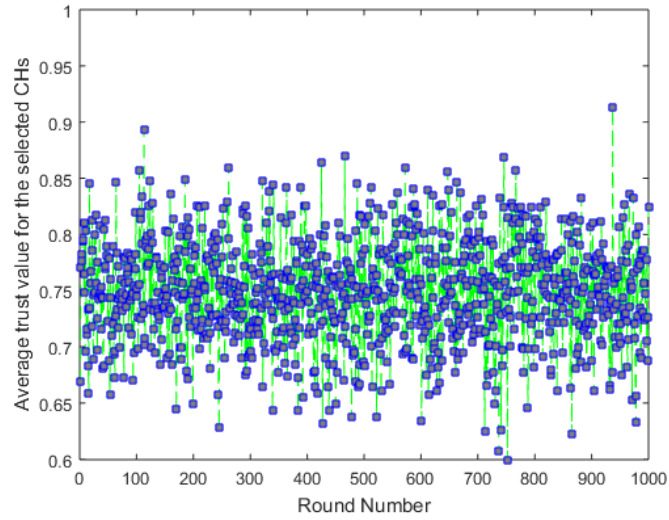


Figure 4: Average trust value of the cluster heads when percentage of malicious nodes is 30% and $T_{th} = 0.5$

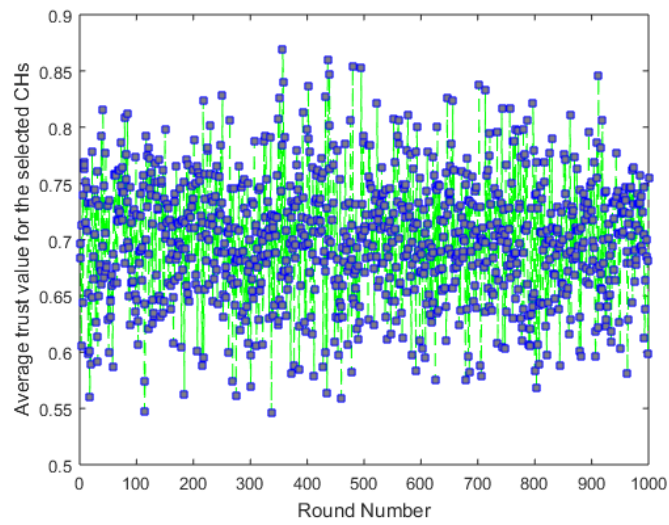


Figure 5: Average trust value of the cluster heads when the percentage of malicious nodes is 50% and $T_{th} = 0.35$

is used to search for the set of nodes which have residual energy and trust value larger than or equal user-defined threshold and in the same time, this set of nodes should together cover every node in the network. From, the simulation results, it can be concluded that our proposed model (HiTSeC) is energy efficient and has network lifetime better than the three well-known clustering algorithms: LEACH, SEP, and DEEC. In addition, HiTSeC can select a trusted CH even if the percentage of malicious nodes in the network is 50% or less. Therefore, HiTSeC model can be used to address the secure and efficient clustering problem for WSN adopted in ITS applications.

In future work, we are planning to evaluate and refine the proposed system to consider the case where the BS is located outside the field as well as the cases where the field size is 200m x 200m, 300m x 300m, and 400m x 400m to consider different application scenarios. Another future work could be using recent bio-inspired optimization algorithms such as Chicken Swarm Optimization to achieve CH selection process.

References

- Abdelwahab, S., Gaber, T., Wahed, M., 2017a. Trust and bio-inspired-based clustering techniques in wireless sensor networks: A survey. In: International Conference on Advanced Intelligent Systems and Informatics. Springer, pp. 714–723.
- Abdelwahab, S., Gaber, T., Wahed, M., 2017b. Trust and bio-inspired-based clustering techniques in wireless sensor networks: A survey. In: International Conference on Advanced Intelligent Systems and Informatics. Springer, pp. 714–723.
- Alam, M., Ferreira, J., Fonseca, J., 2016. Introduction to intelligent transportation systems. In: Intelligent Transportation Systems. Springer, pp. 1–17.
- Bitam, S., Mellouk, A., 2011. Qos swarm bee routing protocol for vehicular ad

- hoc networks. In: Communications (ICC), 2011 IEEE International Conference on. IEEE, pp. 1–5.
- Elhoseny, M., Elminir, H., Riad, A., Yuan, X., 2016a. A secure data routing schema for wsn using elliptic curve cryptography and homomorphic encryption. *Journal of King Saud University-Computer and Information Sciences* 28 (3), 262–275.
- Elhoseny, M., Farouk, A., Zhou, N., Wang, M., Abdalla, S., Batle, J., 2017a. Dynamic multi-hop clustering in a wireless sensor network: Performance improvement. *Wireless Personal Communications* 95 (4), 3733–3753.
- Elhoseny, M., Tharwat, A., Farouk, A., Hassanien, A., 2017b. K-coverage model based on genetic algorithm to extend wsn lifetime. *IEEE Sensors Letters* 1 (4), 1–4.
- Elhoseny, M., Tharwat, A., Yuan, X., Hassanien, A., 2018. Optimizing k-coverage of mobile wsns. *Expert Systems with Applications* 92 (2018), 142–153.
- Elhoseny, M., Yuan, X., El-Minir, H. K., Riad, A. M., 2016b. An energy efficient encryption method for secure dynamic wsn. *Security and Communication Networks* 9 (13), 2024–2031.
- Elhoseny, M., Yuan, X., Yu, Z., Mao, C., Elminir, H., Riad, A., 2015. Balancing energy consumption in heterogeneous wireless sensor networks using genetic algorithm. *IEEE Communications Letters* 19 (12), 2194–2197.
- Elsayed, W., Elhoseny, M., Sabbeh, S., , Riad, A., 2017. Self-maintenance model for wireless sensor networks. *Computers and Electrical Engineering*.
- Fouad, M. M., Oweis, N. E., Gaber, T., Ahmed, M., Snasel, V., 2015. Data mining and fusion techniques for wsns as a source of the big data. *Procedia Computer Science* 65, 778–786.

- Gaber, T., Hassanien, A. E., 2014. An overview of self-protection and self-healing in wireless sensor networks. In: *Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations*. Springer, pp. 185–202.
- Ganesh, S., Amutha, R., 2013. Efficient and secure routing protocol for wireless sensor networks through snr based dynamic clustering mechanisms. *Journal of Communications and Networks* 15 (4), 422–429.
- Guo, S., Zeng, D., Xiang, Y., 2014. Chameleon hashing for secure and privacy-preserving vehicular communications. *IEEE Transactions on Parallel and Distributed Systems* 25 (11), 2794–2803.
- Huang, X., Behr, U., Wiesbeck, W., 2000. Automatic cell planning for a low-cost and spectrum efficient wireless network. In: *Global Telecommunications Conference, 2000. GLOBECOM'00. IEEE. Vol. 1. IEEE*, pp. 276–282.
- Klein, L. A., 2001. Sensor technologies and data requirements for ITS.
- Krishnan, A. M., Kumar, P. G., 2016. An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous wsn. *Wireless Personal Communications* 90 (2), 423–434.
- Lu, H., Li, J., Guizani, M., 2014. Secure and efficient data transmission for cluster-based wireless sensor networks. *IEEE transactions on parallel and distributed systems* 25 (3), 750–761.
- Mantri, D. S., Prasad, N. R., Prasad, R., 2016. Mobility and heterogeneity aware cluster-based data aggregation for wireless sensor network. *Wireless Personal Communications* 86 (2), 975–993.
- Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., Dohler, M., 2013. Standardized protocol stack for the internet of (important) things. *IEEE communications surveys & tutorials* 15 (3), 1389–1406.

- Rawat, P., Singh, K. D., Chaouchi, H., Bonnin, J. M., 2014. Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of supercomputing* 68 (1), 1–48.
- Shoaib, M., Song, W.-C., 2013. Traffic aware optimized zone based hierarchal link state routing protocol for vanet. In: *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*. IEEE, pp. 3117–3122.
- Sung, S., Ryou, J., 2014. Id-based sensor node authentication for multi-layer sensor networks. *Journal of Communications and Networks* 16 (4), 363–370.
- Texas-Transport-Institute, 2015. 2015 Urban Mobility Scorecard. <https://mobility.tamu.edu/ums/>, [Online; accessed 24-November-2017].
- Toutouh, J., Alba, E., 2011. Performance analysis of optimized vanet protocols in real world tests. In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, pp. 1244–1249.
- Wang, T., Wang, G., 2010. Tibcrph: traffic infrastructure based cluster routing protocol with handoff in vanet. In: *Wireless and Optical Communications Conference (WOCC), 2010 19th Annual*. IEEE, pp. 1–5.
- Wasef, A., Shen, X., 2013. Emap: Expedite message authentication protocol for vehicular ad hoc networks. *IEEE Transactions on Mobile Computing* 12 (1), 78–89.
- Worldbank.org, 2015. Global Road Safety Facility . <http://www.worldbank.org/en/programs/global-road-safety-facility#4>, [Online; accessed 24-November-2017].
- Xiao-yun, W., Li-zhen, Y., Ke-fei, C., 2005. Sleach: Secure low-energy adaptive clustering hierarchy protocol for wireless sensor networks. *Wuhan University Journal of Natural Sciences* 10 (1), 127–131.

- Yang, X.-S., 2010. A new metaheuristic bat-inspired algorithm. Nature inspired cooperative strategies for optimization (NICSO 2010), 65–74.
- Yang, X.-S., 2013. Bat algorithm and cuckoo search: A tutorial.